PRIVACY LITERACY 2.0: A THREE-LAYERED APPROACH COMPREHENSIVE LITERATURE REVIEW

_____

A Dissertation

Presented to

The Faculty of the School of Teaching and Learning

Sam Houston State University

_____

In Partial Fulfillment

of the Requirements for the Degree of

Doctor of Education

_____

by

Slimane Aboulkacem

May, 2020

PRIVACY LITERACY 2.0: A THREE- LAYERED APPROACH COMPREHENSIVE LITERATURE REVIEW

by

Slimane Aboulkacem

_____

APPROVED:

Committee Members:

Hannah R. Gerber, PhD
Committee Director

Debra P. Price, PhD
Committee Member

Nancy B. Votteler, EdD
Committee Member

Benita R. Brooks, PhD
Committee Member

Lory E. Haas, EdD
Committee Member

Victoria Hollas, PhD
Committee Member

Stacy L. Edmonson, EdD
Dean, College of Education

DEDICATION

I dedicate this dissertation to my dad's soul, legacy, and memory. His perseverance is a continuous inspiration for me. To my mom, this work is completed thanks to her persistent encouragements.

ABSTRACT

Aboulkacem, Slimane, Privacy literacy 2.0: A three-layered approach comprehensive literature review. Doctor of Education (Literacy Education), May, 2020, Sam Houston State University, Huntsville, Texas.

With technological advancement, privacy has become a concept that is difficult to define, understand, and research. Social networking sites, as an example of technological advancements, have blurred the lines between physical and virtual spaces. Sharing and self-disclosure with our networks of people, or with strangers at times, is becoming a socially acceptable norm. However, the vast sharing of personal data with others on social networking sites engenders concern over data loss, concern for unintended audience, and an opportunity for mass surveillance.

Through a dialectical pluralism lens and following the comprehensive literature methodological framework, the purpose of this study was to map and define what it means to be a privacy literate citizen. The goal was to inform privacy research and educational practices.

The findings of this study revealed that placing the sole responsibility on the individual user to manage their privacy is an inefficient model. Users are guided by unmasked and hidden software practices, which they do not fully comprehend. Another finding was the noticeable increase of citizen targeting and liquified surveillance, which are accepted practices in society. Liquified surveillance takes any shape; is both concreate and discrete; and it happens through complete profile data collection as well as raw data aggregation.

Privacy management, as a research model or management approach, does not prevent data from leaking nor does it stop surveillance. For privacy to be successful,

privacy engineering should include citizens' opinions and require high levels of data transparency prior to any data collection software design. The implications of this study showed that privacy literacy 2.0 is a combination of several inter-connected skills, such as knowledge about the law, software, platform architecture, and the psychology of self-disclosure.

KEY WORDS: Privacy literacy, Privacy law, Social networking sites, Self-disclosure, Big data, Privacy management, Privacy concern.

ACKNOWLEDGEMENTS

First, I acknowledge my parents, Messaoud and Khadidjah Aboulkacem, who have always been there for me, supported me, cheered my love of learning, and who instructed me to respect knowledge and work hard to obtain it. Additionally, I am forever grateful to my partner in crime, who elevated me with her wisdom and love. To my family and what they continue to do to level me up. Without their sacrifices and belief in me, I would not have completed this work. I am also grateful to be blessed with nieces and nephews who continue to inspire me with their smiles and wishes to become better than their uncle. Without the support of my family, I would not have completed this dissertation.

Sincere thanks go to Dr Taha Merghoub for his encouragements and advice, and to Salah Hadj Aissa for his support along this journey. Another sincere thank you goes to Dr Gerber with whom I worked as a research assistant for my time at the graduate school. I thank her for her advice, work ethics, and dedication to learning and research. Another special thank you goes to Dr Samuel Sullivan, Dr Price and Dr Votteler for being the first who encouraged me to earn my doctorate degree at Sam Houston State University. A sincere thanks also goes to Dr Haas for supporting me as a researcher and for her mentorship. Their support was tremendous and without these people around me, I would not have come this far.

Many thanks go to my Sam Houston State University family in Huntsville. I could not have asked for a more supportive doctoral assistantship and experience. A particular acknowledgment goes to the administration of the Literacy department, which allowed me the opportunity to attend a multitude of conferences and professional development

sessions. They have added so much value to me as a person and to my dissertation work. Additionally, thank you to my friends, especially the three stooges, Barbie, Marcela, and Shelly, who have supported me whenever I thought of quitting the process. I cannot forget another friend, Alphonse, who has always told me, “Get it done man!” These friends were always there to lift me up during the years of my coursework and dissertation writing and provided emotional support whenever I was overwhelmed. I could not ask for a better family of friends and coworkers.

I would like to acknowledge my committee members: Dr. Hannah Gerber (Dissertation Chair), Dr. Debra Price, Dr. Nancy Votteler, Dr Benita Brooks, Dr Lory Haas, and Dr Victoria Hollas. They have guided me through this dissertation and inspired me with their abundant experiences and vast knowledge. Thanks to their wisdom and advice, I am a better scholar and researcher today.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Page

CHAPTER I

Introduction

Chapter Overview

In this chapter, I describe my cultural beliefs and how they relate to online privacy and personal data protection. Additionally, I introduce the methodological framework in eight steps. The chapter also states the goal of the study, my philosophical stance, and the comprehensive literature review (CLR) guiding research questions. Finally, I mention the limitations and delimitations relevant to conducting this study.

Introduction

In 2019, I participated in 'OneTrust' professional development day with privacy policy lawyers, company managers, and privacy professionals in Houston, Texas, in the United States. During the meeting, we discussed issues related to compliance with the General Data Protection and Regulation law (GDPR) and the California Consumer Protection Act (CCPA). I noticed, I was the only participant from the education discipline; other participants were either business owners/managers or lawyers. During the lunch break, while I was in line networking and picking delicious food, I was stopped by a CEO of a renowned Houstonian training organization. He asked me, "What company do you work for?" I replied, "I work at a public university as a research assistant… a doctoral student… writing my doctoral dissertation." He got quite excited, shook my hand, uttered his name, and asked, "A doctorate in privacy? Since we talk privacy here. . ." I spelled my name back and replied, "Yes! A doctorate in privacy, and particularly exploring privacy literacy." He froze and looked at me pondering: "Literacy? Huh! Interesting." Waves of silence and curiosity filled his mind. "Could you tell me

more?" The greyish silver-haired CEO was delightfully surprised with the concept of privacy literacy, stopped picking items for his lunch, and waited eagerly for what this young man from another world had to say about privacy literacy. "It is transferring what we have learned so far in today's training about law and policy, about technologies such as social media, data usage in life, etc., to university students; and from there to the general public", I stated. I told him, "I work on bringing awareness and the same way the companies know the ins and outs of data usage, processing, law, and protection; I make sure our students are in control and know their privacy rights." The businessman responded, "I need you to come speak to us, at my organization, about privacy literacy. Take my workers for your students." He continued, "In fact, the new law in California is all about the customer. That is privacy literacy then." I nodded, "It sure is."

Daily life as well as the scholarly literature are filled with images of online privacy and concerns for losing it. Reading the iconic groundbreaking *1984* by George Orwell (1949) or the mysterious panopticon conceptualized by Jeremy Bentham (1790 and 1791), as theorized by Michel Foucault (1975) in his book *Surveiller et Punir: Naissance de la Prison*, one could stop and ponder: how does it feel to be watched by someone, intensively, regularly, and continuously? How would it feel if someone could know where we are headed before we ride-in our car? What if some strangers could know what diseases we have or might have? What intimate things did we research online? What items did we buy that we did not want anybody to know about? In other words, how does privacy feel under constant watch?

The historic examples mentioned above are from dystopian literature. Today, we live in information and swim in data. For example, children can have digital footprints

through what their parents share about them, maybe even before they know how to use any digital devices. The growth of technology is exponential and is inherent in almost every life-related action, from as simple as grocery shopping errands to complex programmable actions such as smart houses run by sensors and supersmart machines. We carry phones and mobile devices and enjoy the features of photography, music, and connectivity. The functionalities the phones offer such as remote pay, health monitoring, and navigation services all require data. Phones and other portable devices need a profile of who we are, and as a condition for a returned quality service. Privacy has taken many shapes and its scholarship has been present in different disciplines as documented in

Table 1. *Privacy related research across disciplines*

Discipline	**Example Citations**
Law	Bedi, 2013; Carbone, 2015; De Hert, Papakonstantinou, Malgieri, Beslay, & Sanchez, 2018; Evans, 2017; Gellert, 2018; Murphy, 2016.
Privacy Policy	DeNardis & Hackl, 2015; Goodrum, 2014; Metzger & Docter, 2003; Montgomery, 2015; Napoli, 2015; Schintler & Kulkarni, 2014.
Economics	Fuchs, 2012b; Langenderfer & Miyazaki, 2009.
Research and Development	De Wolf, Vanderhoven, Berendt, Pierson, & Schellens 2017; Gadekar & Pant, 2015; Kshetri, 2014.

Education	Alt, 2015; Bruneel, De Wit, Verhoeven, & Elen, 2013; Kyei-Blankson, Iyer, & Subramanian, 2016; Lehavot, 2009; Marwick & boyd, 2011; Trepte, Teutsch, Masur, Eicher, Fischer, Hennhöfer, et al., 2015.
Health Privacy	Fu-Yuan Hong & Su-Lin Chiu, 2016; Kim, 2015; Merchant, Weibel, Pina, Griswold, Fowler, Ayala, Gallo, et al., 2017; Syn & Kim, 2016.

Privacy literacy is strongly connected with other literacies such as media and information literacy (Potter 2014) and digital literacy (Park, 2013). Regarding privacy literacy, citizens and users of social networking sites (SNSs) need privacy protection strategies and need to know how data are collected and processed on their behalf (Marwick & boyd, 2014). Social networking sites' privacy research has focused on various topics as illustrated in Table 2.

Table 2. *Privacy research in relation to social networking sites*

SNSs' Privacy Research Topics	**Example Citations**
Self-disclosure	Cheung, Lee, & Chan, 2015; Choi & Bazarova, 2015; Farinosi & Taipale, 2018; Liang, Shen, & Fu, 2017; Marwick & boyd, 2011; Tsay-Vogel, Shanahan, & Signorielli, 2018.
Networked Privacy	Marwick & boyd, 2014.

Users' Trust	Fogel & Nehmad, 2009; Rifon, LaRose, & Choi, 2005; Waldman, 2015; Wu, Huang, Yen, & Popova, 2012.
Privacy Management	Child et al., 2012; Child & Starcher, 2016; Herrman & Tenzek, 2017; Kezer, Sevi, Cemalcilar, & Baruh, 2016; Petronio, 2013
Privacy Paradox	Brinson & Eastin, 2016; Dienlin & Trepte, 2015a; Hallam & Zanella, 2017; Hargittai & Marwick, 2016; Kokolakis, 2017
Privacy Concern	Baek, Kim, & Bae, 2014; Baruh & Popescu, 2017; Child, Haridakis, & Petronio, 2012; Gopal, Hidaji, Patterson, Rolland, & Zhdanov, 2018; Jeong & Kim, 2017; Kyei-Blankson et al., 2016
Concern for Surveillance	De Zwart, Humphreys, & Van Dissel, 2014; Dencik, Hintz, & Cable, 2016; Fuchs, 2012a; Marwick, 2012; Montgomery, 2015
Big Data and Digital Prints	(Baruh & Popescu, 2017; Bertot, Gorham, Jaeger, Sarin, & Choi 2014; Everson, 2017; Ewbank, 2016; Gerber & Lynch, 2017; Schintler & Kulkarni, 2014.
Citizen Profiling and Marketing Targeting	Wachter, 2018; O'Neil, 2017.
Algorithms and Facial Recognition	Bossewitch & Sinnreich, 2013; Bloom & Clark, 2016; Kosinski, 2017; Kosinski, Stillwell, & Graepel, 2013; Power, 2016

Statement of the Problem

Privacy in Western countries, especially in the U.S. manifests itself as a multi-faceted concept and practice (Baek et al., 2014; Baruh & Popescu, 2017; Ewbank, 2016, 2016; Petronio, 2013; Wachter, 2018). Before the age of new media, the Internet, and SNSs, privacy used to be confounded to physical presence in public with family or friends (Warren & Brandeis, 1890). Fast-forward, new media have evolved, and many forms of participatory media appealed to citizens for convenience and ease of access (Aboulkacem, 2019; Aboulkacem & Haas, 2018; Aboulkacem, Haas, & Winard, 2018; Berkowitz, 2014; Kember & Zylinska, 2012; Fleming, 2014; Hobbs, 2016; Potter, 2014; Silverblatt, 2008; Schmidt, 2012). Technologies such as Alexa, Google Nest, facial recognition phone technologies, and predictive algorithms are influencers of digital privacy and users' behavior online (Gerber, 2016; Kosinski, 2019; Lanier, 2013; Power, 2016). Specifically, Silverman (2015) explained that SNSs motivate users to share personal information under the pretense to connect people together and enhance the global community. Berkowitz (2014) added that SNSs' users "… are willing to open up [their] inner worlds… for the price of convenience (n.p)."

Individual users may think that what they share online will not harm them, or that they have nothing to hide anyway (Stein, 2016); however, anything shared on SNSs is stored permanently (boyd & Ellison; 2007; Collins, 2017; Lanier, 2013) and is used to create a virtual persona of individuals with their interests, political and religious beliefs, financial and health problems, and sexual orientations (Givens, 2015; Kosinski, 2017; Kosinski, Stillwell, & Graepel, 2013). Furthermore, data about users are used in

aggregate to make decisions that profile and categorize people in large groups and communities (Davidowitz, 2017; Gerber, 2018; O'Neil, 2016; Williamson, 2017).

Even if users do not share much about themselves, their profiles could still be combined through predictive algorithms, facial recognition software, and through their networks of friends (Kosinski, Stillwell, & Graepel, 2013). Data collected are used not only to optimize the tech services, but also to enhance marketing (Acquisti, 2004; Fuchs, 2012b; Turow, 2012; West, 2019) or citizens surveillance (Wang & Kosinski, 2018; Zuboff, 2019). The individual user is left with a necessary trade to make, that is personal data for social relationships, social capital, and entertainment.

Privacy is sensitive to technological development. Around the year of 2004, Web services have developed from a stage of 'read-only' known as Web 1.0 to 'read-write' known as Web 2.0 (Papathanassopoulos, 2015). Participation in the making of Web content and the mash-up of content (i.e., read-write) marked the line between the two Web generations. Similarly, privacy has shifted from privacy 1.0, where the government entities and a few companies controlled personal data collection and surveillance to privacy 2.0, where SNSs have enabled individuals to share, transfer, and disseminate personal information (Zittrain, 2008). Privacy 2.0 have eliminated information gatekeepers, increased surveillance, lowered digital intimacy, and blurred lines between private and public spaces (Child & Starcher, 2016; Papathanassopoulos, 2015; Wachter, 2018).

The privacy of individuals is fundamental to a moral and modern society (Nissenbaum, 2010). The main problem when discussing privacy 2.0 is the tech companies and service providers (e.g., Google, Amazon, Facebook), as they are the

biggest threat to people's privacy (Thompson, 2012). The companies' software design of their platforms make users behave a certain way, and encourage them to produce content in order to participate (Tsay-Vogel et al., 2018; Vraga, Bode, Smithson, & Troller-Renfree, 2016; Zuboff, 2015). Tech giants have shifted the process of intimate information from a necessary ingredient to establish social/human relationships to a business trade. This follows the logic of, "If you're not paying for the product, you are the product" (Silverman, 2015, p. 254). In a nutshell, Silverman (2015) asserted that today's media and entertainment technology, such as SNSs, are owned and fully controlled by an "… elite class of innovators [who] use our personal information however they choose and push us towards a set of standardized behaviors and values" (p. 19).

The other side of the problem is law, which mainly manifests itself through Terms of Service (ToS) or website privacy policies (Givens, 2015; Waldman, 2016). Privacy policies are written to benefit the companies and force the users to agree (Fuchs, 2014). Privacy policies are framed within the user self-responsibility (Papacharissi & Fernback, 2005). In other words, it is the responsibility of the user to make the necessary measures to protect their information. By agreeing to the Terms of Services, users are left with no choice but to forfeit many of their rights and responsibilities to data companies (Givens, 2015). In the midst of these policies and practices, the U.S. has not established a comprehensive federal law to regulate data and protect the individual citizen and regulate data collection practices (Solove & Schwartz, 2018).

The inadequacy of one's digital privacy practice could be linked to the lack of critical thinking and information literacy. "If we are to save privacy, the first step is

articulating what it is about privacy that makes it worth saving," argued Berkowitz (2014, n.p). Newell and Marabelli (2015) posited that SNSs users are not aware of how much data they produce by using various digital devices and services. Scarce research has been conducted within the realm of higher education to investigate digital privacy literacy (Magolis & Briggs, 2016; Schmidt, 2013). Digital privacy literacy scholarship is limited partly because it is a new literacy (Veghes, Orzan, Acatrinei, & Dugulan, 2012; Warzel, 2019; Wissinger, 2017); it is not well defined (Johnson & Hamby, 2015; Solove, 2003); and it is sensitive to social context (Nissenbaum, 2010). Moreover, online users have their share of responsibility, as they have given up their privacy protection and continue to rely on the settings and privacy protection strategies afforded by different service providers (Fuchs, 2012b; Marwick, 2012; Marwick & boyd, 2011; Obar, 2015).

Methodological Framework

Conducting research relevant to Web 2.0 technology requires comprehensiveness. The researcher needs to pull sources from scholarly work, as well as extend to other sources, in order to speak to technology research, a field that changes quickly. Additionally, it is important to follow clear methodological steps and remain transparent throughout the process for the sake of research replicability (Johnson & Christensen, 2014). Comprehensive literature review, as defined by Onwuegbuzie and Frels (2016, p. 19) is,

> … a culturally progressive approach involving the practice of documenting the process of inquiry in the current state of knowledge about a selected topic as related to philosophical assumptions/beliefs, inquiry (method), and guidelines of practice (organization, summarization, analysis, synthesis, reflection, and

> evaluation), resulting in a product that is a logical argument of an interpretation of relevant published and/or unpublished information on the selected topic from multi-modal texts and settings that primarily comprise five MODES (i.e., Media, Observation(s), Documents, Expert(s) in the field, and Secondary sources).

The current literature review study follows the CLR methodological framework advanced by Onwuegbuzie and Frels (2016). It comprises seven steps: (a) Step 1: Exploring Beliefs and Topics (b) Step 2: Initiating the Search, (c) Step 3: Storing and Organizing Information (d) Step 4: Selecting/Deselecting Information, (e) Step 5: Expanding the Search to MODES (Media, Observations, Documents, Expert, Secondary Data), (f) Step 6: Analyzing and Synthesizing Information, (g) Step 7: Presenting the Comprehensive Literature Review. For the sake of dissertation formatting, I will add (h) step 8: Discussion and Implication of the CLR for Privacy Literacy.

Step 1: Cultural Beliefs (topic selection), Goal of the Study, and Philosophical Stance, and Guiding Research Questions

Researcher cultural background and beliefs. If you take a Closed-Circuit Camera TV (CCTV), gather a neighborhood, and ask them if you could install a couple of them for security and to fight off crimes, you might find that some may welcome the idea, and others may feel the CCTVs are an intrusion of their privacy and would seek alternative ways, such as police patrolling. Privacy is sensitive to culture, and within the same culture, privacy is bound to people's preferences and life circumstances

I came from a small conservative town in the south of Algeria called El-Atteuf (founded in 1012)[1], classified as a UNESCO World Heritage Site. Privacy in my community is a rigid norm and adheres to hardcore community-set standards. Everybody would be furious if they felt that their privacy was breached. Phones and photography of people, especially females, in public places, streets, etc., is strictly prohibited. Privacy in El-Atteuf, my hometown, is a norm, a rewarded act. Majority of females stay or work from home, and their meticulous behavior, dressing fashion, and voice pitch are signs of privacy entitlement. This cultural dimension is completely different than what I experienced growing up, traveling the world, or even currently living in the U.S.

Conversely, living in a small community, like where I came from, can also make you feel that you have no privacy, as everybody knows your business and what is going on in your life. However, the means of access to others' businesses are mostly human-based, i.e., mouth-to-ear tradition. The same information is now available to us, maybe at a higher degree, through Facebook and other SNSs. Some SNSs' users put their house pictures, their bedrooms and showers, and snap pictures that show so much about their body and consider it a regular act of socialization. Other users may conceal any pictures about themselves, surf the net quietly, or hold a fake name and identity. This is probably a rare act today, as it is almost asocial not to hold an online social networking presence.

---

[1] A brief history of the city, the region, and people's need for withdrawal from hostilities for religious freedom, privacy, and culture preservation: http://whc.unesco.org/en/list/188/

This richness and these differences among people make it hard for people, scholars, and educators to agree on one definition of privacy.

Privacy, to me, is fundamental to 21st century life and should be a basic human right. It guards people's freedom and shields their belongings. Privacy is necessary, because people should feel free at expressing themselves and enjoying their life without a concern that their sayings, moves, and/or interactions are being recorded and stored permanently. We, human beings, lose spontaneity of behavior when we are under constant watch (Fuchs, 2012a; Marwick, 2012; Zuboff, 2015) . Moreover, using technology for work or entertainment should only enhance our life, increase the convenience, and work efficacy. It should not impact us negatively with a constant concern over losing our information to unintended audiences and entities. The citizen should have the opportunity to learn about privacy laws, institution data practices, and strategies to physically preserve the right to his/her data. Finally, regulation is needed to protect citizens, especially children and elders, from pervasive data profiling and targeted advertisement.

In my experience attending trainings on privacy, speaking at conferences, and interacting with students from different American universities and from other universities abroad, the question I often receive is one: How can we not lose our data, and have more control over what we share and say online? I sense a sentiment of fear and "freaking-out" whenever I speak to students about different data practices.

The question of self-protection has always intrigued me. When asked about privacy protection, I try to provide tips, but also crowdsource multiple perspectives and experiences from the audience. I then ask the students to reflect on different online

experiences and note statements/conditions related to data collection, website structure, navigation path, and what could not be controlled, except by the service provider. Each time I do this, I notice an improvement in students' reflection on their Web-usage and an increase their consciousness about privacy.

Departing from such conversations, I strongly believe that the individual-responsibility for privacy is unfair, and cannot work. I equally believe that responsibility should shift to data companies and institutions. My beliefs stem from the premise that the citizen, as a user of various digital platforms, should not be the last decisional player in the entire digital privacy manufacturing process. Users of digital platforms, and social networking sites in particular, have no power but to abide by the rules of the service provider and, at a deeper layer, by the software design and structure (see also Lynch, 2016). Therefore, I stand on the belief side of the continuum that software governs and influences behavior, to a great extent (Frabetti, 2015; Gerber, & Lynch, 2017; Kitchin & Dodge, 2011; Lynch & Gerber, 2018; Manovich, 2013; Williamson, 2015, 2017). Software is hidden and is usually an intimidating part of knowledge for many people (Kitchin & Dodge, 2011; Lynch, 2017; Williamson, 2015). In an analogy, I view the matter as the problem of carbon monoxide emissions in the air. The individual drivers could absolutely do their best to reduce their carbon output by servicing their cars on time, driving less, or carpooling more, but more impact will be realized by a combination of efforts between oil companies and car making companies than any singular citizen effort.

Goal of The Study

Newman, Ridenour, Newman, and Demarco's (2003) conceptualized that research studies fall within nine types of goals: (a) predict; (b) add to the foundational knowledge; (c) impact change at the personal, social, institutional and/or organizational level; (d) assess and measure change; (e) understand complex phenomena; (f) test a new theory; (g) generate new ideas; (h) inform constituencies e.g., researchers and groups of interest; and (g) review research. Of these nine types of goals, the goal of this study is twofold: to review research on privacy literacy and to inform researchers, and educators about the scope of privacy literacy skill; its relationship to other disciplines; and what it takes to become a privacy literate individual from the perspective of law, technology, and education. Moreover, I aim at mapping the components of privacy literacy skill from a three-layer perspective: scholarly literature, expert(s) opinion, and public opinion.

Understanding how privacy, as a concept, is embedded in technological services and how personal data are handled is an important prerequisite for a peaceful and democratic society. Big data and citizen profiling could have discriminatory consequences (see also O'Neil, 2016). Hidden software design (i.e., the written code) could contain structures and formulas to isolate certain people or target others (Frabetti, 2015; Lynch, 2017; Williamson, 2017). If citizens can inform themselves, know their basic rights, such as the privacy regulation of data about them, they can live in a society they actively shape: a society that is built on fairness and informed decision.

Philosophical Paradigm

The current study aligns itself with Dialectical Pluralism (DP) 2.0 philosophical research paradigm (Johnson, 2011, 2012, 2017), which I will refer to as DP. The core

principles of this paradigm are appealing to the nature of the topic of privacy literacy in its complexity and multiplicious research approaches.

Ontology. Ontology is concerned with the reality ("to be" or "not to be" question) of knowledge (Lincoln, Lynham, & Guba, 2011). Dialectical Pluralism's ontology "… is committed to the idea that there are many important realities that might need consideration at any point in time" (Johnson, 2017, p. 164). As relevant to privacy literacy, there is some truth to digital privacy as governed by software which operates under exact codes and rules, but its practice is bound to a specific context. Hence, the reality about digital privacy literacy builds upon our experiences as humans (e.g., self-disclosure dynamics) together with the experience of the technology devices themselves (e.g., software behavior, glitches). For these reasons, researching privacy literacy requires one to consider different realities, contexts, while maintaining the core thought about the human-machine relationship. The ontology of privacy dealing with the digital is complicated, but can be unpacked. Lynch and Gerber's (2018) ontological imperative framework allows individuals to unpack what it means to be digital and to thoroughly question the nature of what is and is not made available within digital platforms and digital research, thereby allowing a layer of discussion on matters of privacy literacy.

Epistemology. Epistemology is concerned with what it means to know (Lincoln, et al., 2011). Dialectical Pluralism 2.0 epistemology means ". . . users of DP acknowledge the fallibility of knowledge, have the goal of producing somewhat heterogeneous and somewhat homogeneous wholes that respect multiple standpoints, and place weight on solutions that work in theory and contextualized practice" (Johnson, 2017, p. 164). The current research does not focus on one particular standpoint to

investigate privacy literacy. It uses a combination of emic and etic approaches (Greene, 2007; Johnson, 2011; Onwuegbuzie & Frels, 2013; Onwuegbuzie, Johnson, & Collins, 2009) through literature, anecdotal observations, interviews of experts, and Social networking sites data (i.e., MODES from Onwuegbuzie & Frels, 2016). The sources investigated to conduct this research are multidisciplinary and are pulled from the fields of law, information science, psychology, sociology, marketing, and education.

Under this paradigm, truth is contextual and is shaped by meaning exchange and experience. With this in mind, the current research is inspired by the principles of Fallibilism (Peirce, 1893). Peirce posited that "… our knowledge is never absolute but always swims, as it were, in a continuum of uncertainty and of indeterminacy… [and that] the universe is *not* a mere mechanical result of the operation of blind law. The most obvious of all its characters cannot be so explained (n.p)."

Privacy literacy has a multitude of definitions, but scholars have not reached a consensus about what it really is (Johnson & Hamby, 2015). Solove (2006) argued that privacy, as a concept, is widely discussed, but ". . . nobody can articulate what it means" (p. 477). Fallibilism is inherent in privacy literacy research, since privacy is a complex concept, practice, and has complex consequences. To this end, methodology should be inclusive of many different approaches and from different standpoints.

Despite its complexity, digital privacy literacy, as a skill, could be measured (e.g., Trepte, et al., 2015). Similarly, digital privacy as a concept or a legal right can be measured through the assessment of the security protocol in place and data breaches (e.g., Cambridge Analytica was an assessment of the Facebook's data security system). In this research, privacy literacy is investigated in three interactive and inter-communicative

layers: the scholarly work, the expert opinion, and social/public opinion through SNSs' metadata (i.e., Facebook). These three layers require multiple ways of analysis in order to build solid knowledge and contribute to the field.

Axiology. Axiology is concerned with what it means to value, or the ethics systems undergirding a philosophical stance (Lincoln, et al., 2011). Dialectical Pluralism 2.0 axiology states that "Researchers should state their explicit values, make their implicit values explicit, respectfully and emphatically discuss the relevant values, and put together an apt and agreeable 'package of values' that serves multiple important groups and perspectives for each project" (Johnson, 2017, p. 166). The overall goal of this research is to describe/operationalize privacy literacy in connection with other disciplines, and articulate what it means to be a privacy literate citizen. It is to give voice to the user of social networking sites (SNSs) and data consumers to better manage their data.

Today's online users are constantly illiterate about their personal data and information (Fuchs, 2012a; Marwick, 2012; Marwick & boyd, 2011; Obar, 2015). Technology and data revolve around the user. Behavioral profiling and data processing are driven by how individuals use/consume technological services. As an end value of this research, I am guided by key social and practical values (Johnson, 2017), such as openness, justice to technology consumers/users, and fidelity to the process of building knowledge and argument in addition to trustworthiness, courage, and respect for multiple perspectives.

Methodology. Methodology is concerned with the process of how we seek out information or new knowledge (Lincoln, et al., 2011). Dialectical Pluralism 2.0

methodology posits that “Researchers and stakeholders should dialectically listen and consider multiple methodological concepts, issues, inquiry logics, and particular research methods and construct the appropriate mix for each research study” (Johnson, 2017, p. 167). The current research will examine the history of privacy literacy through seminal theories and works as well as current updates from field experts. This convergence is meant to guide the research and construct a defined picture of the subject matter. The methodological philosophy followed in this research is an interpretation of believing in the complexity of the topic and its multifaceted nature that leads to other disciplines. Following this logic, I will engage in a comprehensive literature review (CLR), which includes both a systematic review of the literature and extension to the MODES (Onwuegbuzie & Frels, 2016). I will use different methods of data collection (systematic review and MODES) and analysis such as frequency analysis, thematic analysis, and keywords-in-context (KWIC). Figure 1 shows how privacy literacy maps into the philosophical paradigm.

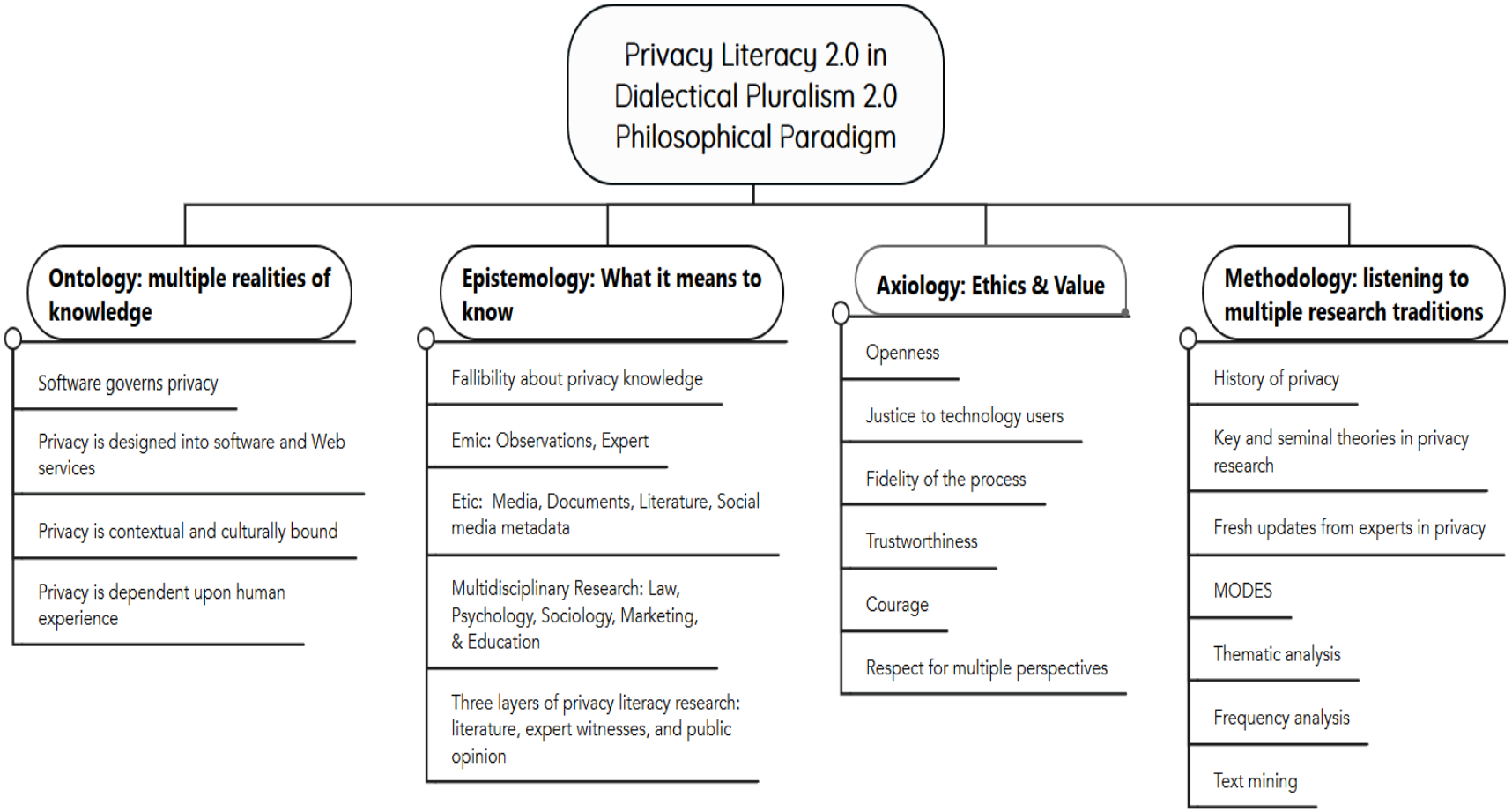


Figure 1. *Mapping of privacy literacy 2.0 into my philosophical paradigm*

Theoretical Framework

Rachel James (1975) argued that the biggest injustice is watching someone who believes he/she is alone. Just like privacy literacy is a concept/practice, theories about digital privacy are conflicting. Under those circumstances, a combination of theories might cover the concept of privacy as a fundamental right. Alfino and Mayes (2003) argued that most privacy theories fall under two broad categories: theories that safeguard access to the person (e.g., Warren & Brandeis 1890); and theories that preserve the right to privacy through controlling access to his/her personal information (e.g., Fried, 1968). Within the second category, I will add a social/public perspective in order to situate today's mass surveillance. As a result, the current study's theoretical framework is a mix of theories and is presented as follows: Access to the person, as in to physically interact and collect information form someone; and access to the person's personal information/affairs, as in digital access, remote surveillance, and ability to control access to information.

Access to the Person

Warren and Brandeis' (1890) work was inspired by the development of technology (Photo cameras), means of mass media and communication (Newspapers), and illegal circulation of persons' information and portraits. The authors were concerned that "… instantaneous photographs and newspaper enterprise [that] have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops" (p. 195). For Warren and Brandeis, the right to privacy was confined to physical intrusion to the person's otherwise private and domestic-self or environment. The same theory posited that only the person, holder of the right to privacy, can allow

access to his/her thoughts, sentiments, and emotions. No one, by any means of press, photography, or recording devices could obtain information about the person, publish, or reproduce them.

Consent is a prerequisite to the application of this theory. No one, other than the person in question, can allow access to themselves. The right to privacy is automatically lost once the person in question releases information, sentiments, or thoughts to the public. The right to be let alone is partially connected to the theory of social privacy protection. Warren and Brandeis (1890) posited that ". . . the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression" (p. 206). Warren and Brandeis' theory focused on physical encounter and property access, and the right to privacy was exclusively accorded to the person when physically present in various life situations.

Access to the Person's Personal Information

One of the seminal works in the field of privacy theory that dissected the privacy and its relation to ourselves, social structures, and the governmental institutions is that advanced by law scholar Charles Fried (1968). Fried was among the first to question the role that modern technologies play in the ecology of privacy, and how they can affect individuals' liberties. He wrote, "There are available today electronic devices to be worn on one's person which emit signals permitting one's exact location to be determined by a monitor some distance away" (p. 475). Fried predicted that the advancement of technology, in what he called 'not too distant future,' will change privacy and be able to scrutinize one's diseases, such as diabetics or blood pressure, and even know one's

patterns of his/her brain or thinking. Although these devices were essentially developed to monitor prisoners in and outside prisons, Fried (1968) posited that they might be used to monitor the grand public.

Monitoring means it is discrete and unknown to the person. Concern over the collected information falling in the wrong hands was an important trait explained by Fried in his theory of privacy. He posited that surveillance disturbs social life and means ". . . the opportunity presented for harassment, the inevitable involvement of persons as to whom no basis for supervision exists, the use of the material monitored by the government for unauthorized purposes, the danger to political expression and association, and so on" (p. 477). The most important part of Fried's theory is the fact that he considered privacy as a nest and a determining factor of respect, love, friendship and trust. As fundamental as these traits are to our lives, Fried argued that the four human principles are inconceivable without privacy.

Therefore, threats to privacy are direct threats to a person's life. Because privacy is a necessary component of self-respect, respect for others, love, friendship, and trust in others and institutions, it should allow people to have power not on how much others know about them, but to control access to information about themselves. Fried (1968) stated that privacy means "… control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well" (p 483). To illustrate, people might know someone is traveling to a particular country, but the traveler should have the power to control information related to who they met during the trip, and what items they shopped and brought back home. Privacy is fundamental to human relationships (i.e., inter-personal) and to intra-personal

development as in self-respect. Citizens should not be scrutinized or monitored discretely and be convinced to believe that it is a necessary trade for safety and liberty (Fried, 1968).

Privacy, as theorized by Fried, is a moral capital that people spend to nurture relationships of love, friendship, and trust. The moral capital is intangible, discrete, mutual, highly sensitive to context and social circumstances. Losing control over who can access information about us, to subtle surveillance, and to unintended audiences threatens personal privacy and the fundamental principles of life: love, friendship, and trust. "There is always an unseen audience, which is more threatening because of the possibility that one may forget about it and let down his guard, as one would not with a visible audience" (Fried, 1968, p. 490).

To summarize, privacy is more than a single right or law. It is multifaceted and is related to the fundamentals of living as humans in a community. Self-respect and intimacy are human qualities upon which life, in its entirety, is built. Self-respect and intimacy, in addition to love, friendship, and trust feed essentially from privacy. Privacy as theorized here is that which allows individuals ". . . not just an absence of information abroad about ourselves; [but] a feeling of security [and] control over that information" (Fried, 1968, p. 493).

Research Questions

The following research questions will guide this study. They are designed to examine privacy literacy from multiple angles and within multiple disciplines, such as law and education:

1) How does the Comprehensive Literature Review process inform and develop a definition and understanding of privacy literacy mainly on SNSs:
    a. Through existing literature/scholarly work?
    b. Through select expert opinion?
    c. Through select publicly available social networking sites data?
    d. Through law and current legislation?

Significance of the Study

The public seems to struggle with privacy protection (Ewbank, 2016; Gopal, et al., 2018; Kyei-Blankson, et al., 2016). Research has shown that the millennials, including digital natives, have trouble understanding how much data they release and how data are processed and used by companies (Fuchs, 2012a; Marwick, 2012, Marwick & boyd, 2011; Obar, 2015). Privacy literacy, according to Trepte et al., (2015) could help secure participants' data and enhance their digital participation. Mackey and Jacobson (2011) posited that privacy literacy is a survival skill that develops hand-in-hand with technology; it enables individuals to take control over their usage habits; and it mitigates risks associated with personal data loss.

In order for us, as educators, to be able to design practical solutions such as curriculum, information sessions or seminars, and spread knowledge to the public, it is important to map digital privacy literacy within the new media ecology. According to Postman (1970), media ecology theory examines media as an environment. Postman posited that environments control what we can see and force us to behave in specific ways. In a similar fashion, media environments like books, television, and radio implicitly influence people. Studying media as an ecology is to expose the implicit

influences and render communications that happen between the individual and the media explicit.

New media ecology is driven by the Internet and software engineering. It encompasses artificial intelligence (AI), SNSs, fast information supply through mega search engines, such as Google and Bing. The software environment (e.g., SNSs) dictates the way(s) in which individuals can use technology. As individuals use various technologies, data are generated. Through big data analysis, new media ecology examines the interaction between technology infrastructure, information companies (e.g., Google and Microsoft), the government (e.g., information laws and regulations), and citizens use of technological devices (Quinn, 2014; Scolari, 2012; Shin & Choi, 2015).

In my research, I aim to use existing scholarly work, empirical studies, and meta-analyses to construct a comprehensive image, definition, and understanding of privacy literacy. Moreover, the study will include current updates from experts via expert interviews, and closely listen to public opinion through SNSs data procured through application programming interface keys (API keys) that allow access to back-end metadata and front-end SNSs feeds (see also Gerber & Lynch, 2017). Hopefully, this CLR will contribute to further studies through its findings about privacy literacy; enhance the conceptualization of privacy; and showcase an innovative process of conducting CLRs by incorporating multiple voices and stand-points.

Pragmatism, as an overarching philosophical paradigm, does not mandate the researcher to follow a set of methods for data analysis (Johnson & Onwuegbuzie, 2004). I was flexible in remixing multiple methods in online spaces within each major tradition of research: qualitative and quantitative (Gerber, Abrams, Curwood, & Magnifico, 2017).

"When applied to discussions of research methods, remix offers flexibility, but it also requires the researcher to constantly negotiate and rationalize methodological and paradigmatic choices." (Gerber, et al., 2017, p. 15). Because reality cannot be known in its entirety and, from a dialectical pluralist stance, remixing the methods for data analysis was a decision I made based on the time allotted to the study and work efficacy.

Definition of Terms

Privacy Literacy. Trepte, et al., (2015) defined privacy literacy as:

> . . . a combination of factual or declarative ('knowing that') and procedural ('knowing how') knowledge about online privacy. In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection, and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection. (p. 339)

Software. Software is a system or a mechanism that is coded/programmed to be automatic and instantaneous. Software has a structure, rules of operation and execution, an ideology, and an objective (Lynch &Gerber, 2018).

New Media Ecology. Media ecology studies media as an environment (Postman, 1970). New media ecology is driven by the Internet and software engineering. New media ecology encompasses artificial intelligence, social networking sites, and fast supply of information through Google, YouTube, etc.

Artificial Intelligence. Artificial intelligence is a set of code and algorithms put together to simulate human intelligence in machine. Artificial intelligence enables machines to operate smartly and independently, like humans.

Algorithms. A mathematical formula that is inserted in a computer for a multitude of functions such as profiling, data processing, content management, facial recognition, etc., (O'Neil, 2017). Algorithms enable computers and machines to operate, learn, unlearn, and relearn for themselves and operate off of "if" "then" scenarios.

Big Data. Big data are data that are too big for a human brain to process. Big data are generated from the ". . . widespread diffusion of digital devices that have the ability to monitor our everyday lives" (Newell & Marabelli, 2015, p. 3).

Self-Disclosure. Self-disclosure is a ". . . communication phenomenon; it is the act of telling" (Millham & Atkin, 2018, p, 53). Self-disclosure is the release of private information about the self to a determined audience (Petronio, 2002).

Social Networking Sites (SNSs). Social networking sites, such as Facebook and YouTube, constitute ". . . a group of internet-based applications that are built on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content" (Kaplan & Haenlein, 2010, p. 61).

Networked Privacy. Marwick and boyd (2014) advanced the concept of networked privacy as an ongoing process of negotiating the information and content accessibility, as well as, collectively working on protecting data and information.

Delimitations

The CLR will primarily include peer-reviewed articles and extend to the MODES (Onwuegbuzie & Frels, 2016). The peer-reviewed articles were selected from different

research traditions (i.e., qualitative, quantitative, and mixed methods) and published peer-reviewed articles from 2013 to 2019. Additionally, the selection of articles to include in the CLR followed a set of selection and deselection criteria, as mentioned in Chapter III. I extended the search to include the MODES (Onwuegbuzie & Frels, 2016). For media, I selected works from YouTube, Amazon Prime Video, and Netflix. For observations, I used my own reflective notes from the classes I co-taught at the university. Documents included books, dissertations, conference proceedings, unpublished works, essays, blogs, and government reports. Experts interviewed in this CLR were educational researchers, privacy researchers, and law specialists. Secondary data focused on analyzing Facebook comments of Facebook users who interacted with Mark Zuckerberg's testimony before the senate in April 2018. Data was procured using Facepager API, a program built by Till Keyling[2] from the University of Munich, Germany. Facepager uses the Facebook API to be pull user data (from publicly available discussions and forums).

Limitations

The CLR was narrowed to privacy literacy in higher education. This resulted in limited applicability of the findings. Therefore, broad generalizations of the answers to the research questions is inappropriate. Additionally, as a synthesis of articles and MODES and according to Onwuegbuzie and Frels (2016), the CLR is further limited by the inherent characteristics of meta-synthesis and meta-analysis. Namely, the syntheses

[2] Read about Facepager here https://www.alumniportal-deutschland.org/en/science-research/news-from-science/facepager-till-keyling-social-media/

are interpretive, and they require coding and analysis which are systematic but subjective. The selection and deselection criteria as well as the research keywords were created by the researcher. Hence, the scope of this CLR was determined by the researcher; therefore, it is not complete. Decisions to include or exclude literature and MODES were made by the researcher. Although selection and deselection was systematic and transparent, it still remains subjective. Consequently, the research findings are vulnerable to heightened researcher-bias in their determination and their application.

Additionally, I used QDA Miner Lite to code the selected articles, which is a version with limited functionalities compared to the commercial version QDA Miner Lite. In addition to software coding, I manually mapped and coded the selected articles. Coding and mapping the articles was replete with my choices, decisions; therefore, the process was open to bias and subjectivity. Miles, Huberman, and Saldaña (2014) stated that, "The researcher's decisions – which data chunks to code and which to pull out, which category labels best summarize a number of chunks, which evolving story to tell – *are all analytic choices* (emphasis in the original)" (Miles et al., 2014, p. 12).

These limitations and delimitations along with other threats to internal and external credibility, as discussed by Onwuegbuzie and Leech (2007), may have had an influence on the findings' dependability, reliability, and truth. Of specific concern to this study was my experience, culturally and professionally, with privacy, which may have reduced legitimation and increase researcher and confirmation biases. Threats such as observational bias and reactivity were inherent in the process of selecting the literature and media work. The external threats to credibility, interpretive validity, and generalizability are possible, and with this work, I intend not to generalize; however, the

threats may also stem from my personal experience with privacy, my readings, and teaching experience.

Chapter Summary

In this chapter, I have described my cultural beliefs, goal of the study, the philosophical stance, and guiding research questions (Step 1). Additionally, I provided a detailed description about my philosophical stance in four components: ontology, epistemology, axiology, and methodology. I also stated the goal and significance of the study and what limitations and delimitations the reader needs to bear in mind while reading this work.

In the following chapter, I present an overview of the study and situate privacy within the field of literacy, law, and software engineering. The rationale for the overview is to show the links that exist between literacy, as in reading and writing, and other literacies, such as digital, informational, and media. I then present privacy literacy 2.0 as a new literacy and introduce its linkages to current Web 2.0 technologies and new media. Lastly, I present privacy literacy in relation to law (federal and international) as well as explain how software or technology drive change in social society.

CHAPTER II

Literature Overview

Chapter Overview

This chapter lays the foundation and expands the first step mentioned in the introduction: Step 1 (exploring researcher's beliefs and topics). Chapter Two stands as a stepping stone into the rest of the Comprehensive Literature Review (CLR) with its steps: Initiating the Search (Step 2), Storing and Organizing Information (Step 3), Selecting/Deselecting Information (Step 4), Expanding the Search to Media, Observation, Documents, Expert, and Secondary Data (Step 5), Analyzing and Synthesizing Information (Step 6), Writing the Report (Step7), and Discussing the Findings and Implications (Step 8).

This chapter presents an overview of the literature regarding privacy literacy 2.0 as a new literacy that is related to traditional, digital, media, and information literacies, also combined as multiliteracies (The New London Group, 1996) or metaliteracy (Mackey & Jacobson, 2011). In this chapter I focus on showing how digital data are generated and processed for various reasons, mainly for surveillance and marketing. I highlight the fact that personal information could easily be compromised, and underline the participatory/networked privacy as a way to enhance personal data protection. I show the role software engineering plays in influencing users' online behavior, as well as drive law and legislation. A summary will conclude this chapter.

Literature Overview

Social Networking Sites (SNSs) and Privacy

Digital communication technologies are on the rise. With over 3.3 billion active SNSs users (Kemp, 2019; Mohsin, 2019), with a new SNSs account opening every ten seconds and over 50 billion text messages sent through Facebook Messenger and WhatsApp daily (Smith, 2019). Social networking sites (SNSs) are changing the way people communicate and share information with one another (Child & Starcher, 2016; DeNardis & Hackl, 2015; Jordaan & Van Heerden, 2017; Marwick & boyd, 2011; Quinn, 2016; Tsay-Vogel, Shanahan, & Signorielli, 2018). The average person spends at least 116 minutes on a daily basis to manage approximately five SNSs accounts (Smith, 2019). Sharing is at the heart of SNSs presence.

Social networking sites, as defined by Kaplan and Haenlein (2010), constitute, "A group of internet-based applications that are built on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content" (p. 61). Of particular interest, SNSs' interactions amongst users, including the way that users move across the spaces are tracked and stored in data banks through back-end user metadata (O'Neil, 2016). Given that SNSs are operating for commercial ends, their chief goal is to capitalize on advertising, which often includes selling personal user data that map behavioral trends of the users (Fuchs, 2012b). The black box of the dynamics of metadata are only understood by a minority (Berry, 2011; Baruh & Popescu, 2017; Everson, 2017; Lynch & Gerber, 2018; Manovich, 2013; De Montjoye, Radaelli, Singh, & Pentland, 2015). I asked Ian O'Byrne, an educational technology researcher and privacy scholar about the black box and he responded, "We do not understand what the

algorithms are doing with our data. We do not understand what the algorithms are doing either… you know, your data and your identity are being slurped up 24/7" (I. O'Byrne, personal communication, February 12, 2020).

Many SNSs users believe their click/commenting behavior or conversations (e.g., in public or private) are immune to advertising companies and government watch (Bedi, 2013). boyd (2012) elaborated that,

Most people are unaware that their data is aggregated with others to construct portraits of individuals that predict their interests based on others' habits. Our interpreted selves aren't simply the product of our own actions and tastes; they're constructed by [deciphering] similar patterns across millions of people. (pp. 348-349)

Although many people consider SNSs as an important means for relationship maintenance or entertainment, the usage of SNSs carries a risk of losing private information to an unwanted audience, privacy breaches, account hacking, lurkers, hate speech, etc., (Armerding, 2018).

Concern for loss of privacy or exposing private user data to criminals, to unintended audience, or even to third-party companies, is a common phenomenon among SNSs'—known as privacy concern (Child & Starcher, 2016; Dienlin & Trepte, 2015; Proudfoot, Wilson, Valacich, & Byrd, 2018; Trepte, Teutsch, Masur, Eicher, Fischer, Hennhöfer, et al., 2015). A survey conducted by Rad Campaign found that 61% of SNSs users have trouble trusting social networking sites (King, 2018). Among the main reasons that are keeping the users away from SNSs are issues related to privacy. Additionally, of the 713 individuals who were surveyed by Rad Campaign, 47% of those who use Facebook claimed they share less of their personal life with their friends via

Facebook; however, 87% stated that despite the privacy issues, they continue to use SNSs (King, 2018).

Despite concerns over privacy, Internet users continue to use SNSs. For instance, in the wake of the Cambridge Analytica[3] scandal that hit the Facebook bank of data, Ipsos conducted a survey and discovered that nearly 50% of Facebookers in the U.S. did not change their surfing habits. The tech giant, Facebook, published its earnings report of the first quarter of 2018 and identified no signs of users or advertisers' lack of Facebook usage (Kats, 2018). Furthermore, research of Internet usage trends indicates that 83.5% of Internet users aged (12-17); 90.5% of those aged (18-24); and 81.1% of those aged (25-34) will still be using Facebook by 2020 (eMarketer & Squarespace, 2019).

However, people's increasing usage of SNSs, despite the privacy breaches aforementioned, indicates that there may be some tangible benefits that make Americans concede to allowing personal data collection in return for using SNSs. The phenomenon of releasing personal data in return for any benefits is known as data auction or bargain. Rainie and Duggan (2016) explained the concept of data bargain as when a customer receives a free service or occasional discounts for allowing a commercial company to track their purchases, interests, and online clicking behavior, known as clickstream data. Social networking sites companies follow the same business model of data auctioning or data bargaining, where users can communicate, share, and maintain relationships in

---

[3] Cambridge Analytica was a breach of more than 50 million Facebook users' personal data for the sake of analyzing behavioral trends and tendencies. More details here https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

return for the tracking of their data. In return, their behavioral cues and digital footprints are used for marketing purposes and to generate profit.

Self-disclosure, data, and digital surveillance. The giant tech companies such as Google, Amazon, and Facebook handle users' data in a way that instigates convergent views among Americans. Rainie and Duggan (2016) used the phrase 'it depends' to frame the American citizen's view of SNSs privacy. Digital privacy is not a one-click button or a setting, and safety is guaranteed. It is a negotiation of multiple factors such as, data amount, data use and purpose of collection, and who has access to data. As an example of the 'it depends' privacy mindset, 44% of Americans feel their online personal information is somewhat secure, and 17% feel their data are very secure (Statista, 2017a). In contrast, a Pew survey (Madden & Rainie, 2015) stated that 76% of Americans do not trust that data that are collected about them by advertisers will remain secure and private; additionally, 69% of respondents felt SNSs data are insecure.

Mass surveillance is another activity that motivates data collection. In that regard, 81% of Americans admit that government surveillance is hard to avoid (Madden & Rainie, 2015). Government surveillance not only involves emails and phone calls, but it also involves aggregated data from commercial entities— that is from for-profit companies' banks of data. For example, the U.S. leads the rest of the world regarding law enforcement requests[4] of data release sent to Google with 74, 286 users/accounts

[4] Under FISA (Foreign Intelligence Surveillance Act, 1978), the government of the United States can send court orders to tech companies such as, Google and Facebook, to release data about foreign users.

requested[5] in the first half of the year 2019 (Google, 2019)[6], as compared to Russia or India with 259 and 19, 665 requests respectively. The U.S. government sent 42,466 data release requests to Facebook in the first half of the year 2018 compared to 16,580 sent, for instance, by India which ranks second in requesting data on its citizens. Despite the U.S. being the third largest world population after China and India, it remains the first country by large in digital surveillance requests sent to Google and Facebook, two of the world's largest information companies.

In the case of the U.S., the requests[7] could be related to national security or foreign surveillance. The requests need to be processed legally under (a) search warrant, (b) subpoena (c) Title III that requires the release of on-time information related to someone committing a crime or is related to a crime communication, (d) tracing information such as IP addresses release, and (e) a court order that requires Facebook data. Table 3 shows the types of requests Facebook received from the U.S. government from January to July 2019.

---

[5] When it comes to the United States, digital data requests include subpoenas, search warrants, court orders, and other legal orders, and are protected by law and colloquially known as gag orders.

[6] Google transparency report is accessed here https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period

[7] The Facebook transparency report is accessible here https://transparency.facebook.com/government-data-requests/country/US

Table 3. *Data requests from the U.S. government to Facebook*

Request	**Number**
Search warrants on Facebook users/accounts	46, 088
Subpoena	17,816
Title III user/account	389
Court orders on different matters	3,968
Tracing of accounts	9,361

Foreign Intelligence Surveillance Act (FISA) orders are relevant to the U.S. surveillance of foreign agents in the U.S. or overseas. In the period from July to December 2018, The Federal Bureau of Investigation and the National Security Agency have sent 83, 500 account request to Facebook.

Regarding online behavior, 33% of Americans say they consistently work on concealing their online movements (Statista 2017a). Interestingly, only 9% of Americans say they have enough control over their online data (Madden & Rainie, 2015). Companies of information processing, such as Google and Facebook, use data and advertising as their main currency. It is meant by information processing as in either storing user data and pre-packaging them for sale, marketing, or behavioral analysis and profiling. Information processing can also mean engineering software and hardware to enable access to information with speed and accuracy.

Exchanging data among tech companies keeps them up and running. In a survey by Morning Consult (2018), 78% of U.S. Internet users felt uncomfortable with commercial companies' ability to purchase their personal data for adverting ends. Statista

(2017a) reported that about 92% of American fall in the range from medium to highly concerned about the security of their data on SNSs. Although the majority of survey respondents (N= 92%) expressed concern about data security, 22% of U.S. Internet users said they managed to conceal themselves online (Morning Consult, 2018).

Mass surveillance and massive data collection of citizens' moves online create a concern for privacy. Privacy concern weighs heavy on citizens, especially with the increase in the number of data breaches: from 157 million incident in 2005 to 781 million breach incident in 2015 (Information is Beautiful & Thomson Reuters, 2019). To illustrate, the case of Cambridge Analytica alone caused more than 70 million accounts to be compromised (Worldwide, 2017). In August 2016, Yahoo revealed information about a breach incident that originally happened in 2014. The incident compromised more than 500 million users' emails and passwords. A few months later, the company uncovered another breach of 1 billion records which dated back to 2013. Following this breach, Yahoo stated that it affected another 3 billion connected accounts to mark one of the largest breaches in modern history (Information is Beautiful & Thomson Reuters, 2019).

I prefer to share my life on Facebook. Sprout Social (2017) surveyed 1, 220 American Internet users about what SNS they used to share information about their life and 94% chose Facebook. When asked about the type of content shared on SNSs, the participants stated that they mainly share their holiday news (66%), vacation and travels (60%), family (59%), and relationship (58%). When compared to the global population of Internet users, Americans seem a no exception. At a global scale, 87% of SNSs users share photos and videos of travel; 70% share videos of their children; 54% share private

and sensitive photos and videos of themselves; and 45% share sensitive videos and photos of others (Worldwide, 2017).

Regarding the reasons for which Americans share content on SNSs, 54% of participants in the survey (Sprout Social, 2017) said it was to invite their network of friends and followers to celebrate; 43% to inform their network about different things; whereas 17% indicated it was to seek social standing. Statista (2017b) investigated the tangible reasons for using Facebook and found that 79% of Facebook users in the U.S. have received advice on things to use or try; 67% purchased things cheaper than they found in stores; 69% made new friends; and, 40% made a work opportunity connection. When asked about the negative experiences on SNSs, issues related to privacy characterized the users' complaints. For example, 56% complained of having an unintended audience checking their posted pictures and links, either constantly or frequently (Statista, 2017b). Protecting one's data and information shared from unintended audience requires privacy literacy and skill.

Digital privacy and safety. Safety is human and it is one of the fundamental needs of human existence (Maslow & Mittelmann, 1941). Definitions of safety have underlined the notion of being responsible, i.e., in charge or in control. Maurice, Lavoie, Laflamme, Svanström, Romer & Anderson (2001), for instance, associated the meaning of safety with control and defined it as, "… a state in which hazards and conditions leading to physical, psychological or material harm are controlled in order to preserve the health and well-being of individuals and the community" (p. 238). Privacy concern, thus, is not a new concept nor is it associated with the advent of the technological means of communication. Privacy concern is a construct used in privacy literature to depict the

state of worry over individual's disclosure or sharing of self-information that may reach unintended audience—be seen by select known or unknown people (Belanger & Crossler, 2011; Osatuyi, 2014; Smith, Milberg, & Burke, 1996; Westin, 1967).

When it comes to privacy literacy and privacy concern, scarce research has been conducted within the realm of higher education, especially using qualitative methods (Magolis & Briggs, 2016). Schmidt (2013) claimed that current research on media literacy, including privacy literacy, is heavily focused on curriculum and program evaluation of K-12 education. Schmidt added that there is scarce media literacy research in secondary or higher education. In the same line of argument, Potter (2014) posited that, "We have reached a point where privacy may be the most important media literacy issue because of the very low level of public awareness about this problem coupled with the risks we all take when we are aware of these serious threats" (p, 238). Potter (2014) emphasized the fact that if the individual lacks knowledge about privacy, it may lead to so much loss of private information which may lead to identity loss.

Privacy Literacy

The concept of privacy, as known in today's literature, originated from Warren and Brandeis (1890) definition of privacy as ". . . the right to be let alone" (p, 193). Warren and Brandeis wrote about privacy from the standpoint of law when photography started to invade people's personal spaces. About a century later Burgoon (1982) worked on the dimensions of online privacy behaviors and classified them into informational, social, and psychological. In his model, Burgoon considered the informational dimension as the amount of identifying information people share about themselves. Social privacy captures the amount of people who can have access to the shared information about the

self (e.g., our online friends in today's social networking sites terminology). The psychological privacy dimension discussed by Burgoon (1982) refers to the degree of intimacy of information. Figure 2 below depicts the Burgoon's conceptualization of online privacy.

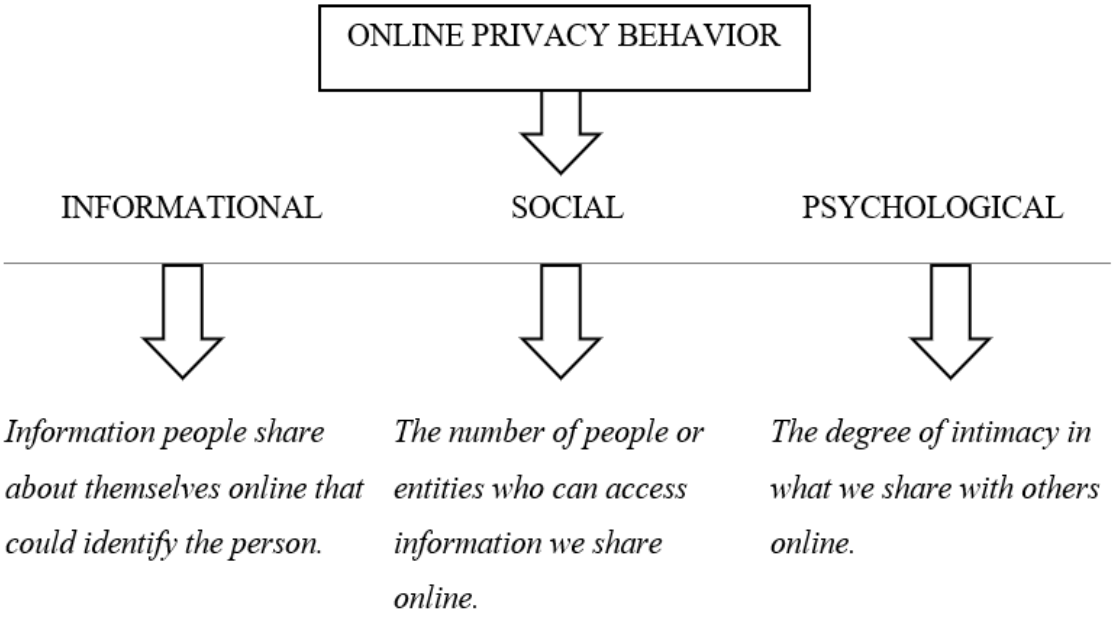


Figure 2. *Burgoon's (1982) model of online privacy behavior*

Burgoon's model was advanced before the invention of SNSs and the rise of the sharing culture; however, this model stands as a background to understand the privacy moves of people today. Researchers have tried to theorize privacy literacy based on previous definitions of privacy and advancement in technology. It is important to bear in mind that privacy, as a concept, may be steady, but its manifestations and practices are subject to frequent changes in parallel with technology innovation. Debatin (2011) posited that privacy literacy "... encompasses an informed concern for . . . privacy and effective strategies to protect it" (p. 51). For Debatin, to be a privacy literate citizen, one needs to be aware of their privacy and act accordingly using technological affordances to

develop strategies to protect themselves online. Trepte, Teutsch, Masur, Eicher, Fischer, Hennhöfer et al., (2015) further elaborated the concept of privacy literacy and stated, Online privacy literacy may be defined as a combination of factual or declarative (‘knowing that’) and procedural (‘knowing how’) knowledge about online privacy. In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection, and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection. (p. 339)

Privacy in Networked Spaces. The current politics of software design marked the shift from Privacy 1.0, where the government surveilled, controlled, and censored content at will to Privacy 2.0 where content is generated and communicated by the users through endless opportunities of sharing and distribution (DeNardis & Hackl, 2015). Zittrain (2008) claimed that SNSs companies have successfully combined Privacy 1.0 and 2.0 in the sense that they not only enable the users to take control over data exchange and content production, but also place tremendous power in the hands of governments to surveil, profile, and scrutinize citizens. The age of new media is marked by peer-to-peer interaction and sharing. Zittrain (2008) noted that SNSs enables us to share content about ourselves and others as well, which promotes the creation of a public persona to everyone. With SNSs proliferation and cheap means of access to media creation and release, there is hardly any anonymous user or speech. In other words, speech is regulated and the means through which we communicate today are strictly governed. Balkin (2014) posited that,

The infrastructure of free expression increasingly is merging with the infrastructure of speech regulation and the infrastructure of public and private surveillance. The technologies and associated institutions and practices that people rely on to communicate with each other are the same technologies and associated institutions and practices that governments employ for speech regulation and surveillance. (p, 4)

Social participation in privacy 2.0. Among the researched topics on uses of SNSs is the motivation of using and maintaining a SNSs profile despite the mounted number of threats to privacy (Ajayakumar & Ghazinour, 2017; Hargittai & Marwick, 2016; Jordaan & Van Heerden, 2017; Millham & Atkin, 2018; Taneja, Vitrano, & Gengo, 2014). Special and Li-Barber, (2012) surveyed 127 university freshmen about their motives for using and keeping a Facebook profile; satisfaction the users received from their goals of having a SNSs presence; and the type of information they shared about themselves, and how they managed their audience.

It is important to note that there are two types of audiences: intended and unintended. The intended audience are the users selected by the user to see his/her shared information. Unintended audiences are the users who may get access to content without permission from the account holder, such as from lurkers and stalkers or from personal information being shared beyond that which the user intended. Usually SNSs' information leaks beyond the intended audience via others using screen capture technology and sharing information (Gerber, Abrams, Curwood, & Magnifico, 2017).

In this study by Special and Li-Barber (2017), the researchers counted for the intended audience. Freshmen students seemed to prioritize relationship maintenance for which they mainly used Facebook. Special and Li-Barber (2012) also expressed using

Facebook as a pastime and a tool for entertainment, especially within female participants (N= 90). The most satisfactory goal for using Facebook was to maintain various relationships.

Self-disclosure in privacy 2.0. Regarding self-disclosure, of 127 university students, 81% of participants attested to disclose their personal information including work and education related information (Special & Li-Barber, 2012). Their privacy practices were basic and included the functions afforded by Facebook, such as 54% of participants allowed their 'friends only' to have access to what they share. Special and Li-Barber concluded their research with a caveat finding that the higher the social benefits are, the higher motivation there is to maintain a SNS presence.

Other research has examined self-disclosure from a privacy standpoint. Both undergraduate and graduate students (N= 299) responded to a survey about their SNSs usage intensity (Jordaan & Van Heerden, 2017). About 61% of students felt out of touch without Facebook in their lives. Similarly, 61% of participants mentioned that Facebook is a daily must-do activity. Additionally, 67% of students stated that they would feel sad if Facebook shuts down. The researchers also examined the predictors of less Facebook usage and discovered that lack of control over what information is collected, over personal information, and threats to the loss of privacy were the three major concerns of Facebook users.

The Theory of Planned Behavior (Fishbein & Ajzen, 1975) posited that the attitude of an individual is dependent on the value (positive or negative) that they place on a certain behavior. In other words, the value that Internet users associate with self-disclosure influences their behavior online; and consequently, shapes their beliefs. The

theory of Planned Behavior could be used to explain SNSs self-disclosure. Online self-disclosure is subjective; it is driven by the social value and interest, i.e., positive value. Conversely, if a negative value is obtained as a result of an online self-disclosure act (e.g., data breach), it could restrain the act of sharing online. Therefore, users of SNSs may plan their behavior of sharing and disclosure based upon the potential value (positive or negative) they expect from such social engagement.

Social norm can also affect how individuals act. The perceived social pressure to engage or refrain from certain behaviors, in this case, adoption of privacy security measures, can be promoted by close friends, family members, and online social peers. Taneja, Vitrano, and Gengo (2014) designed a model of privacy attitude measurement to examine the beliefs that individuals hold about adopting and using privacy measures as provided by Facebook. Drawing on a survey of 249 college undergraduates, the results showed that both attitude and social norms positively influenced intentions to adopt and use privacy settings. In return, Taneja et al., found that attitude is positively influenced by the cost of using and of not using Facebook's privacy settings. Interestingly, Taneja and colleagues mentioned that individuals would only adopt the privacy measures if they did not require much work and time.

Using privacy control settings was found to be challenged by the joy of using Facebook or other SNSs, which, at heart, are designed for people to share and mark their online presence (Almgren & Olsson, 2016; Bastos, 2015; Farinosi & Taipale, 2018; Quinn, 2016; Special & Li-Barber, 2012). Online presence drives lurkers and quiet browsers, which motivates participants of SNSs to secure themselves with more heightened privacy measures. Taneja et al., (2014) explained a psychological factor

attached to the cost of using high privacy measures, stating that sometimes it implies that an individual either has something to hide or may be asocial and weird. Moreover, using high privacy controls also has a negative cost that may hint to the employers that their employees have something to hide. In conclusion, as for measuring the cost of using privacy controls, there is a cost and a social impact associated with both actions—whether to use high privacy settings/controls or not.

Social Networking Sites and Privacy Paradox

Privacy Optimism

Using privacy measures is often associated with the notion of comparative optimism or pessimism. In other words, some users may feel secure or insecure online by comparing themselves to others. As a result of optimistic thoughts, adults usually underestimate young individuals' privacy controls/settings. In contrary, young online SNSs users tend to consider their privacy at risk more than their older peers (Kondor, Hashemian, Montjoye, & Ratti, 2018). According Baek, Kim and Bae, (2014), those engaged in highly protective privacy measures usually develop a comparative optimism. Baek et al., also found a relationship between those who are optimistic and those who support a governmental intervention to regulate information online, i.e., more security to boost their optimism.

Data de-identification when optimistic about privacy. Optimism is a feeling that may be different for every individual, but regardless, data can always be traced back to the individual even if the privacy measures are high. Data cues are one way among others to de-identify the user. De-identifying data is especially easy if the information is made public (Gerber, Abrams, Curwood, & Magnifico, 2017; Kennedy & Moss, 2015;

Kondor, Hashemian, De Montjoye, & Ratti, 2018; Zimmer, 2010). For example, Ajayakumar and Ghazinour (2017) studied the Twitter Application Programming Interface (API) and its method to curate data from public Twitter accounts. They found that textual cues could lead to inferences about the user's location with high accuracy. The researchers used the software Geopy[8] which reverses metadata geo-tags into street names and specific locations. Moreover, textual cues published in the tweets could hint at the location and infer on what the user is doing. According to Ajayakumar and Ghazinour (2017), Twitter users should be informed that developers access and harvest their data; and Twitter users should be given a chance to have control over their data from being crawled, harvested, and scraped.

It was meant to work like this. Social networking sites' privacy is a concept that is multifaceted and highly complex. Understanding how SNSs works can help the understanding of privacy issues and enable a safe practice on the Internet. Social networking sites work mainly to serve the people's needs to communicate, to sustain social relationships, and to validate one's self. As an example, Facebook's guiding principles (2018)[9] emphasize that users have freedom to share any content with other user(s). Facebook also guarantees content protection through the available privacy settings; however, at the same time the company also rejects the responsibility of what other users or third-party companies may do with the shared content, whether online or

[8] For more information about Geopy and how it works visit https://geopy.readthedocs.io/en/1.20.0/

[9] See Facebook data policy here https://www.facebook.com/full_data_use_policy

offline. The company encourages the free flow of information and assures that users "… have practical tools that make it easy, quick, and efficient to share and access … information" (Facebook, 2018, n.p). Twitter (2018)[10] declares that "Everyone should have the power to create and share ideas and information instantly, without barriers" (n.p). Information is the fuel of SNSs. Social networking sites need information to operate successfully and accurately. Trading information among users, extensive collection of data, data disclosure to third parties for advertisement and profiling of human behavior, real-time identification of users, and disclosure of data to governments for surveillance are among the actions that engender high privacy risks and concerns (Baruh, Secinti, & Cemalcilar, 2017; DeNardis & Hackl, 2015; Kyei-Blankson, Iyer, & Subramanian, 2016; Proudfoot, Wilson, Valacich, & Byrd, 2018).

Self-disclosure is Necessary to Communicate

People, to an extent, are aware of privacy issues and risks that are related to their movements online. Users, despite the issues related to privacy, maintain a strong digital social presence. Humans instinctively need to communicate (Bennett, 1967), and the phenomenon manifests itself through online disclosure and participation in SNSs. Disclosure has attracted a fair load of scholarship, especially with regards to privacy and privacy paradox (Choi & Bazarova, 2015; Dienlin & Trepte, 2015b; Farinosi & Taipale, 2018; Hallam & Zanella, 2017; Hargittai & Marwick, 2016; Millham & Atkin, 2018). Several issues are related to self-disclosure such as trust in people and in the medium,

[10] See Twitter Rules here https://help.twitter.com/en/rules-and-policies#twitter-rules

risk of losing control over information, and online turbulences with individuals in case privacy is breached (Petronio, 2002). Self-disclosure, according to Millham and Atkin (2018), is a "… communication phenomenon; it is the act of telling" (Millham & Atkin, 2018, p. 53).

Self-disclosure is not new (Luft, 1969). According to Sandra Petronio (2002), self-disclosure is the act of releasing of private information about the self to a determined audience. Social networking sites' self-disclosure plays a crucial role in maintaining relationships and managing a user's identity, just as face to face self-disclosure is vital for real life relationships' development (Altman & Taylor, 1973; Luft, 1969). With 606 college students, Millham and Atkin (2018) conducted an online survey about the students' perceptions regarding disclosure, privacy concerns, privacy beliefs, and trust. The value the participants placed on their information influenced their disclosure behavior in the sense that highly valuing information mitigates disclosure. Moreover, the researchers noticed that sharing information implies that users trust each other. Afterwards, the level of trust increased with reciprocity—mutual sharing feeds mutual trust. Trust in sharing information increases as a result of the frequency of reciprocal information exchange.

Noticeably, privacy management remains a complex practice despite users' measurement of pros and cons of disclosure, also known as privacy calculus (Dinev & Hart, 2006). The nature of a SNSs network, with its diverse and multilayered audience, makes it almost impossible to determine who can access disclosed information (Jeong & Kim, 2017; Marwick & boyd, 2011). The seeming lack of control over the shared information, real-time identification of users, varied metadata collection on individuals

(i.e., where, when, user IP, Hardware ID, software configuration, location and time, search activity, etc.), and the sharing of data with third-party companies for profit (Baruh & Popescu, 2017; DeNardis & Hackl, 2015; Everson, 2017; Fallik, 2014) are some issues that are at the heart of user's privacy concern.

Privacy Paradox and Self-disclosure

The asymmetry that exists between privacy concern/worry and users' disclosure of information is another area of research in the realm of digital privacy (Dienlin & Trepte, 2015; Hallam & Zanella, 2017; Hargittai & Marwick, 2016). It is also labeled a privacy paradox (Barnes, 2006). A privacy paradox happens when the user's concern for their personal information mismatches their actual disclosure behavior. In an extensive literature review on privacy paradox, Kokolakis, (2017) drew clear distinction between privacy as a concern and as an attitude. Privacy concern is a feeling that accompanies SNSs' users in general. Attitude is more precise; it is privacy concern as it relates to specific context; concern for privacy loss as an attitude changes with the change of context and situation (Kokolakis, 2017). The literature review by Kokolakis (2017) concluded that privacy paradox, as a phenomenon, has produced conflicting results. Some studies showed that privacy concern is not aligned with the attitude and the act of information protection (Acquisti & Grossklags, 2005; Blank, Bolsover & Dubois, 2014), while others showed that privacy concern leads to less disclosure and more privacy control attitude (Debatin, Lovejoy, Horn & Hughes, 2009; Lee, Park & Kim, 2013).

Privacy concern is influenced by many other SNSs issues which, in turn, influence the user's privacy behavior. Social networking sites' issues are various such as immediate gratification (Quinn, 2016), relationships that require sharing and disclose

(Cheung et al., 2015), and the lack of privacy literacy (Park, 2013). Kokolakis (2017) illustrated that privacy auction studies showed that users may attach a low value to their personal data or simply give it away for free; however, this may not be an open invitation for uncontrolled and unconsented data collection by tech companies. Similarly, researchers (Jeong & Kim, 2017; Marwick & boyd, 2011; Tufekci, 2008) agreed that privacy is strictly bound to a specific context, and so is users' concern over privacy. Kokolakis (2017), and in agreement with Nissenbaum (2010), added that privacy is highly contextual and information sensitivity changes frequently as users attribute different values to their information.

Privacy paradox and social gratifications. Different surveys and testing models of privacy have yielded different results. Sharing personal information usually follows a calculus or an assessment of risks and benefits. Studies (e.g., Dinev & Hart, 2006; Jiang, Heng & Choi, 2013; Xu, Luo, Carroll & Rosson, 2011) showed that privacy calculus is used by users whenever they felt concerned about their data or activity online; however, the perks of SNSs, such as entertainment, need for relationships, and identity building (Debatin, Lovejoy, Horn, Hughes, 2009) may challenge the privacy calculus model and completely undermine it at times. Debatin et al., (2009) added that when using SNSs becomes routine, self-disclosure becomes routine, and it is hard to deviate from routine.

Hallam and Zanella (2017) were the first to apply the Construal Level Theory (Trope & Liberman, 2000, 2010) to explore SNSs disclosure and the gap that exists between privacy as concern and privacy as action. The theory posits that behavior follows a risk appraisal, and if risk is perceived to persist for a long time, the protection behavior will increase, and vice versa is true. In a survey study with 222 participants, Hallam and

Zanella (2017) found that privacy risk is an abstract concept and is perceived by SNSs users as distant and far in time; conversely, self-disclosure to earn social rewards is perceived as immediate and tangible. We humans are genius and able to convince ourselves of risks to be far and distant in time in order to disclose ourselves for immediate earns or gratifications. Hallam and Zanella's hypothetic model showed that privacy paradox could be explained when a decision to self-divulge is made following a near future social gratification.

The finding from Hallam and Zanella's (2017) study is closely related to cognitive biases users are known to have when managing their privacy. For instance, Baek, Kim, and Bae (2014) posited that individuals see a comparative optimism in the sense that others are more likely to fall victims of privacy infringement than they themselves fall victim to privacy infringement, especially if the comparative target population is younger. In other words, individuals see privacy risks close to others and far from happening to them. Comparative optimism when added to social gratifications can explain, to a great extent, the phenomenon of privacy paradox.

Affect heuristic is another cognitive bias that accompanies human decision making (Slovic, Finucane, Peters, & MacGregor, 2007). Affect heuristic allows people to make quick judgements based on impressions and feelings. Affect heuristic manifests itself in the world of SNSs when individuals assess privacy risks and tend to ignore them when associated with things they like, while overestimating the risks when associated with things they dislike. A positive affect heuristic, i.e., accepting the risk of self-disclosure, could be motivated by social capital or social validation. Simply put, processing the risks associated with self-disclosure on the one hand, and assessing the

gratifications a user obtains through sharing on the other could explain privacy behavioral paradox.

Regarding the methodology through which privacy paradox has been assessed, through a meta-analysis of studies, Kokolakis (2017) made a distinction between systematic and heuristic processing of privacy risks in the sense that individuals' responses to privacy management questions in surveys are a result of systematic/logic processing; however, their behavior in reality may be a result of heuristic processing which involves multiple biases and changes from a livable situation to another. This could, in fact, be one of the explanations of the privacy paradox in the sense that users' behavior regarding privacy is unpredictable and contextual (Nissenbaum, 2010).

Privacy paradox in college. In an attempt to understand the privacy paradox phenomenon with college students, Hargittai and Marwick (2016) used a series of focus groups and a survey to examine the relationship between Internet usage, privacy concern, and potential privacy risks. Additionally, the researchers explored the relationship between SNSs self-disclosure and privacy risks; privacy concern and privacy literacy; and whether cultural differences influence the participants' behavior. Hargittai and Marwick (2016) contested that the participants showed an understanding of the potential privacy risks, and those with high privacy concern spent less time on the Internet. However, there was no significance recorded regarding concern for privacy loss and use of SNSs. The students showed their concern about the lack of control over their personal information due to the structure of SNSs. The business model of SNSs thrives on the act of sharing and online presence, which may jeopardize personal privacy (Hargittai & Marwick, 2016; Marwick & boyd, 2014).

The findings from Hargittai and Marwick's (2016) study distinguished among two types of students. Those with high privacy concerns tended to adopt privacy protection measures and share less of their personal information, whereas those with high privacy literacy skills maintained a regular use of SNSs and applied strong privacy protection measures. More research needs to be conducted to study the relationship between privacy concern, SNSs use, and privacy protection measures. Therefore, having privacy concerns may lead to self-censorship of content and hesitant online practice (Hargittai & Marwick 2016; Vitak, Lampe, Gray, and Ellison, 2012).

Hargittai and Marwick (2016) discovered that privacy paradox could be related to other issues than merely a lack of privacy literacy or understanding. The researchers showed that losing privacy could partly be due to the pragmatics of SNSs. To explain, SNSs privacy is complex in the sense that sharing content means sharing privacy; privacy settings change frequently; and, lastly, SNSs users share content according to settings of their network (friends, and family members). Provided these conditions, privacy leaks may be avoided by complete opt-out. It is unrealistic, as SNSs are highly important in today's networked environment (Taddicken, 2014). A participant in Hargittai and Marwick's (2016) study said,

I feel like [pause], then you have the choice between not using the Internet and therefore keeping free of the surveillance, or living with it. So, I do care [about privacy]; but I guess I don't care enough not to use the Internet. And I'm not sure what the alternative is at the moment. (p. 3751)

Privacy as a Collective Social Norm

When discussing privacy and individuals' interactions online, it is important to consider human nature and its social aspect. Gofman (1959) posited that people's interactions with each other are regulated by context and audience. Social networking sites give people the opportunity to see others and allow others so see them. Sharing is the currency of participating on these sites. Therefore, privacy, as is self-disclosure, is contextual and depends on the audience. Privacy is individual while human societies are collectively intertwined (Cohen, 2012). Altman (1977) theorized that privacy is a collective concept since sharing is at the heart of human relationships. Managing privacy involves the constant management of boundaries among different spheres and communities (Palen, & Dourish, 2003). On SNSs and on the Internet, people must type themselves into being. Sharing is existing and self-disclosure does not happen solely with individuals; it also happens with a group of individuals.

Networked privacy. The difference in age, relationship with the SNS account holder, education level, etc., that exists among the audiences (intended and unintended) causes what Marwick and boyd (2011) call "context collapse." Context collapse happens when content that is destined to a certain category of the SNS audience (e.g. work colleagues) may be accessed by another audience (e.g., family members). Context collapse renders privacy control difficult for individuals to maintain, but possibly attainable collectively. In other words, privacy is ideally attainable if the different audiences (e.g., friends, family members, etc.) who have access to content share the same understanding of privacy.

Marwick and boyd (2014) suggested a framework to examine privacy in connected societies or SNSs that is 'networked privacy.' The concept of networked privacy places responsibility for any privacy loss on the constellation of audience, software, and shared social norms or context within which content is shared. Like Altman's (1977) concept of collective privacy, networked privacy involves the constant negotiation of boundaries and contexts that are fluid and often collapse with slight changes in audience—for example if a parent joins the child's online circle of friends, privacy settings may change. Privacy protection in a networked context is not a mere control of who can access what content, but it is having a strategic and meaningful control over the contexts in which information circulates. Marwick and boyd (2014), therefore, claimed that regulating privacy based on the individual's practice, such as SNSs settings, does not reflect the networked society of today.

Sandra Petronio (2002) conceptualized privacy as a give-and-take process and authored the theory of Communication Privacy Management (CPM). One of the basic tenets of the theory is privacy ownership. In agreement with Altman (1977), Cohen (2012), and Marwick and boyd (2014), Petronio (2002) posited that information is private and under total control if unshared. However, once sharing information, the ownership becomes an equal responsibility between the owner and the recipient. This co-ownership could be either assumed or declared depending on the level of trust between individuals. If the ownership contract is broken, then privacy turbulence may occur. Therefore, privacy is a collective responsibility and the boundaries are constantly being negotiated depending on context and audience. Privacy is a process of negotiation with the co-

owners of the information and depends on the situation where personal data is being used.

Web 2.0 Technologies and the Literacies

Literacy as a term has traditionally referred to a basic competency in reading and writing. It is the ability to "… read the ordinary texts of modern society— newspapers, information books, novels; to be able to write using correct spelling and grammar; and to appreciate high- cultural values through exposure to a taste of the literary canon" (Cope & Kalantzis, 2015, p. 1). Beginning the 1990's, living and engaging in society as a performant citizen required more than just traditional literacies. The shift was also driven by mass media, Internet, and the availability of modern forms of text. The New London Group (1996) manifesto suggested that participating in a modern society requires a broader understanding and practice beyond language. The group encapsulated their work in one word: Multiliteracies. Multiliteracies extend beyond text to include visual, spatial, audio, and behavioral contexts, forms of learning/expression, and meaning making (The New London Group, 1996).

In this literature review, I consider the four classic modes of communication, as in reading, writing, listening, speaking, are foundational to acquire the new literacies: information, digital, and media. Within these literacies (information, digital, and media), I will situate privacy literacy, as a new literacy and discuss it from a multi-disciplinary approach. The rationale for selecting these literacies (information, digital, and media) is because they are closely related to privacy literacy and they are sensitive to technology and media development. Moving forward, the word literacies will refer to traditional literacy (reading and writing), digital literacy, media and information literacy, and

privacy literacy. I will use the metaliteracy framework (Mackey and Jacobson, 2011) to discuss these literacies together.

Web 2.0 are products and services that function on the premises of user-generated content, sharing, and participatory culture (Mackey & Jacobson, 2011). Social networking sites, as an example of Web 2.0 technologies, have generated tremendous amounts of data as a result of sharing and transferring loads of information between individual users and among networks/groups. Among the topics related to literacies and technology, scholars have focused on SNSs and attempted to unravel how SNSs can inform education and social practices as well as shape identity performance(s) across spaces (Eaton, 2017; Gerber, Abrams, Curwood, & Magnifico, 2017; Mohamed, Gerber, & Aboulkacem, 2016).The escalation in the amount of shared information across digital spaces makes it increasingly necessary for users to acquire skill sets, i.e., the literacies, in order to safely and proficiently benefit from participating in the digital age. Parallel to the development of technologies, literacies have developed and continue to develop. Because literacies are sensitive to technological advancement, their definition lacks a consensus. Nevertheless, the existing literacies (e.g., information, digital, and media), as mentioned prior, do intersect and build upon each other. The current study focuses on privacy literacy, but it is important to discuss the related literacies: information, digital, and media literacies or, metaliteracy as an enveloping framework—as suggested by Mackey and Jacobson (2011).

Information literacy is critical thinking. In the U.S., information literacy has been used since the 1980s to discuss issues related to technology use and information consumption. For instance, in 1989, the American Library Association (ALA) published

the *Presidential Committee on Information Literacy: Final Report*, where the authors expressed their motivation to write the report saying, "Information is expanding at an unprecedented rate, and enormously rapid strides are being made in the technology for storing, organizing, and accessing the ever-growing tidal wave of information" (n.p). This sentence could be adapted to define technological innovations as well. Technology and information literacy are closely related.

Digital literacy. The term digital literacy has been around since the 1990's to refer to the ". . . ability to read and understand hypertextual and multimedia texts" (Bawden, 2001, p. 246). It involves reading, writing, viewing, listening and representing information across online spaces (NCTE, 2019). Understanding hypertextual and multimedia texts encompasses ways an individual can apply to access reliable sources of information and be able to evaluate content. According to the NCTE's digital literacy framework (2019), an individual should be able to:

- Effectively act in the networked world;
- Investigate content in its variety of presentation and design;
- Mindfully consume information, collect, and recreate content across spaces and contexts;
- Develop cross-cultural competencies to collaborate and solve common issues;
- Examine the laws and regulations of creating and sharing online content; and
- Read text (in various formats) and trace the underlying narratives, biases, and ideologies.

In addition to information literacy, digitally literate individuals need to also be able to sift through content to extract the most accurate information for use. Lanham's (1995) dichotomy between literacy and what he calls 'multimedia literacy' may help better understand digital literacy as a concept and a set of skills. To Lanham, literacy in

online environments is to understand information as presented, i.e., raw processing of information. Digital literacy or multimedia literacy, to Lanham, is the ability to select and understand various forms of content, such as sound, picture, and picture in motion. In this case, digital literacy is the ability to be selective about access and understanding of digital content.

According to Paul Glister's (1997) early work in digital literacy, digital literacy is ". . . the ability to access networked computer resources and use them" (p. 2). Jones-Kavalier and Flannigan (2006) posited that, "Digital literacy represents a person's ability to perform tasks effectively in a digital environment, with 'digital' meaning information represented in numeric form and primarily for use by a computer" (p.9). Projects, such as https://www.digitallearn.org/ which was launched in 2013 by the Public Library Association, provide a broader idea of digital literacy skills that extend from simple functions, such as creating an email box, to complex practices such as detecting reliable information or managing online privacy. Jones-Kavalier and Flannigan (2006) concluded that, "Literacy, in any form, advances a person's ability to effectively and creatively use and communicate information" (p. 9).

The term Information Communication and Technology (ICT) is also connected to the concept of digital literacy and they both focus on information processing and the appropriate selection of digital tools (Mackey & Jacobson, 2011). The International ICT Literacy Panel (2007) agreed that ICT literacy means "… using digital technology, communications tools, and/or networks to access, manage, integrate, evaluate, and create information in order to function in a knowledge society" (p. 2). Like ICT literacy, technological literacy is defined as a literacy that "… focuses on the use of digital tools,

resources, and technologies for the advancement of student learning, development, and success…" (ACPA & NASPA, 2015, p. 33). Noteworthy, Digital literacy builds upon information literacy in the sense that access to information and knowing how to critically filter content is a steppingstone into knowing how to produce information using adequate digital equipment.

Information, as it changes in definition, obliges us, as educators and learners, to constantly shape-shift our skills and update them to survive. Literacy, in its various forms, is more than a survival skill. As information production and dissemination change, the rest of literacies and critical thinking associated with them will change and evolve. Said differently, technology causes a ripple effect that radiates to other literacies and skill sets. New media, or the technological developments in media, have brought about many changes and led scholars to research a combination of literacies called media and information literacy (Potter, 2014; Silverblatt, 2008; Schmidt, 2012; Fleming, 2014; Hobbs, 2016).

Information should be accessible to everybody; hence, information literacy is the responsibility of everyone. These motives and necessities are still relevant to today's age and probably with more knowledge requirements, as information and knowledge are managed by more sophisticated technologies and content-algorithms today than they were in 1989.

The ALA' 1989 report emphasized that public participation in making and sharing content as well as becoming an information literate person is of utmost importance. The authors of the report defined information literacy as being, "… able to recognize when information is needed and have the ability to locate, evaluate, and use

effectively the needed information" (n.p). At the heart of this definition lies critical thinking. Over two decades ago, Gilster (1997) linked critical thinking to the digital age and posited, "[It] is the ability to make informed judgments about what you find on-line" (p. 1). Critical thinking enables citizens to exercise their rights by making informed decisions, especially within the flood of information we experience today. The ALA report, despite written in 1989, still retains its validity and relevance to the age of SNSs 2.0. Its authors claimed, "Instead of drowning in the abundance of information that floods their lives, information literate people know how to find, evaluate, and use information effectively to solve a particular problem or make a decision" (n.p). An example of information overload is news, including but not limited to broadcast news, online news sites, and newspapers. Deciphering information, news, and other content online is a key 21st century SNSs literacy skill (Aboulkacem & Haas, 2018). Aboulkacem and Haas (2018) designed a framework through which they suggested examining online content, news, and SNSs information. Among the factors that influence the individual's decision about a piece of information are family and friends, location of information, beliefs, content management algorithms, others' comments and suggestions, and SNSs political orientations. Being an information-literate citizen mitigates the influencing power of these factors and allows for a well-informed decision and participation in the public community.

From a general point of view and in relation to all technologies, Mackey and Jacobson (2011) argued that an information literate individual,

Must be aware of these information surroundings and understand the ever-increasing impact that information and emerging technologies have on our lives. This requires an

ongoing exploration of the legal, economic, political, and social issues that mediate our access to technology and often define the types of documents we evaluate and use. (p. 70) Knowing how knowledge is prepackaged and how content is organized are key critical thinking and information literacy skills that would enable Internet users to safely browse content while consciously consume necessary information. Eisenberg (2008) defined information literacy as a "… set of skills and knowledge that allow us to find, evaluate, and use the information we need, as well as to filter out the information we don't need" (p. 1). In this body of literature, the literacies mentioned above were found to co-exist, or interconnect, by definition and scope of practice; however, they were also found to have no consensus over their definitions. This applies to critical thinking as well; it has multiple definitions with no consensus over one recognized definition among scholars (Johnson & Hamby, 2015). Critical thinking is connected to all literacies. Information literacy seems to be the core skill that lays the foundation to digital, media, and privacy, since information literacy helps us access knowledge with efficient tools of selection and evaluation.

Media and information literacy. Much like critical thinking and the aforementioned literacies, media literacy has no consensus definition (Hobbs, 2016). According to Hobbs, media literacy does not have a clear history, because the experiences with media and technologies are unique and differ according to the individual's, "… personal and intellectual histories" (p.3). There are few definitions that are consistently used in media literacy scholarship. For instance, the attendees of the Aspen Media Leadership Institute conference (1992) agreed to define media literacy as, "The ability to access, analyze, evaluate and communicate messages in a wide variety of

forms" (Aufderheide & Firestone, 1993, p. 7). Thoman and Jolls (2005) viewed media literacy as a principal set of skills based on inquiry that is primordial to citizens living in democracy. Tessa Jolls, President and CEO of the Center for Media Literacy, in Malibu, California, and a founder of the Consortium for Media Literacy, a research nonprofit, posited that, "There is no democracy without reliable information, nor is there true information without reliable media" (Personal communication, 2017). The citizen's right to access information and be able to obtain true information, she said, "… is part of our responsibility as researchers and educators" (Personal communication, 2017).

Access to information and various forms of media with critical thinking can guarantee civic engagement and active participation in public sphere. In today's enmeshed information world, reading the media and its messages, as well as producing meaningful media, are highly important skills. Twenty first century life and digital culture are fluid and constantly shifting especially with social Web 2.0 technologies, or 'push technologies' as described by Mackay and Jacobson (2011). Push technologies (e.g., Facebook, Apple news, workout apps, etc.) are convenient. Push technologies enable media content to come to the individual, but the individual users "... must develop a critical thinking filter to continuously differentiate the usable from the unusable. If the filter is not already present in the medium itself, the information user must develop one as part of the search process" (Mackay & Jacobson, 2011, p. 72).

How does media literacy, also referred to as media and information literacy or media education, transfer to real life skills? In other words, what is it like to be a media-literate citizen? Part of the answer is Jeremy Stoddard's (2014) claim that living in a fluid age of media and technologies, where information production and content change

frequently, the individual is required to know about "…the expertise or viewpoints of people contributing to the information [we] are accessing… the design of applications, databases, search algorithms, and web pages" (p. 1-2).

Critical Thinking: The Golden Standard Underlying the Literacies

Becoming a media-literate individual can mean the "… active inquiry and critical thinking about the [media] messages we receive and create… [Media literacy] develops informed, reflective and engaged participants essential for a democratic society" (National Association for Media Literacy Education, 2007, n.p). Becoming a media-literate requires individuals to be aware of the information ecology and understand its ever-happening effect through emerging technologies and different formats of 'text' (Hobbs, 2010). Mackay and Jacobson (2011) posited that this necessitates searching information related to the legal, economic, political, and social issues that orbit around our use of technology. Philosopher Paulo Freire (1970) advised that reading the world precedes reading the word. In other words, becoming familiar with the technological world around us should be a pre-requisite to reading content with its varied formats.

Beyond Traditional Literacies

Traditionally, literacy in its basic definition refers to the acts of reading, writing, speaking, and listening. However, means of communication have developed tremendously, and many current forms of communication might extend beyond the traditional definition (New London Group, 1996). For example, with the emergence of emoji writing, Artificial Intelligence, predictive text writing, natural language processing softwares and the like, people have created symbols and languages of their own, in addition to the known forms of communication. Additionally, the affordable means of

media production (e.g., phones with cameras) and dissemination (e.g., YouTube) have changed the meanings of literacy, of reading, of writing, and of text. Hobbs (2010) defines text as "…any form of expression or communication in fixed and tangible form that uses symbol systems, including language, still and moving images, graphic design, sound, music and interactivity" (pp. 16-17).

The world in which we live has been called by the New London Group (1996) a world of "Multifarious cultures that interrelate… [through] a plurality of texts that circulate…" (p. 61). The group in their seminal article suggested that literacy pedagogy and teaching should account for the multitude of texts and multimedia content associated with information technologies. The context of media (e.g., books, movies, photos, etc.) is indeed critical to defining and instructing literacy education. Renee Hobbs (2010, 2016) added an emphasis on 'text,' as defined prior, and argued that part of being a media literate citizen is being able to dissect the message elements (form, content, and context). She also posited that a media message is socially interpreted as everybody is connected. So, what is 'text' considering the rapid technological shifts and how could message format, content, context, and means of production influence the definition of traditional and media literacy?

Reading traditional text requires content clarity as well as knowledge about context. In the case of SNSs, Marwick and boyd (2014) argued that Web 2.0 made context, text, and audience collapse together. The context is blurred and so is the participatory audience. Social networking sites have rendered the production and dissemination of content convenient. Equally important, social media have also rendered comprehension and critiquing of information a tedious process that is governed by many

‘influencing powers’ such as software structure, family, friends, content algorithms, and others’ viewpoints (Aboulkacem & Haas, 2018).

In online spaces it is important to note that different literacies are interrelated, not segmented and isolated excursions into meaning making and comprehension (Gerber, 2008). Contemporary literacies require critical thinking and a sharp comprehension of the surrounding informational environment. Overall, Hobbs (2010) pictured the profile of a digital media literate person as someone who:

- Makes responsible choices about information access by finding, sharing, and comprehending ideas;
- Analyzes messages by reviewing the author, his/her point of view, and content reliability;
- Creates content using image, still and in motion, sound, and language and a variety of ICTs;
- Applies social responsibility and ethical principles to reflect on his/her own conduct online and offline;
- Takes social action individually and collectively to exchange content and actively participate in solving family, workplace, and/or community problems.

Becoming a media literate individual is “... to possess the necessary tools to access media content, raise the appropriate questions, and follow through with solid critical thinking to synthesize and inform personal decisions” (Aboulkacem, 2019). Web 2.0 technologies have collapsed contexts and audiences and scattered information across multiple digital spaces (Chock, Wolf, Chen, Schweisberger, & Wang, 2013; Marwick & boyd, 2014); hence, browsing media content to locate the needed piece of information and produce meaningful media content requires refined skills.

Digital Privacy

Horton (2007) in a UNESCO report, *Understanding information literacy: A primer*, grouped the existing literacies in a family and described them as 'the survival literacies.' The family of literacies, according to Horton, have a complementary and interactive relationship. The survival literacies are the core or traditional literacy skills (reading, writing, speaking, listening), computational literacies, media literacy, online and e-learning, cultural, and information literacy. The constellation of literacies suggested by Horton could be foundational to continuing to survive in a fluid media and technology environment. Tuominen (2007) reflected on the continuous emergence of new technologies and stated that "New kinds of literacies are needed in dealing with the various born-digital document types and genres—like short-text messages, emails, blogs, wikis, podcasts and RSS feeds—that are forming an increasingly larger part of our present day and future information environments" (p. 6). Literacies, such as digital, information, media, and privacy, grow and evolve in scope, definition, scholarship, and are responsive to technological advancement.

One takeaway from this body of literature on privacy literacy is the lack of consensus on its definition. The existing definitions are dependent on the perspective from which the author/researcher undertook the topic or the scholarship and scope of practice. Like critical thinking, privacy literacy is a field of study with a multitude of definitions and little consensus (Johnson & Hamby, 2015). Solove (2006) argued that privacy, as a concept, although widely discussed, "… is in disarray [and] nobody can articulate what it means" (p. 477).

Privacy has taken many shapes and followed many standards in law, politics, economics, research, education, and health. For this reason, defining privacy as one simple practice is extremely difficult. It is not only because the concept of privacy differs from one discipline to another, but it is also viewed differently in different cultures and among different people. An individual's conceptualization of privacy continuously changes and adapts to context (Nissenbaum, 2010). Taking law as an example, Europe's view and legislation of law concerning digital data privacy through the General Data Protection Regulation (GDPR) is different than the current U.S.' regulations (e.g., California, Vermont, or San Francisco privacy laws) of digital data and privacy.

Social psychologist Irwin Altman (1977) conceived privacy as ownership of who can have access to the self. He argued, "Privacy is a boundary control process whereby people sometimes make themselves open and accessible to others and sometimes close themselves off from others" (p. 67). Echoing Altman, Rachels (1975) discerned the concept of privacy as someone gatekeeping access to any personal information. Ideally, one may strive to have privacy by isolating himself or herself from others while maintaining social relationships and bonds; however, this situation is unrealistic and is dependent, to a great extent, on the diversity of social situations and the medium of communication.

The new panopticon. New technologies and social media have made it difficult to protect personal data. The constant watch and enhanced surveillance techniques, since almost everyone has a social persona, brought back the concept of the panopticon (Bentham, 1791; Foucault, 1975). The panopticon, as a concept, was written by philosopher Jeremy Bentham in 1787 in a series of letters sent from Russia to England

(Bentham & Bozovic, 1995). Later, the letters were followed by two postscripts in 1790 and 1791. Bentham's work was first brought to the public attention by Michel Foucault (1975) in his book *Surveiller et punir: Naissance de la prison.* The Panopticon was conceptualized as a ring-shaped building in the middle of a prison which alludes inmates that the guards are inside and constantly watching them (Bentham, 1791; Foucault, 1975). According to Bozovic (1995), the panopticon was "… a simple idea in architecture, never realized, describing a new mode of obtaining power of mind over mind… the possessor of this power is the inspector with his invisible omnipresence" (p. 1). Building a panopticon was meant to give prison-inmates a sense of continuous monitoring and invisible omnipresent surveillance. The same concept of constant watch was illustrated by Orwell's *1984* work with TV screens in-watch of citizens' homes and the Newspeak language that suppresses any rebellion or political discourse. Some scholars considered the current new technologies as a process that emphasizes the concept of the 'big brother' (Orwell, 1949) and claimed that ambient technologies recreate a sense of omnipresent surveillance—whether by the government or commercial companies using Artificial Intelligence (AI) and predictive analytics (Bloom & Clark, 2016; Bossewitch & Sinnreich, 2013; Gerber, 2018; Power, 2016; Safire, 2002; Solove, 2007). Owning a phone or any other connected communication technologies increases the risk of data amassment, profiling, surveillance, and targeting (Albrechtslund, 2008; Marwick, 2012; O'Neil, 2017; Power, 2016).

Privacy literacy, a new literacy. Veghes, Orzan, Acatrinei, and Dugulan (2012) argued that privacy literacy is, "… a new concept proposed in order to assess and explain the consumers' [or internet users'] attitude regarding the collection, processing and

employment of their personal data" (p. 705). Warzel (2019) commented on the term privacy as "… an impoverished word—far too small a word to describe what we talk about when we talk about the mining, transmission, storing, buying, selling, use and misuse of our personal information" (n.p). We lose our privacy when we lose any piece of data that could potentially relate back to our physical person in real life. Thus, privacy literacy could be, "… the understanding that consumers have knowledge of the information landscape with which they interact and their responsibilities within that landscape" (Langenderfer & Miyazaki, 2009, p. 383). The heart of privacy literacy is being able to protect ourselves in multiple settings. Warzel (2019) clarified,

Privacy is about how that data is used to take away our control. Today, our control is chipped away in ways large and small. It may be as innocuous as using your listed preferences, browsing behavior, third-party information about your annual income and a rough understanding of the hours that you're most susceptible to make a purchase to nudge you toward buying a pair of shoes. Or it may be as potentially life-altering as the inability to get a loan or see a job listing. (n.p)

Privacy literacy serves to help users of SNSs or other interactive websites, where personal data are needed for functionality, to discern the risks and weigh them against their privacy values and personal information (Correia & Compeau, 2017). In other words, privacy literacy involves knowledge about the practices of information amassing and profiling as well as what shared information about ourselves could be harmful to us in real life.

In the age of big data, part of becoming a privacy literate individual means having the necessary "… understanding and awareness of how information is tracked and used in

online environments and how that information can retain or lose its private nature" (Givens, 2015, p. 53). Mackey and Jacobson (2011) argued that learners need more understanding and practice than just learning how to use a computer. The authors considered the literacies needed for survival today are "… a set of intellectual capabilities, conceptual knowledge, and contemporary skills associated with information technology" (p. 66). In brief, Debatin (2011) encapsulated privacy literacy saying it "… encompasses an informed concern for […] privacy and effective strategies to protect it" (p. 51). Firstly, privacy literacy includes an awareness about the danger of losing personal information to an unintended public; and, secondly, privacy literacy calls for active involvement in seeking strategies and ways to mitigate disclosure and manage personal data.

Privacy literacy operationalized. Research related to privacy literacy focused on knowledge and awareness of individuals vis-à-vis data collection practices, privacy laws and policies, in addition to ways to protect personal data (Park, 2013; Trepte et al., 2015) . With ambient technologies such as Alexa, Siri, Google assistant/interactive microphone, and a plethora of free social media websites, the scholarly debate on privacy has escalated and protecting personal data became a primary vital life skill (Ajayakumar & Ghazinour, 2017; Bartsch & Dienlin, 2016; boyd & Hargittai, 2010; Child, Haridakis, & Petronio, 2012; Park, 2013).

Before Web 2.0 technologies, privacy studies had the same goal, that of studying personal data protection and dissemination; however, the research scope was different. For instance, privacy research in the 1990's revolved around direct marketing and intrusion of personal lives as well as the ways customers sought to opt out from the

mailing lists (Culnan & Regan, 1995; Nowak & Phelps, 1997). Today's privacy literacy shifted to focus on developed marketing mechanisms empowered by sophisticated AI and algorithm systems. Technology remains the main driver of literacy skills as well as law and regulation. Privacy literacy today, and in most cases, means knowing what personal data are collected and what possible strategies available to protect them. It is, however, important to notice that the concept of privacy literacy is starting to grasp its identity and definition (Wissinger, 2017).

With Web 2.0 technologies, almost every conversation involves some sort of self-disclosure. Privacy literacy in this context means control over personal data and digital footprints. Park (2013) argued, "In the digital era, the idea encompasses critical understanding of data flow and its implicit rules for users to be able to act. Literacy may serve as a principle to support, encourage, and empower users to undertake informed control of their digital identities" (p. 217). Correia and Compeau (2017) assumed that users with privacy literacy education can assess the risks of disclosing themselves online including those incurred as we share information online.

Correia and Compeau (2017) borrowed the principle of situational awareness (Endsley, 1995) to develop a definition of privacy awareness. Endsley defined situational awareness as "… the perception of elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" (p. 36). In other words, situational awareness is perception as in knowledge about the situation components; comprehension as in how people collect, interpret, memorize, and use information; and projection as in is the use of perception and comprehension to predict or plan the future. Situational awareness is usually used in pilot

training, surgery emergencies, or military warfare. Correia and Compeau (2017) suggested the use of situation awareness to analyze the current privacy driving elements such as "… technology, regulations or common practices used by companies or individuals to collect, use and share user's private information" (p. 4024).

Correia and Compeau operationalized privacy literacy in light of situation awareness and posited that "[Perception] is related to previous studies on knowledge and literacy while [comprehension] applies [perception] to the current environment. [Projection] relates future implications or risks of the private information collected or the advancements in technology, laws, and common practices" (p.4024). Put differently, privacy literacy is about having the necessary skills to analyze the technological environment, apply that to reflect and protect oneself from personal data loss, and make sure one remains up-to-date with subsequent technological and law developments.

Privacy paradox happens when attitudes and thoughts about privacy do not match the actual user's behavior online. Trepte, et al. (2015) published a seminal article operationalizing privacy literacy and suggested that privacy literacy will act as a stopgap to the privacy paradox. Trepte and colleagues (2015) assumed that people are, in effect, worried about their digital privacy and would like to handle their data and online reputation effectively. Inspired by Ackerman's (2008) work on cognition and types of knowledge—declarative versus procedural—Trepte et al., (2015) conceptualized privacy literacy as a combination of declarative and procedural knowledge. Privacy declarative knowledge is "The user's knowledge about technical aspects of online data protection and about laws and directives as well as institutional practices" (Trepte, et al., 2015, p. 339). Privacy procedural knowledge is, "The user's ability to apply strategies for

individual privacy regulation and data protection" (Trepte, et al., 2015, p. 339). To better plan for privacy literacy teaching and education or technology design, it is important to know what students' or internet users know about privacy designs, laws, and companies' practices of data collection.

Meta-Literacy: A Theory for Social Networking Sites Research

Specifically related to social networking sites literacy and the collaborative environment of Web 2.0 technologies, metaliteracy, as advanced by Mackey and Jacobson (2011), is considered an umbrella set of knowledge that enables individuals to form a solid competence that develops hand-in-hand with technology. As such, Mackey and Jacobson highlighted the connectedness of online users and studied the effort individuals share together to produce and share content. The authors argued that,

> While information literacy prepares individuals to access, evaluate, and analyze information, metaliteracy prepares individuals to actively produce and share content through social media and online communities. This requires an understanding of new media tools and original digital information, which is necessary for media literacy, digital literacy, and ICT literacy. (p. 76)

In relation to privacy, today's information dissemination as well as participation encourage sharing and collective production of information as well as data. To relate metaliteracy with privacy literacy, Mackey and Jacobson (2011, 2014) and Kember and Zylinska (2012) warned that users should be aware of the impact technological devices have on us. Mackey and Jacobson (2011) argued that metaliteracy requires a multidimensional education. In other words, online privacy literacy, as in metaliteracy, "... requires an ongoing exploration of the legal, economic, political, and social issues

that mediate our access to technology" (Mackey & Jacobson, 2011, p. 75). Metaliteracy theory, as found in this literature review, is the only theory that acknowledges the role of SNSs users' participation in knowledge creation. The theory seeks to empower users and equip them with the necessary tools to accurately self-evaluate their skills as they browse online content, understand their role as producers of content, and remain critical in understanding how their data are collected and processed (Mackey & Jacobson, 2011, 2014).

As explained prior, literacies are interconnected, and they complete one another. These literacies (i.e., information, media, digital, and privacy) are crucial to coping with technological advancements. Traditional modes of communication as in reading, writing, speaking, and listening are strongly connected to digital and information literacies. Privacy literacy involves comprehending the context and data processing activities. Additionally, privacy literacy involves comprehending the law and the fine print of online service providers' policies. Finally, privacy literacy is comprehending the affordances of software in order to make an informed decision about participation in SNSs.

Chapter Summary

The main objective of Chapter Two was to lay the foundation to introduce privacy literacy, and position it as a concept and a survival skill among other literacies needed for the age of push media 2.0. Additionally, I explained the pervasiveness of personal data collection and processing for commercial ends or mass surveillance. However, due to SNSs self-disclosure gratifications, these platforms have also facilitated much of data collection. In this chapter I defined the literacies and positioned privacy literacy within

software and law. I also demonstrated how software, as a written text of code, limits the users' behavior online, influences law, and benefits a certain population of elites on the detriment of SNSs information consumers who have no choice.

CHAPTER III

Research Methodology

Chapter Overview

In this chapter, I discuss the research methods I used to compose the Comprehensive Literature Review (CLR) from a dialectical pluralism 2.0 stance (Johnson, 2011). Onwuegbuzie and Frels (2016) defined the CLR as,

> … a culturally progressive approach involving the practice of documenting the process of inquiry in the current state of knowledge about a selected topic as related to philosophical assumptions/beliefs, inquiry (method), and guidelines of practice (organization, summarization, analysis, synthesis, reflection, and evaluation), resulting in a product that is a logical argument of an interpretation of relevant published and/or unpublished information on the selected topic from multi-modal texts and settings that primarily comprise five MODES (i.e., Media, Observation(s), Documents, Expert(s) in the field, and Secondary sources). (p. 19)

A CLR differs from a systematic literature review in that a systematic literature review only examines what is available within existing databases. Although the systematic literature review aims to present the findings in as neutral and unbiased a way as possible, a systematic literature review is still lacking contemporary and relevant findings that exist in gray literature, social media posts, blogs, news, media, etc. A CLR is the solution to address the gaps left by a systematic literature review (Onwuegbuzie &Frels, 2016).

Research methods are the decisions and steps scholars follow to produce research and make studies understandable to the reader (Johnson & Christensen, 2014). The current CLR follows Onwuegbuzie and Frels (2016) *Seven Steps to a Comprehensive*

Literature Review methodological framework with an additional Step 8 that I am including to engage in further discussion about privacy literacy 2.0. In this chapter I describe the three main phases of the CLR: Exploration, Integration, and Communication. The Exploration Phase includes the Steps 2-5: Initiating the Search, Storing and Organizing Information, Selecting/Deselecting Information, and Expanding the Search to MODES (Media, Observations, Documents, Expert, Secondary data). The Integration Phase (Step 6) shows Analyzing and Synthesizing Information. Step 7 is the Communication Phase, which explains the writing and communication of the report. Step 8 is an additional step that I added to discuss the findings and implications. Figure 3 maps the process of the CLR and shows the steps I followed as inspired by Onwuegbuzie and Frels (2016) framework for the CLR.

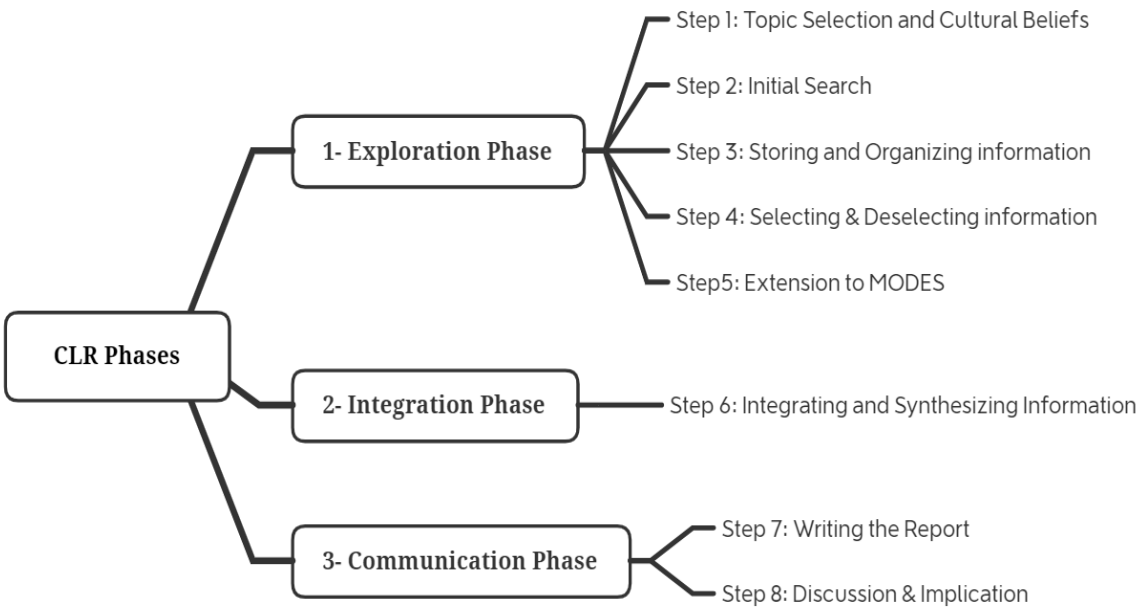


Figure 3. *Steps and Phases followed to conduct the Comprehensive Literature Review*

Chapter one delineated Step 1 and my cultural beliefs as related to my topic selection of privacy literacy. As stated in Chapter one, the goal of this CLR is to inform

educational practitioners and researchers about the scope of privacy literacy 2.0, how it relates to other disciplines, and what it takes to become a privacy literate individual from the perspective of law, technology, and education. Methodologically speaking, I aim to map privacy literacy 2.0 in three-layers: (a) the scholarly literature, (b) expert(s) opinion, and (c) the public opinion. To this end, the following research questions were set to guide this study:

1) How does the Comprehensive Literature Review process inform and develop a definition and understanding of privacy literacy around individuals' use of social networking sites (SNSs):

a. Through existing literature/scholarly work?
b. Through select expert opinion?
c. Through current legislation and select publicly available SNSs data?

Exploration Phase

Step 2. Initial Search

Following the topic selection in Step 1, in the initial search I performed a wide exploration of the topic of privacy literacy from books, past literature reviews, and scholarly articles. This step contained sub-tasks, such as locating research databases, conducting the initial search with major keywords, storing and reading initial findings, and generating a focused list of keywords. It is important to mention that I documented the process through an audit trail (Halpern, 1983; Onwuegbuzie & Frels, 2016) as part of my scholarly responsibility, "...which is adhering to best practices through documenting and reflecting on decisions made throughout the CLR process" (Onwuegbuzie & Frels, 2016, p. 86).

Task 1. To start the process, I identified the appropriate databases to begin my initial search. Because "… fields and disciplines are recognized by the academic journals in which research is published" (Onwuegbuzie & Frels, 2016, p. 88), it is important to first identify a series of databases that will yield the most appropriate information for a given field and discipline. In order to make sure that I covered the widest possible range of databases that would yield pertinent and relevant literature later in the process, Onwuegbuzie and Frels (2016) recommended doing a first level search of (a) basic library subscription databases and (b) public Internet sources. As suggested by Onwuegbuzie and Frels (2016), public Internet sources include (a) subject directories; (b) search engines; and (c) metasearch engines. Performing initial searches within these larger databases enables the later narrowing of the topic, as these databases will yield information on the types of journals and discipline-specific databases to use in the refined search stages later.

In order to meet the requirement of using both basic library subscription databases and public Internet sources, for my first level searches I selected the Sam Houston State University (SHSU) Newton Grisham Library's Engine Orange with no limiters to years or type of document. In parallel, I used the same keywords through Google Scholar for a metasearch engine search as well as Microsoft Academics for my search engine search, which was particularly helpful in obtaining the most cited articles.

As a step to begin to narrow down the search, initial search terms should be determined and then used for a first level search in the selected search engines. Table 4 shows the list of the initial search terms/keywords and the limiters I used across Engine Orange, Google Scholar, and Microsoft Analytics. The initial searches in Engine Orange,

Google Scholar, and Microsoft Academics allowed me to further refine the subject-specific databases needed to conduct the first-level extensive search, which will be explained in Task 2.

Table 4. *Sample of the first level search and keywords for five of the searches*

#Search ID	Keywords	Search Engine	Limiter	Results/ Hits
S1	"Privacy literacy"	Engine Orange Microsoft Aca. Google Scholar	No limiters	3.394 51 546
S2	"Social networking sites" AND "privacy"	Engine Orange Microsoft Aca. Google Scholar	No limiters	40,000 88 60,000
S3	"Digital privacy literacy"	Engine Orange Microsoft Aca. Google Scholar	No limiters	5 322 19

S4	"Social media privacy"	Engine Orange Microsoft Aca. Google Scholar	No limiters	3,393 392 2,240
S5	"Privacy concern"	Engine Orange Microsoft Aca. Google Scholar	No limiters	12,424 233 20,500

Task 2. In Task 2, I performed the first-level extensive search, and based on my previous readings (i.e., those completed before the start of the CLR process) in the field of privacy literacy and media and information literacy. I gathered the following keywords for the initial search: "privacy literacy," "Facebook AND "privacy," "online privacy" AND "college students," "social media privacy" AND "college students," "social media" AND "privacy management," "social networking sites" AND "privacy," "Social media" AND "privacy concern" , " information privacy" AND "law."

I used these keywords with the SHSU's online library Engine Orange, Google Scholar, and Microsoft Academics to further refine the subject-specific databases that would be used for the first-level extensive search. For instance, on Microsoft Academics, the search only showed one article related to privacy literacy with 238 citations, which to

date was the highest cited article that I had come across in my searches. Table 5 shows a sample of each pair of keywords that I searched, the limiters I used, the resulting hits, the database I used for the search, and the number needed through statistical sampling theory (Krejecie & Morgan, 1970) in order to obtain a representative sample.

Table 5. *Audit trail sample from Communication and Mass Media Complete*

S#	Keyword	Hits	SS
	Database: Communication & Mass Media Complete Scholarly (Peer Reviewed) Journals; Date: 2013-2019		
S1	AB “Facebook” AND AB “privacy”	78	65
S2	AB “information privacy” AND AB “law”	1	1
S3	AB “social media” AND AB “privacy concern”	4	4
S4	AB “social networking sites” AND AB “privacy”	24	24
S5	AB “Social media” AND AB “privacy management”	9	9
S6	AB “social media privacy” AND AB “college students”	0	0
S7	AB “online privacy” AND AB “college students”	2	2
S8	AB “privacy literacy”	2	2
	Total Studies		**107**

Based on sampling theory, I also narrowed down the main subject-specific databases that would be used for the CLR. Table 6 displays the main subject-specific

databases I used for the initial search with the total articles I obtained from each of the databases through sampling theory.

Table 6. *Databases for initial search and statistically selected articles*

Folder name	**Number of stored articles**
Academic search complete initial search	306
Privacy initial search	90
Library and Information Science initial search	45
All databases Privacy Literacy initial search	38
Privacy Legal databases	97

Task 3. Task 3 is identified as exploring the information that resulted from the initial search in Task 2. The application of the keywords selected in Task 2, as noted by Table 4, across multiple search engines yielded findings at every search hit[11]. The search hit results were subject to a statistical sampling (see the audit trail sample in Table 5) model advanced by Krejecie and Morgan (1970). The statistically sampled articles were then downloaded (See Table 6, mentioned prior, for the sampling numbers used) and stored on Zotero 5.0., which is a local database.

I used Zotero (see Figure 4) to manage and organize information. In order to generate more keywords about privacy literacy, I read six articles from each of the total results of the statistically sampled articles I gathered across each of the first-level initial

[11] A search hit is when I open a search engine, type the keywords and hit search. The number of article obtained are considered the search hit results.

searches from Engine Orange, Google Scholar, and Microsoft Academics (i.e., initial search). Guest, Bunce, and Johnson (2006) posited that analyzing a minimum of six documents or interviews might be effective to generate meaningful insights and that 12 documents or interviews will yield enough data to ensure saturation and variation. For this CLR, reading the first 18 articles of each search (i.e., six each from Engine Orange, Google Scholar, and Microsoft Academics) was meant to generate focused key terms around the topic of privacy literacy. Tables 7, 8, and 9 list the 18 initial articles that I read in full to generate additional keywords about privacy literacy for the focused literature review search.

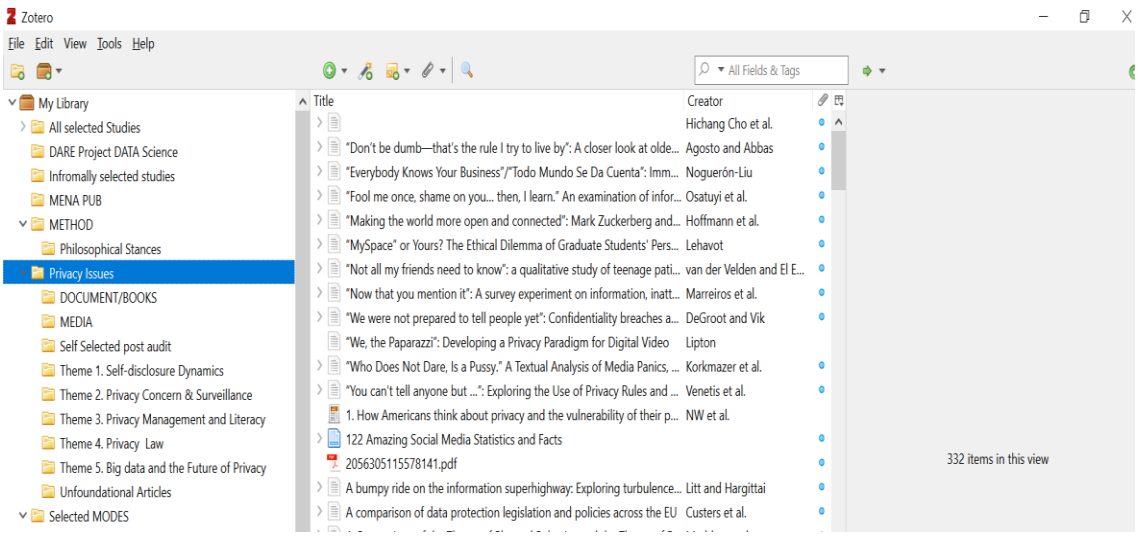


Figure 4. *Zotero initial search findings and storage under "Privacy Issues" folder*

The tables contain the author, the year of publication, and the number of times the article had been cited as of June 2018, which was when I started researching the topic of privacy.

Table 7. *List of articles I read entirely from Engine Orange search engine*

Author and Year	**Article Title**	**Number of times cited**
Noguerón-Liu, S. (2017)	Everybody knows your business	75
Wissinger, C. L. (2017)	Privacy literacy: From theory to practice	8
Baruh, L., Secinti, E., & Cemalcilar, Z. (2017).	Online privacy concerns and privacy management: A meta-analytical review	90
Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016).	Age differences in privacy attitudes, literacy and privacy management on Facebook	40
Hargittai, E., & Marwick, A. (2016).	"What can I really do?" Explaining the privacy paradox with online apathy.	115
Antón, A. I., Bertino, E., Li, N., & Yu, T. (2007)	A roadmap for comprehensive online privacy policy management.	100

Table 8. *List of articles I read entirely from Google Scholar search engine*

Author and Year	**Article Title**	**Number of times cited**
Sánchez Abril, P., Levin, A., & Del Riego, A. (2012)	Blurred boundaries: Social media privacy and the twenty-first-century employee.	296
Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013)	Teens, social media, and privacy.	791
Madden, M. (2012)	Privacy management on social media sites.	351
Marwick, A. E., & Boyd, D. (2014)	Networked privacy: How teenagers negotiate context in social media.	542
Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011)	Negotiating privacy concerns and social capital needs in a social media environment.	284
Zheleva, E., & Getoor, L. (2009)	To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles.	609

Table 9. *List of articles I read entirely from Microsoft Academics search engine*

Author and Year	Article Title	Number of times cited
Besmer, A., & Lipford, H. R. (2010)	Moving beyond untagging: photo privacy in a tagged world.	275
Lipford, H. R., Besmer, A., & Watson, J. (2008)	Understanding privacy settings in Facebook with an audience view.	270
Park, Y. J. (2013)	Digital literacy and privacy behavior online.	238
Beresford, A. R., & Stajano, F. (2003)	Location privacy in pervasive computing	1925
Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015)	Security, privacy and trust in Internet of Things.	1049
Stalder, F. (2009)	Privacy is not the Antidote to Surveillance.	182

Task 4. Task 4 is defined by Onwuegbuzie and Frels (2016) as the point in defining key terms for refining the search process inside the selected databased. These key terms are contextualized through reading a sampling of articles that has provided saturation and variation (see Guest, Bunce, and Johnson, 2006) as evidenced in Tables 7, 8, 9. Following Task 3, I read the selected articles entirely and created a list of revised keywords for the focused search. Following Onwuegbuzie and Frels' (2016)

recommendation, the reading task was done to generate operational keywords (those collected from books and articles) and constitutive keywords (derived from encyclopedias and/or thesaurus search). Table 10 lists these additional keywords that were created during Task 4.

Table 10. *Additional list of focused keywords*

Search ID	**Keywords** Database: Com. & Mass Media Complete Peer Reviewed Journals; Date: 2013-2019
S1	privacy and big data
S2	social media and big data
S3	social networking sites and surveillance
S4	social media and surveillance
S5	Facebook and privacy setting
S6	digital privacy and Law
S7	privacy law
S8	social networking sites and privacy concern
S9	social media privacy
S10	Facebook and privacy concern
S11	digital privacy behavior
S12	GDPR
S13	self-disclosure and privacy
S14	privacy calculus
S15	social media and privacy settings
S16	internet of things and privacy

S17	privacy paradox

Task 5. Task 5 is defined as focusing the search in order to lead to a strategic representation of selected literature. After conducting tasks 1-4, I selected a number of databases from the disciplines of education, psychology, computer science, sociology, and mass communication that stemmed from the most useful databases, as indicated in Table 6, using the keywords from Table 10 (with specific limiters as discussed next). Table 11 displays a sample audit trail of the focused search using Communication and Mass Media Complete Database.

Using operational and constitutive keywords, I performed a focused search across all databases (see Table 6 for databases) with limiters of scholarly peer reviewed journal articles and years 2013 to 2019. I limited my searches to five years, because privacy is a technology-sensitive field that develops rapidly. Table 11 details the focused search.

Table 11. *Sample of focused search using focused keywords*

Search ID	**Keywords** Database: Com. & Mass Media Complete Peer Reviewed Journals; Date: 2013-2019	**Hits**	**SS**
S1	privacy and big data	32	28
S2	social media and big data	43	40

S3	social networking sites and surveillance	9	9
S4	social media and surveillance	47	40
S5	Facebook and privacy setting	4	4
S6	digital privacy and Law	2	2
S7	privacy law	7	7
S8	social networking sites and privacy concern	0	0
S9	social media privacy	105	82
S10	Facebook and privacy concern	2	2
S11	digital privacy behavior	0	0
S12	GDPR	5	5
S13	self-disclosure and privacy	15	14
S14	privacy calculus	9	9
S15	social media and privacy settings	5	5
S16	internet of things and privacy	22	19
S17	privacy paradox	14	14
	Total		**280**

Every result from a keyword hit was statistically sampled according to Krejecie and Morgan (1970) methods for determining sample sizes with non-probabilistic samples. The listing of statistically sampled articles was stored on my EBSCO library account. Table 12 shows the organization of my EBSCO account and the total of articles obtained using focused keywords across databases.

Table 12. *Organization of my EBSCO library account: Focused-search files*

Database	**Statistically Sampled Articles**
Education Source	20
Mater File Premier Database	15
Library & Information Science Source	21
Legal Source & Legal Information Center & Legal Collection	70
ACM Digital Library	54
Com. & Mass Media Complete	280
Computer Source	85
Total focused search articles	**545**

Step 3. Storing and Organizing Information.

Storing and organizing information is an important step in the entire CLR process. The initial storage was in my EBSCO library account. The account had multiple folders named after the databases I searched (see Table 12). However, each folder contained the total number of articles that were statistically sampled. The articles (N= 545) were

subjected to selection and deselection criteria, and were eventually stored locally using Zotero 5.0.

Step 4. Selecting and Deselecting Information

Selection and deselection of articles was completed by interrogating each article with the following list of criteria. These criteria were inspired by my personal readings as well as the initial search findings from Task 1, Task 2, Task 3 and Task 4. The criteria for selecting or deselecting articles for inclusion in my CLR were guided by these four yes/no questions:

1. Is the research about digital privacy behavior, skills, and/or concerns on SNSs?
2. Is the research about the companies' privacy regulation/suggestions/practices?
3. Is the research about privacy literacy?
4. Does the article provide a sound argument through its method, design, and analysis?

A "yes" to any one of the questions indicated that I should store the article in the appropriate folder in Zotero 5.0. A "no" to all four of the questions indicated that I classified the article as 'deselected work.'

Rationale for selection criteria. The rationale for the first criterion was that the CLR may stand as a foundation for further educational content creation. The second criterion was set to capture the practices of one of the main players in online privacy that is the tech companies (e.g., Facebook and Google). The third criterion reflected the core skill investigated in this CLR, which is privacy literacy. The last criterion was the basis for the selection of any research work, a sound method and design. A solid research and argument were important to increase the validity of the articles as well as the reliability of the CLR findings.

I applied the four selection and deselection criteria to the statistical samples of articles that were stored in my EBSCO library account (N= 545). I read the abstract of each article from the statistical sample to see if it would be selected or deselected for the first-stage full article review. A total of 225 article abstracts were read and selected for first stage full-article review.

After applying the initial selection and deselection criteria to these 225 articles, I selected a total of 145 articles to read in full for later consideration of inclusion in the CLR. A more focused selection and deselection followed at a later stage and the process became iterative where initially deselected articles were later considered for selection based on new findings or challenges to theoretical or conceptual understandings. This latter stage of selection and deselection was completed by uploading the articles (n=145) to QDA Miner Lite and further deselected articles that did not match the selection criteria and obtained a sample of 73 for manual mapping (see figure 22). The final stage of mapping yielded a final sample of 43 articles that constructed the core of this CLR (see figure 23 for a map of the entire process).

Step 5. Extension to MODES

From a dialectical pluralism 2.0 stance (Johnson, 2011), it is important to listen to multiple perspectives and include different standpoints of the same topic. The comprehensiveness of this work lies in the expansion to other sources of knowledge. As we live in an age of technology, many researchers and institutions, as well as individuals that are invested in the field of privacy literacy, share a wealth of up-to-date content using different media platforms. Expanding the search to include such information, the MODES (Media, Observations, Documents, Expert Interviews, and Secondary Data

Sources), increases the comprehensiveness of the literature review (Onwuegbuzie and Frels, 2016). Figure 5 shows the interface of the Zotero database and the organization of the MODES into files.

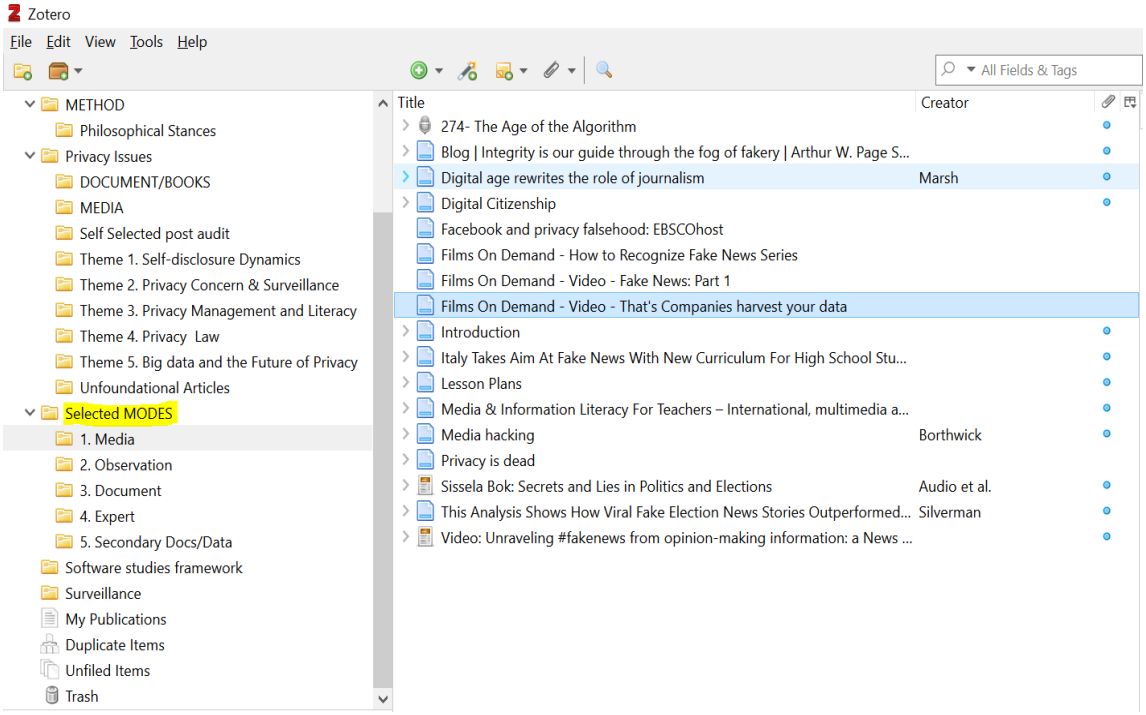


Figure 5. *The interface of the Zotero database and the organization of the MODES into files*

For Media, I consulted the social video sharing sites of YouTube, Netflix, and Amazon Prime Video. For Observations, I used my anecdotal reflections from my teaching assistantship at SHSU as well as from my guest lectures to students from a university in Northeast United States as Observations. For Documents, I used government documents and legal reports, such as the U.S. State Department *National Privacy Research Strategy Report* (2016). For Experts, I interviewed six expert/scholars and practitioners from the field of education, research, law, and policy making. For Secondary Data, I used data from a public conversation on Facebook around the

Zuckerberg-Senate hearing and I used the Facepager application to harvest the metadata from Facebook. Table 13 shows the listing of MODES used in the CLR.

Table 13. *The MODES used in the CLR*

MODES	Number	Example
Media	17	*Black Mirror* series on Netflix
Observation	4	Students' reflections from a class I co-taught on Privacy Literacy
Document	65	UNESCO report Horton, F. W. (2007). *Understanding information literacy: A primer.* Paris, France: Information Society Division, Communication and Information, UNESCO.
Expert	6	Expert Interview, e.g., with Tom Liam Lynch, a software theorist.
Secondary data	22	SNSs meta-data collected using Facepager.

Facepager is a tool developed by Till Keyling[12] from the University of Munich, Germany that allows users to gain access to various metadata from Facebook. Figure 6 shows the Facepager interface. In order to think through the metadata that I received from

[12] Read about Facepager here https://www.alumniportal-deutschland.org/en/science-research/news-from-science/facepager-till-keyling-social-media/

Facepager, I adhered to the five principles of the ontological imperative framework (Gerber & Lynch, 2017; Lynch & Gerber, 2018; Gerber, Lynch, & Onwuegbuzie, forthcoming) in order to deconstruct the data returned by the API key to ensure transparency with data collection and analysis. The five principles of the ontological imperative set out by Lynch and Gerber (2018) are:

(1) What digital tools, systems, and services are at play in my study? Who created them and why?

(2) What data do these digital tools, systems, and services render?

(3) What hidden limitations might there be to the data rendered via these digital tools, systems, and services?

(4) What are the epistemological implications of this ontological analysis?

(5) What are the axiological implications of this ontological analysis?

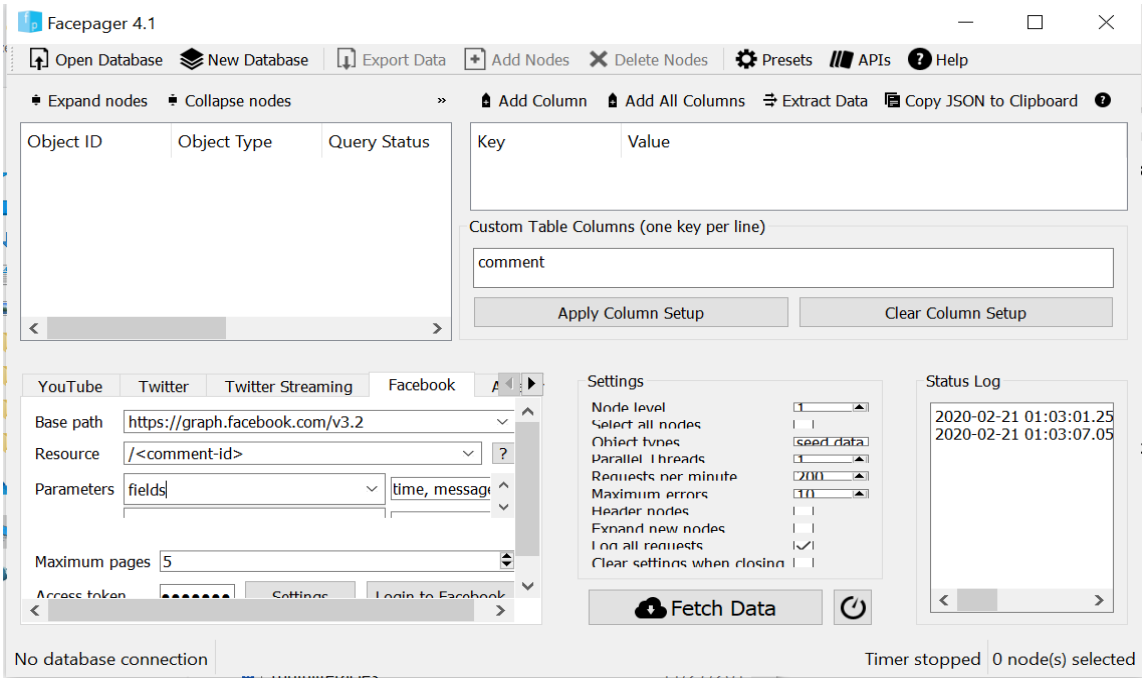


Figure 6. *The interface of the Facepager API used to scrape Facebook comments*

Oral history and expert opinion. Personal communication with experts in the field (i.e., someone directly related to the subject matter, literature production, and/or concept under study) can yield greater insight on the topic under discussion (Morris, Onwuegbuzie, & Gerber, 2018). Experts can engage in conversation (through methods of personal communication) about the topic for which they are an expert. These conversations are not used in any type of systematic coding and analysis, rather they are conversations done solely to confirm or dispute ideas presented in the literature (e.g., commentary on an article written by the expert or commentary on a product designed by the expert). Expert "… interviews are only used to support the literature and are not analyzed systematically for generalizability (Morris, Onwuegbuzie, & Gerber, 2018, n.p)." The Common Rule states that this type of activity (i.e., personal communication with experts) does not fall under Federal Regulations because it is not part a systematic and generalizable research process. In fact, the Common Rule illustrates that, "Scholarly and journalistic activities (e.g., oral history, journalism, biography, literary criticism, legal research, and historical scholarship), including the collection and use of information, that focus directly on the specific individuals about whom the information is collected"[13], are not considered forms of human subjects research.

Therefore, in the case of experts, I engaged in interviewing and discussing the topic of privacy literacy with six key scholars in law and legal studies, privacy,

[13] https://www.hhs.gov/ohrp/regulations-and-policy/requests-for-comments/draft-guidance-scholarly-and-journalistic-activities-deemed-not-to-be-research/index.html

technology and education. Table 8 lists the experts, their titles/expertise, and the dates of the interviews. I gained permission to cite our conversation as personal communication in my publications. I contacted each expert, asked them if I could engage in a conversation on the topic, and then set up a videocall for the conference as well as face-to-face meetings. After each conference call or meeting, I allowed the experts to see the full transcript and edit or redact any information that they wanted to change.

Table 14. *Expert witnesses, affiliation, and dates of the interviews*

Expert Name	**Affiliation**	**Date of Interview**
Caitlin Fennessy	Research Director at the International Association of Privacy Professionals (IAPP)	September 5, 2019
Paul Eaton	University professor Educational leadership and social media expert	February 10, 2020
Ian O'Byrne	University professor Educational technology researcher and privacy scholar	February 12, 2020
Hannah R Gerber	University professor, Digital literacies and software theory expert	February 12, 2020
Tom Liam Lynch	Educational researcher and software theorist	February 18, 2020

Renee Lowe Williams	Attorney at Law specialized in Healthcare law	February 24, 2020

Integration Phase: Analyzing/Synthesizing Information

Step 6. Integrating and Synthesizing Information

The Integration Phase included multiple tasks: (a) reading the articles that I stored in Zotero 5.0 in their entirety for a focused selection and deselection process; (b) analyzing the selected articles to discern potential literature gaps; (c) mind-mapping the articles as part of the thematization process; (d) organizing the articles into folder with themes; and finally, (e) plan for the CLR writing with the inclusion of MODES. The goal of the Integration Phase was to analyze and synthesize information in order to report on it in a final writing.

Task 1. I engaged in the initial selection and deselection of articles, and stored the selected articles in Zotero 5.0. I then read the articles and made a second round of selection and deselection that I call a focused selection. That enabled me to discard any irrelevant information before deep-level analysis.

Task 2. I installed QDA Miner Lite[14] and analyzed the abstracts of the selected articles' according to the following:

1. Topics researched.

[14] A Provalis software for qualitative and quantitative data analysis. For more details, please visit https://provalisresearch.com/products/qualitative-data-analysis-software/

2. Methods used, including instrument.
3. Theories used.
4. Population/sample type.

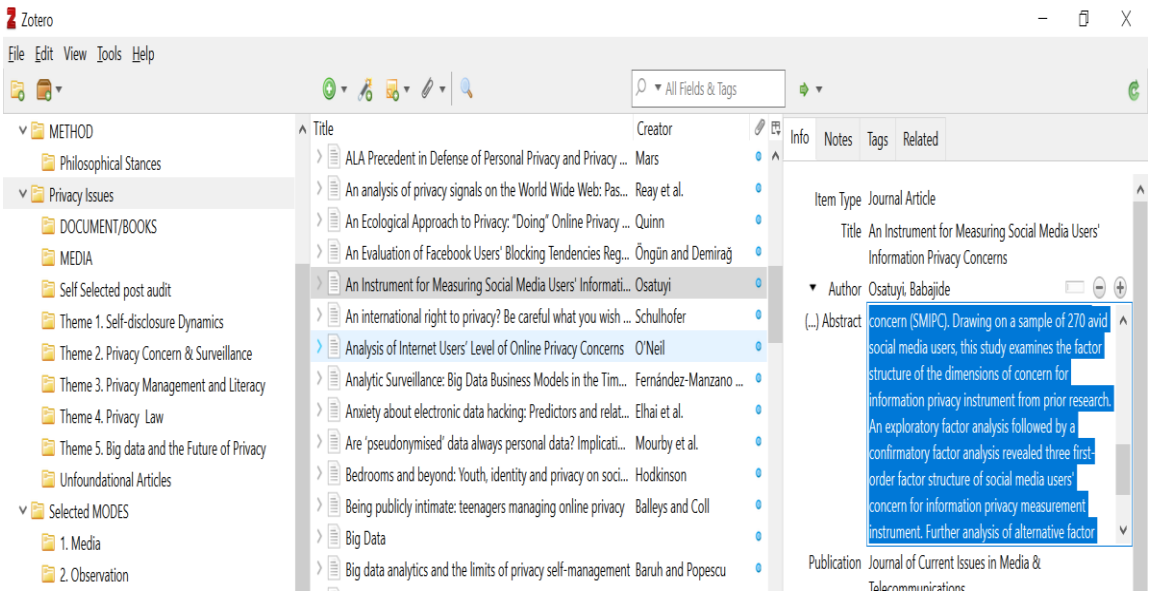


Figure 7. *Abstract reading on Zotero before copying to QDA Miner Lite*

To report this information, I used Frequency Analysis measure in order to understand possible gaps in privacy literacy scholarship with regards to topic, method, theory, and population. Figure 7 shows the frequency of topics; Figure 8 shows the percentages of methods; Figure 9 shows the frequency of theories; and Figure 10 shows the breakdown of population/sample studied.

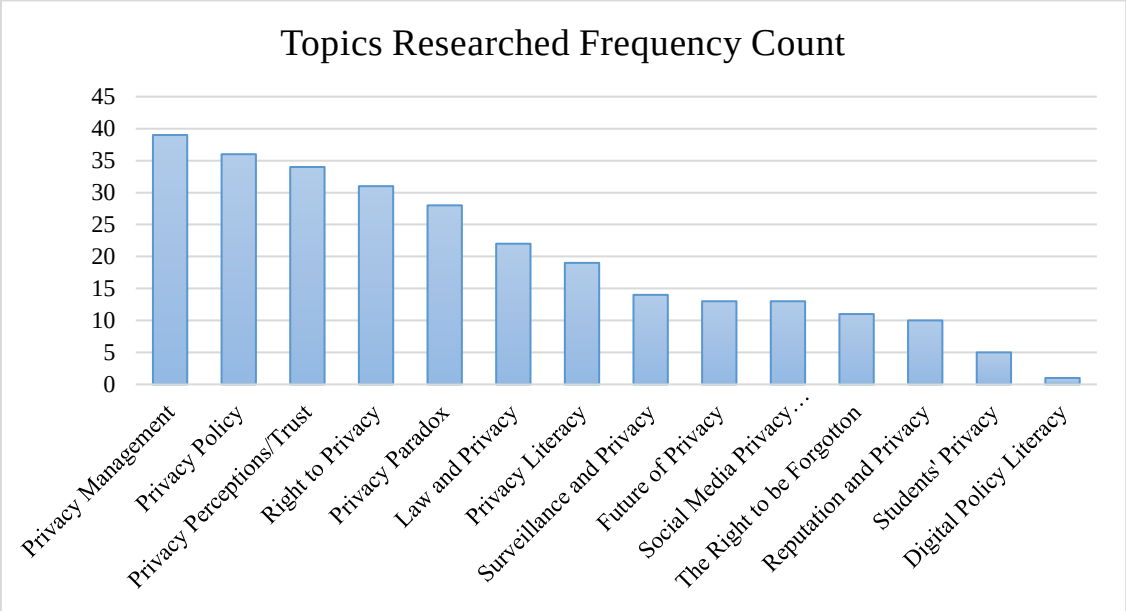


Figure 8. *Frequency of topics researched in literature*

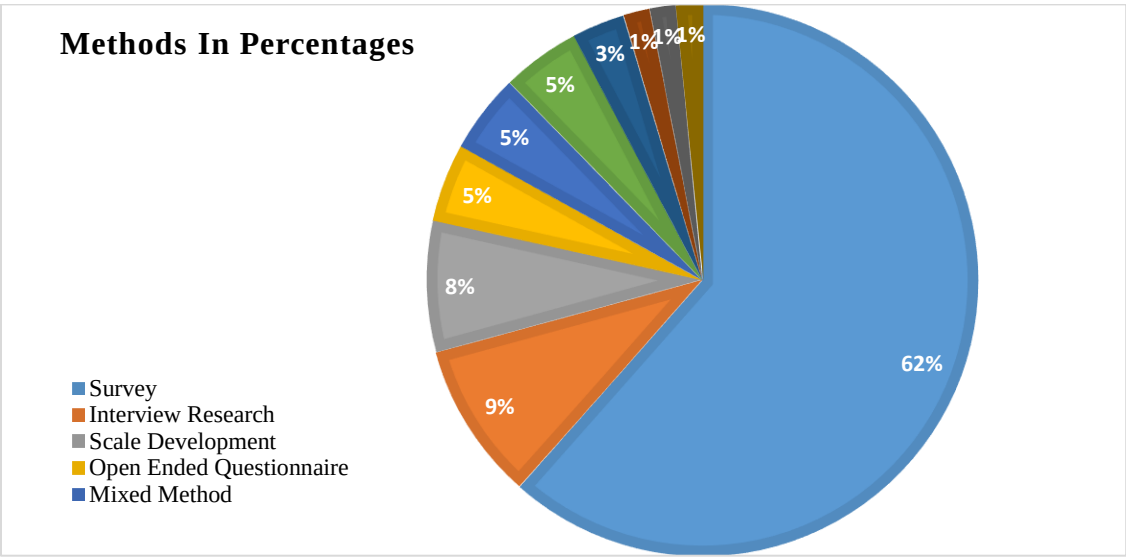


Figure 9. *Methods and instruments used to research privacy literacy*.

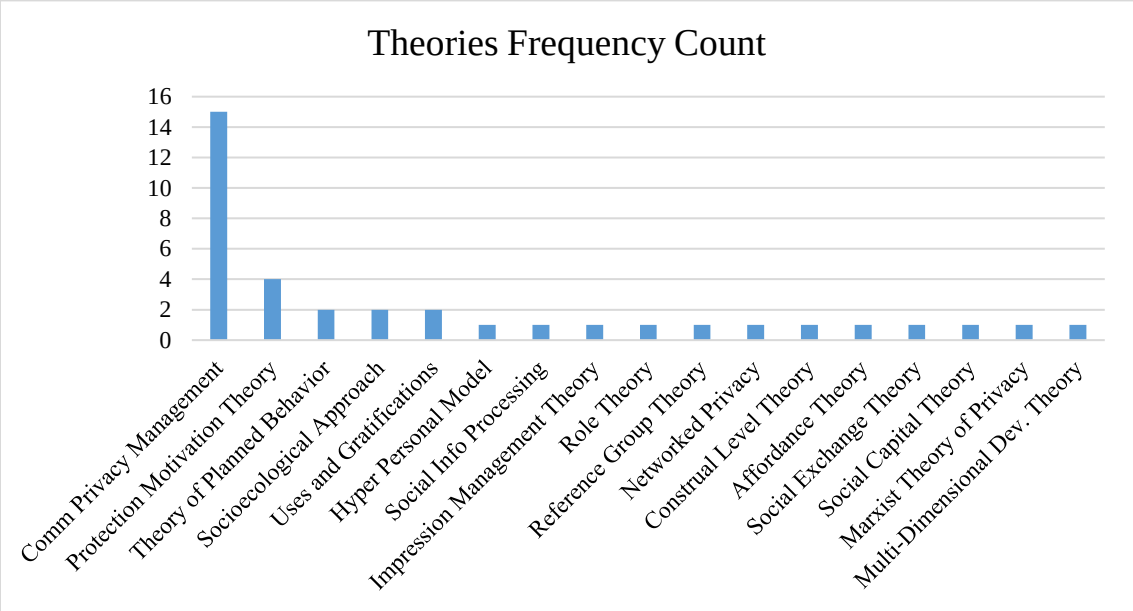


Figure 10. *Frequency count of the theories used in privacy literacy research*

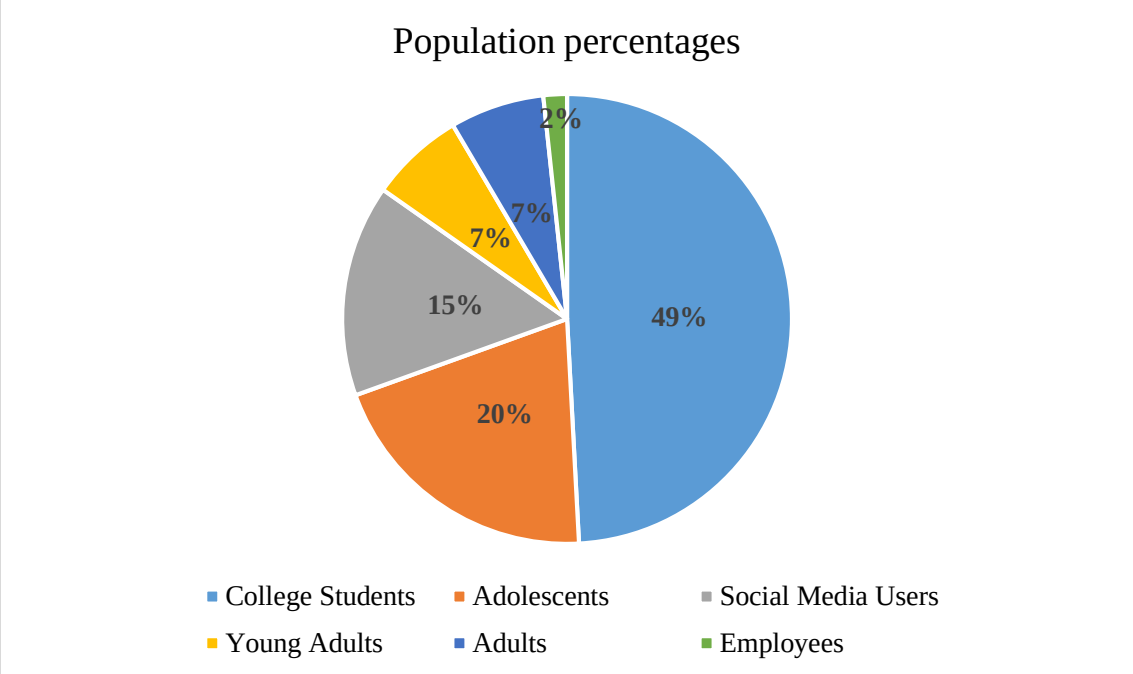


Figure 11. *The breakdown of population/sample studied.*

The frequencies and percentages of topics, methods, theories, and populations were conducted in my initial stage (Braun, Clarke, Hayfield, & Terry (2019) in order to identify possible gaps in the literature.

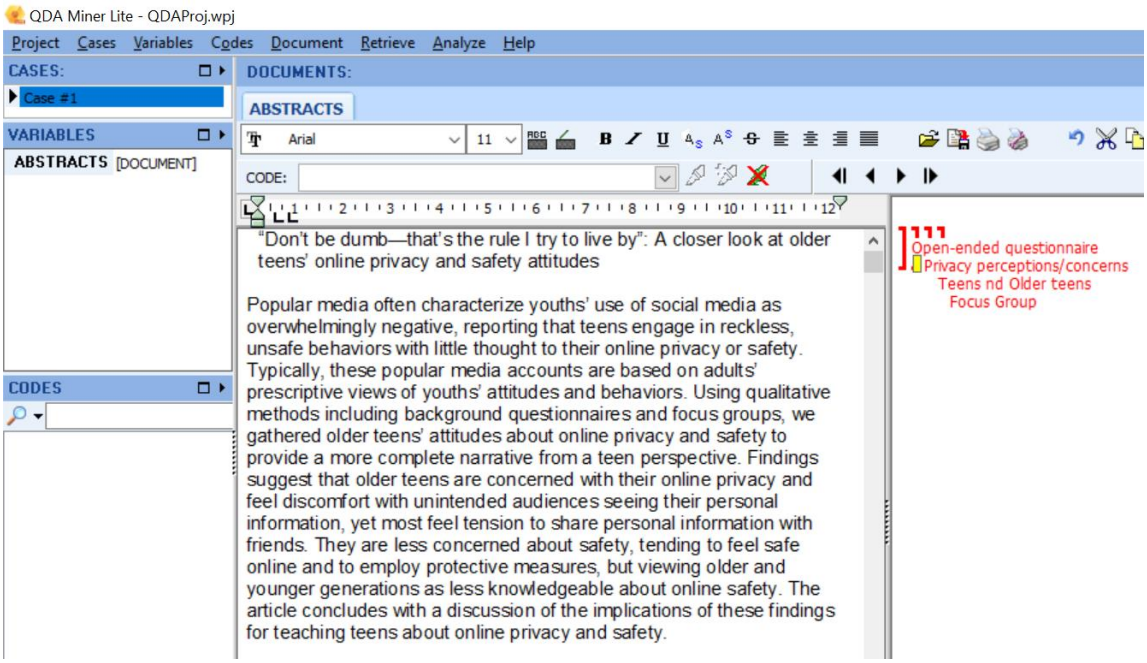
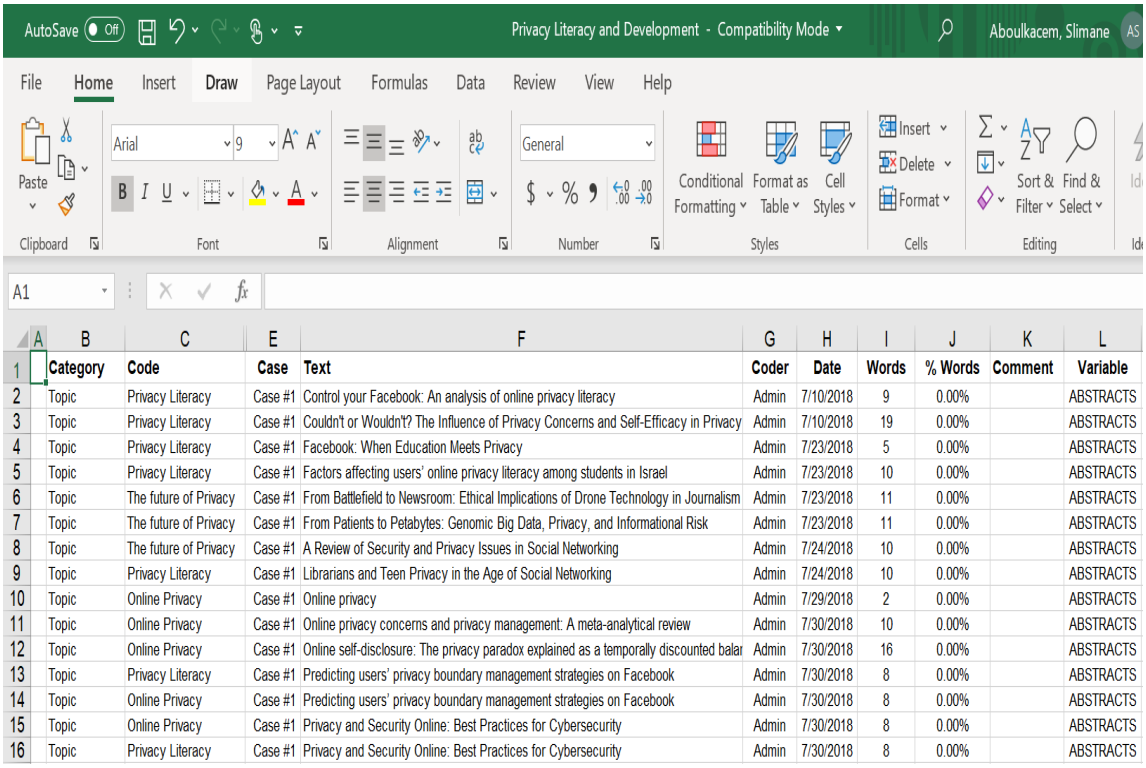


Figure 12. *The process of coding the abstracts on QDA Miner Lite*

As an example of the QDA Miner Lite coding and frequency analysis, charting these gaps allowed me to see that the most used method/instrument to investigate the topic of privacy literacy was survey research. For example, surveys (n= 40) appeared to be the standard method used to measure the construct of privacy literacy. The benefit of using surveys is time efficacy, wide reach of populations, and it can report on multiple aspects about the participants at once such as thoughts, feelings, values, and best practices (Johnson & Christensen, 2014). In a meta-synthesis research, Kokolakis (2017) made a distinction between systematic and heuristic processing of privacy related research. The researcher argued that participants' responses to privacy management questions in surveys are a result of the participants' systematic/logic processing; however, individuals behave differently in reality as a result of heuristic processing, which involves multiple biases and changes from a livable situation to another. Therefore, when dealing with multifaceted topics that are sensitive to culture and other

factors, it is important to not solely focus on self-reporting research protocols, i.e., surveys. Given that surveys are the primary method, it can be evidenced that perhaps future research should examine privacy literacy from different angles and use different methodologies, which I will explore further in Chapter VI.

Task 3. For the sake of synthesizing information, I stored article titles/studies with their relevant codes that I obtained from QDA Miner Lite on an Excel sheet. This helped me group the studies by theme and then further mind-map every study to decide on the final themes. This was the second cycle of thematizing the literature. Figure 19 shows the article counts across all themes for a general understanding of 'Privacy Literacy Development.' The 'code' column represents the codes I generated on QDA Miner Lite. The 'text line' is the title of the study and the 'variable' is the abstract, since I analyzed abstracts on QDA Miner Lite. The initial theme was privacy literacy development. It then changed to privacy management and literacy after a detailed mapping of the studies.



	Category	Code	Case	Text	Coder	Date	Words	% Words	Comment	Variable
2	Topic	Privacy Literacy	Case #1	Control your Facebook: An analysis of online privacy literacy	Admin	7/10/2018	9	0.00%		ABSTRACTS
3	Topic	Privacy Literacy	Case #1	Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy	Admin	7/10/2018	19	0.00%		ABSTRACTS
4	Topic	Privacy Literacy	Case #1	Facebook: When Education Meets Privacy	Admin	7/23/2018	5	0.00%		ABSTRACTS
5	Topic	Privacy Literacy	Case #1	Factors affecting users' online privacy literacy among students in Israel	Admin	7/23/2018	10	0.00%		ABSTRACTS
6	Topic	The future of Privacy	Case #1	From Battlefield to Newsroom: Ethical Implications of Drone Technology in Journalism	Admin	7/23/2018	11	0.00%		ABSTRACTS
7	Topic	The future of Privacy	Case #1	From Patients to Petabytes: Genomic Big Data, Privacy, and Informational Risk	Admin	7/23/2018	11	0.00%		ABSTRACTS
8	Topic	The future of Privacy	Case #1	A Review of Security and Privacy Issues in Social Networking	Admin	7/24/2018	10	0.00%		ABSTRACTS
9	Topic	Privacy Literacy	Case #1	Librarians and Teen Privacy in the Age of Social Networking	Admin	7/24/2018	10	0.00%		ABSTRACTS
10	Topic	Online Privacy	Case #1	Online privacy	Admin	7/29/2018	2	0.00%		ABSTRACTS
11	Topic	Online Privacy	Case #1	Online privacy concerns and privacy management: A meta-analytical review	Admin	7/30/2018	10	0.00%		ABSTRACTS
12	Topic	Online Privacy	Case #1	Online self-disclosure: The privacy paradox explained as a temporally discounted balar	Admin	7/30/2018	16	0.00%		ABSTRACTS
13	Topic	Privacy Literacy	Case #1	Predicting users' privacy boundary management strategies on Facebook	Admin	7/30/2018	8	0.00%		ABSTRACTS
14	Topic	Online Privacy	Case #1	Predicting users' privacy boundary management strategies on Facebook	Admin	7/30/2018	8	0.00%		ABSTRACTS
15	Topic	Online Privacy	Case #1	Privacy and Security Online: Best Practices for Cybersecurity	Admin	7/30/2018	8	0.00%		ABSTRACTS
16	Topic	Privacy Literacy	Case #1	Privacy and Security Online: Best Practices for Cybersecurity	Admin	7/30/2018	8	0.00%		ABSTRACTS

Figure 13. *Privacy management theme stored in Excel with codes, studies' count, and titles*

Figure 12 shows each major theme. Each bar is representative of number of studies included within that theme.

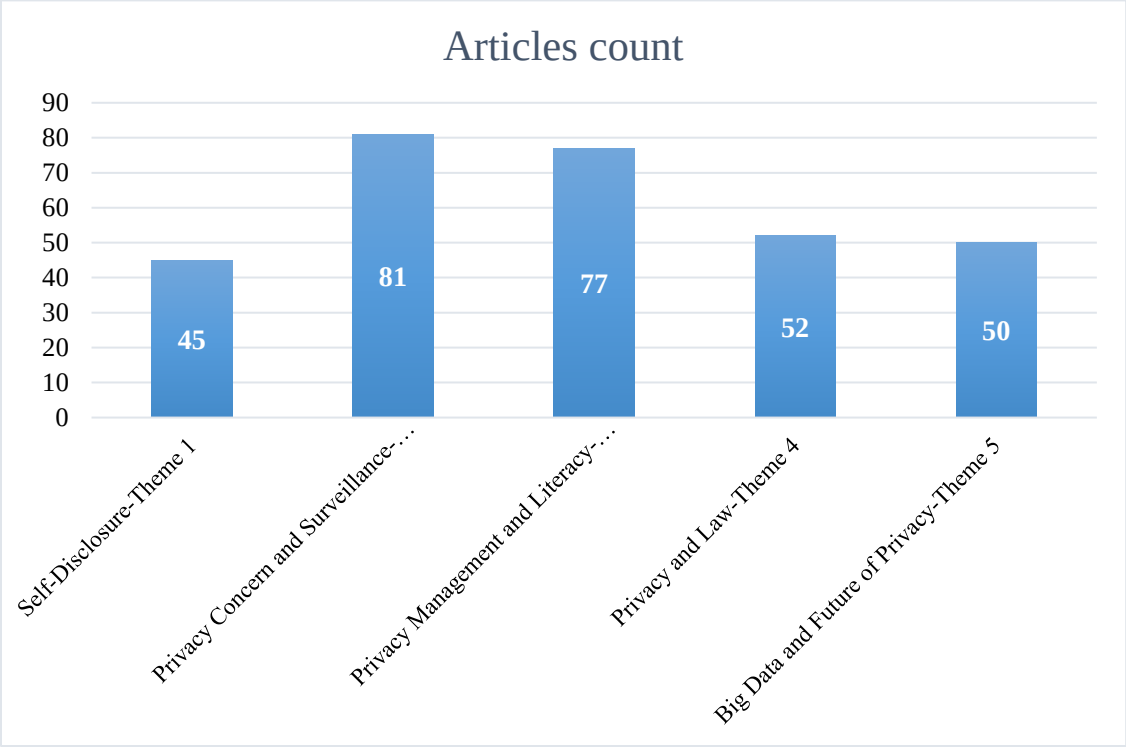


Figure 14. *Articles count for Privacy Literacy Development*

Now that I had every study/article listed with a respective theme, I then started reading and manually mind mapping every selected article (see Figure 13). The mind map was the third cycle of thematization/coding. The mind map focused on the argument made in the article, the main findings, and other details about population and instrument.

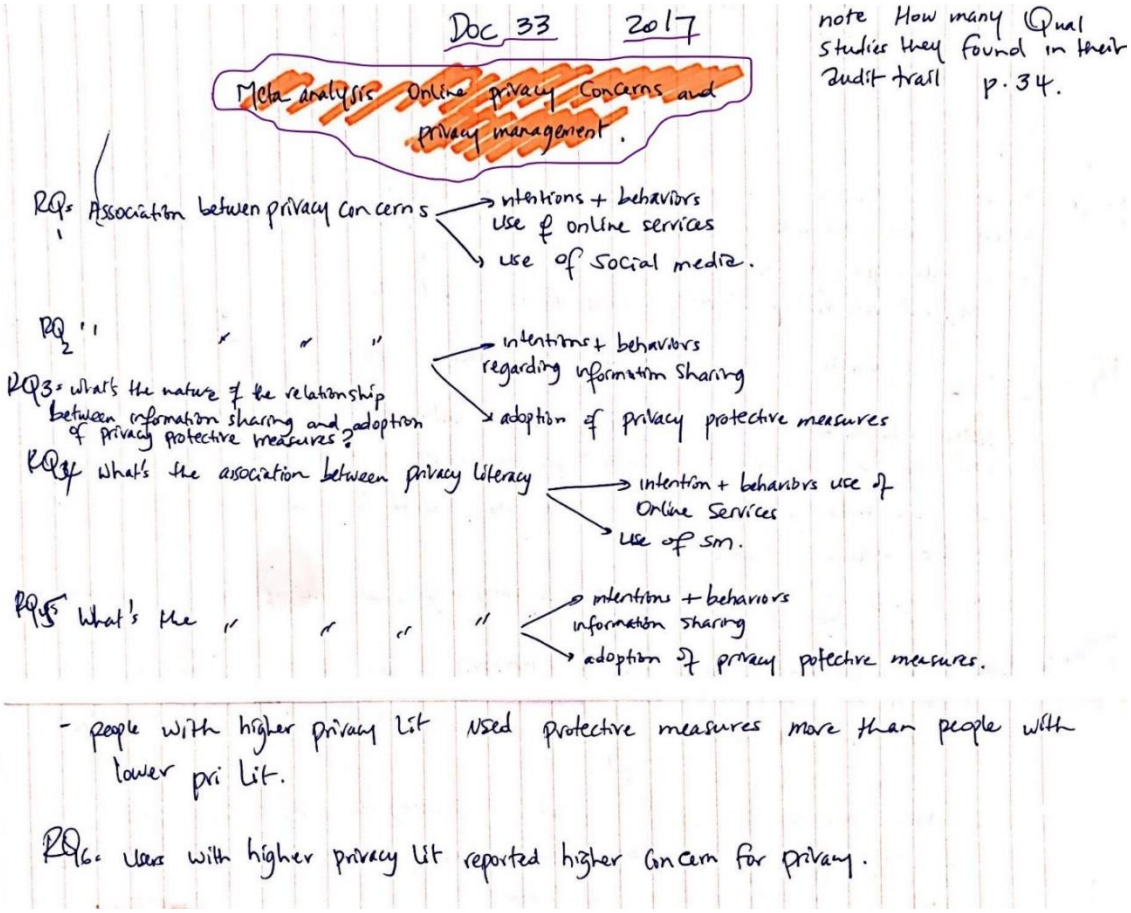


Figure 15. *Manually mapping the studies for solid arguments and main findings*

The Fourth Cycle of coding was to assign the mind maps a colored code, as shown at the top of the map. The combination of the color codes helped me see the connections and disconnections among the main studies, generate themes (Cycle Five), and reorganize my Zotero folders by theme. Cycle Six of coding was to pull out the themes, define them, and foresee the possible connections among them. The last cycle was done by revisiting the themes, as I traced them back to Cycle Four and checked for solid connections among the codes, the categories, and the themes. Table 15 shows the thematizing process of the core selected articles (n= 43).

Table 15. *Thematizing process of selected articles (n= 43), as inspired by Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019).*

Coding cycle	Process	Objective
Reading Data	Screening the abstracts for a general impression and familiarity.	To select the ones for further analysis and leave others for potential use later.
Cycle One	Transferred the abstract to QDA Miner Lite and coded for: Topic, population, method, and sample/population.	Obtained initial codes, generated frequency counts, and started getting familiarized with the data.
Cycle Two	Gathering the codes about topic category and storing them in Excel and generated initial themes.	Transferred article titles, their respective topic code, and grouped them by themes (Five initial themes).
Cycle Three	Read the articles in full and mapped the entire article focusing on main findings.	Further selection and identification of potential relationships among studies, theories, and

		implications in the field of privacy literacy.
Cycle Four	Revisited the manual maps and started looking at every map as a piece of data and assigned a code.	The code were assigned according to key findings and potential in-connections among articles.
Cycle Five	Colors were assigned to codes.	The color-coded categories were generated and turned into themes.
Cycle Six	Generate the final themes.	The themes were extracted and defined.
Cycle Seven	Verification and reverse process.	Revised the themes by tracing them back to Cycle Four and solidifying the connection between the colored categories and the themes.

Figure 14 shows the process of literature selection, initial search, focused search, selection and deselection process, as well as the extension to MODES with numbers for transparency.

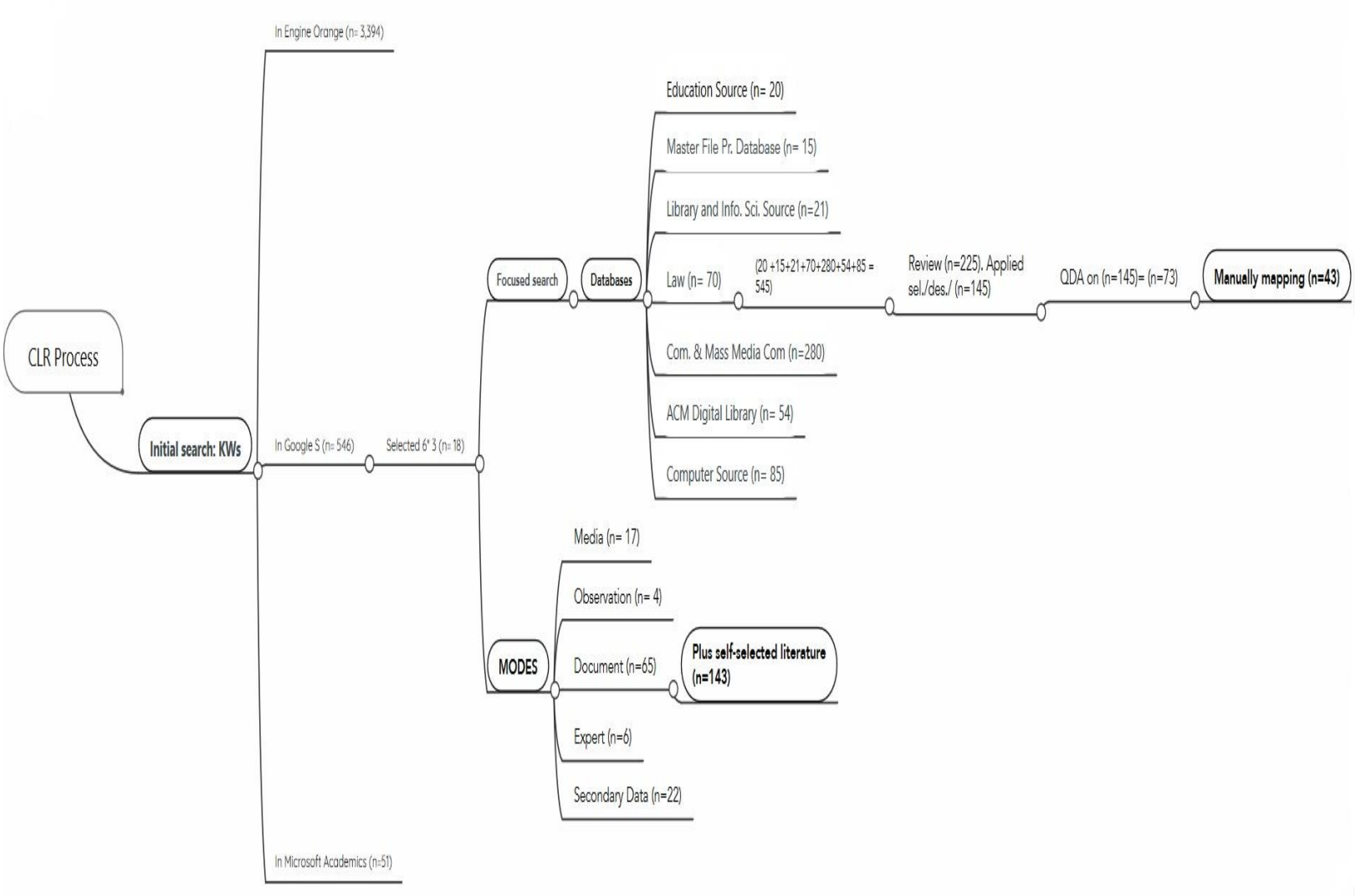


Figure 16. *Transparency and audit trail map*

Task 4. Once the themes were determined and defined, I then created folders in Zotero 5.0., and synchronized the respective articles so that they would be stored in each respective folder. The end result was five folders (i.e., according to themes).

Once the articles were analyzed and thematized, I then moved to analyze media content (e.g., YouTube, Vimeo, Netflix, etc.), expert interviews, and Facebook metadata. The expert interviews were used anecdotally to support the published scholarly work (Morris, Onwuegbuzie, & Gerber, 2018). The Facebook metadata, analyzed through the lens of the ontological imperative (Lynch & Gerber, 2018), allowed me to understand public discourse about privacy. I used Voyant Tools to analyze the data and I employed Keywords-in-Context analysis (Leech & Onwuegbuzie, 2010) to analyze the actual comments. The Facebook data solidified the main findings from the CLR.

Task 5. I used the mind maps' analysis and the QDA Miner Lite results to plan for the writing of the findings. Each theme/finding had several sub-themes. Figure 15 highlights the major five themes and first level subthemes. Each of these themes and subthemes will be fully explored in Chapter IV.

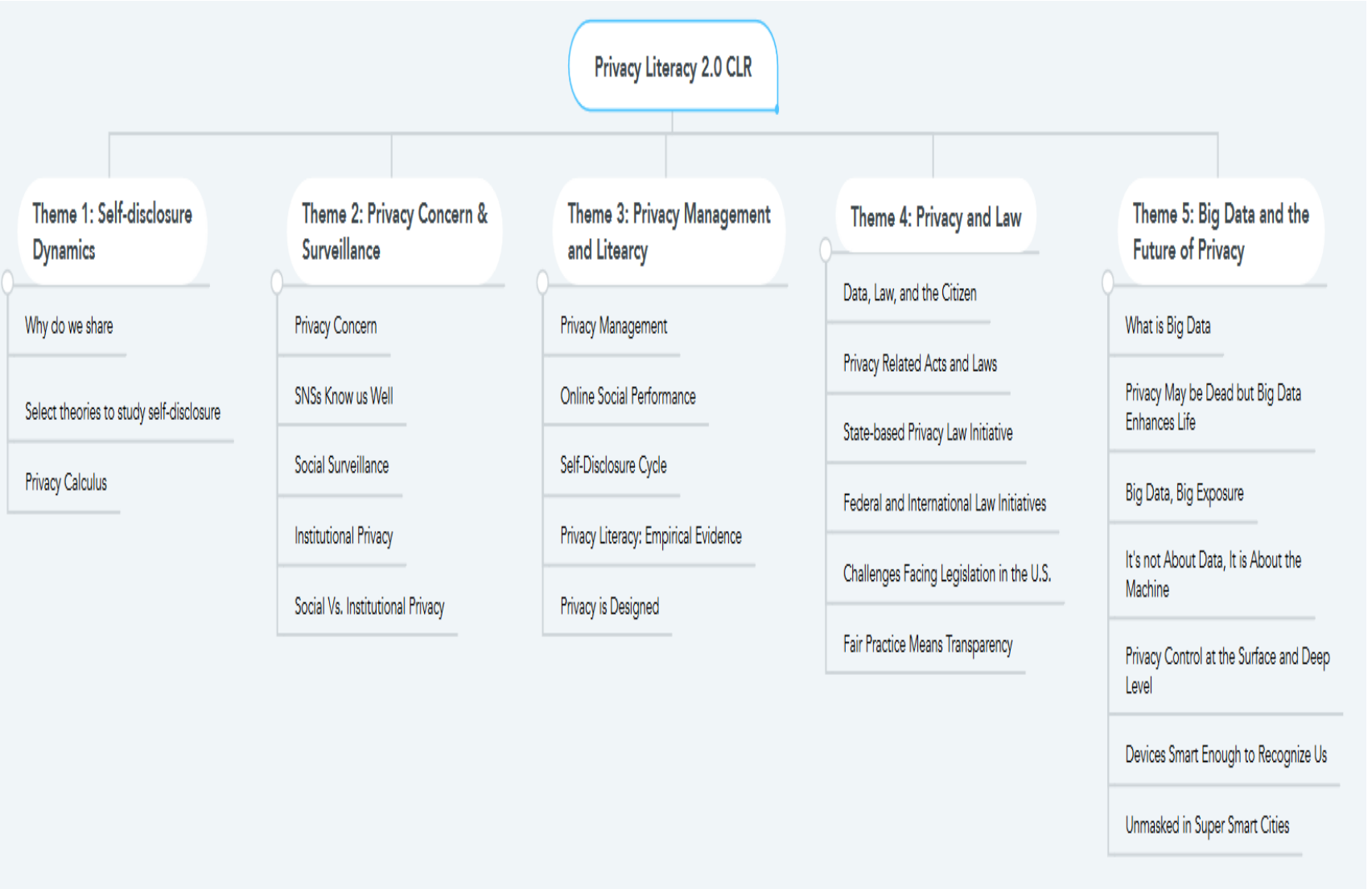


Figure 17. *A map of the major themes and their sub-themes*

Communication Phase

Step 7. Writing the Report

Step 7 is the report writing phase. This step was planned around the three layers of privacy literacy I mentioned prior: (a) the scholarly work, (b) expert opinion, and (c) public opinion. The rationale behind this plan was to deepen the analysis of privacy literacy and solidify the findings by extending them to the public (general public and expert) to include current conversations and up-to-date insights. The entire CLR will be presented through a literature review in Chapter IV and V, and visualized via a mind map in Chapter VI. The purpose of the final mind map is to highlight the main intersections and disjunctures in the scholarship of privacy literacy. The map will then introduce privacy literacy 2.0.

Step 8. Discussion and Implication

Guided by the theoretical framework of 'the right to be let alone' (Warren & Brandies 1890), the main findings were discussed and implications were drawn as relevant to privacy literacy 2.0 in Chapter VI. Main concepts, theories, and research orientations were also discussed in Chapter VI along with suggested future directions, mainly through reflective questions.

Chapter Summary

In this chapter, I described the methodological steps I followed to conduct the CLR on privacy literacy. This chapter provided details on how I wrote the CLR, as well as the procedures and methods I followed to access, select, store, and analyze information. Moreover, the chapter also outlined how I integrated up-to-date information in order to realize the goal of tackling privacy literacy in a three-layer fashion: (a) the scholarly work, (b) expert opinion, and (c) public opinion. Finally, in this chapter, I illustrated the course of action anticipated from this CLR, which is to

inform research and groups of interest, such as researchers, practitioners, and educators.

CHAPTER IV

Step 7. Writing the Report: Presentation and Analysis of the Findings

Chapter Overview

In Chapter Three, I explained the methodological procedures that I followed to select and deselect literature, as well as explained the methods I used to select the related MODES (Media, Observations, Documents, Experts, and Secondary data) that informed this CLR. This chapter aims to present the major themes I found, as well as their respective sub-themes. The presentation of my findings consists of a mix of (a) the scholarly work, (b) expert opinion, and (c) public opinion. The expert opinion is used to inform the analysis of the literature as necessary through direct quotes and paraphrasing of quotes, while the public opinion is presented as its own section in Chapter Five. The major themes that emerged from the analysis are: (a) Self-disclosure dynamics, (b) Privacy concern and surveillance, (c) Privacy management and literacy, (d) Privacy and law, (d) Big data and the future of privacy.

It is important to remind the reader of my beliefs on privacy and how I stand on the side of the spectrum, which recognizes that software controls and limits citizens' effort(s) to protect their personal information (see also software study theorists Frabetti, 2015; Kitchin & Dodge, 2011; Lynch, 2016; Manovich, 2013; Williamson, 2017). I also believe that the current model of commercial companies coding the platform/interface, establishing their own terms, policies, and navigations paths, and then transferring the responsibility of privacy and protection to the individual citizen will not work.

Theme 1: Self-disclosure Dynamics: A Closer Examination

Without self-disclosure and human digital interactions, social software will lack functionality (Manovich, 2013). Manovich in his groundbreaking book, *Software*

Takes Command, delineated the features of software/machine/apps that people use to participate in culture-making. The focus of this comprehensive literature review (CLR) is on privacy as it relates to any software used to access, distribute, or publish media information (e.g., Facebook, Vimeo, YouTube, TikTok). Today's cultural software (Manovich, 2013) needs data in order to operate. Additionally, data we release as users of technology/software stands as the currency against which we receive digital services without having to pay monetarily for these services. Therefore, personal data enables accessibility and functionality of the digital world.

In the United States (U.S.) alone, about 72% of adults use at least one social networking site (SNS) (Perrin & Anderson, 2019). Worldwide, 3.5 billion people actively use SNSs (Kemp, 2019; Mohsin, 2019). Individuals connected via SNSs generate 2.5 quintillion bytes of data per day (Walker, 2015). In the years from 2013 to 2015, technology users have generated more than 90% of the data ever created by humans (Walker, 2015). To simplify the picture of how much data we swim through in a single day, every day we would need 10 million blue-ray discs to record the 2.5 quintillion bytes of daily generated data (Walker, 2015). The abundance of data and information produced today is magnificent; it is big data. In order to trace the unfoldment of literature findings and to provide an understanding as to how all of the aforementioned data streams play into SNSs users' and citizens' self-disclosure, I mapped the themes and subthemes. Figure 16 maps Theme 1 "Self-Disclosure Dynamics" and shows the connected subthemes. The following narrative will fully explain how the literature and MODES inform an understanding of self-disclosure.

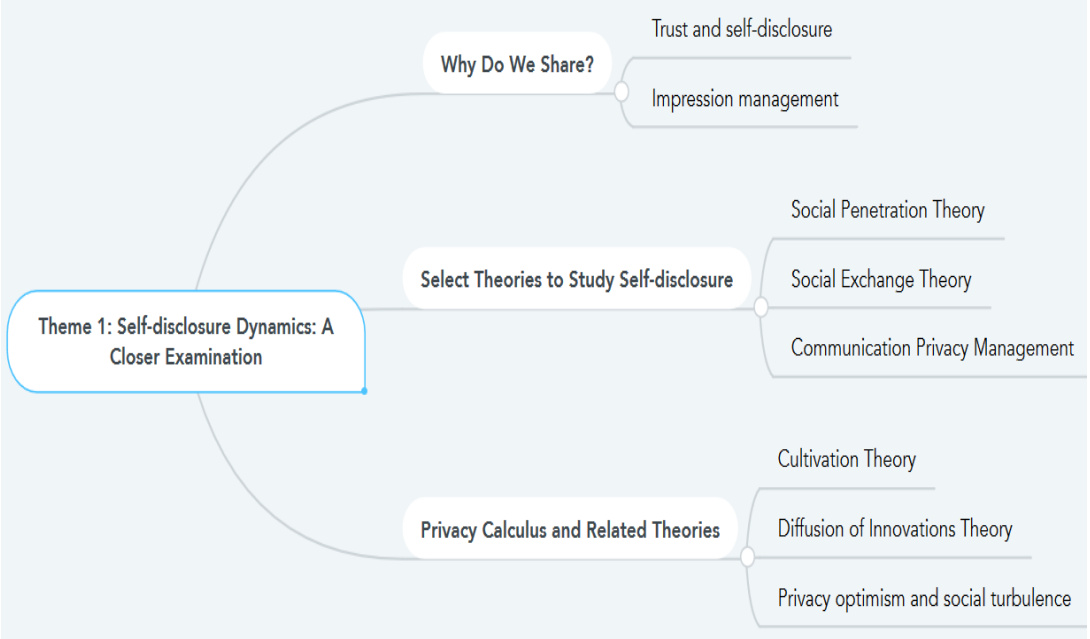


Figure 18. *Mind map of theme one: Self-disclosure dynamics*

Why do we share?. Self-disclosure is strictly connected to privacy (Baruh & Popescu, 2017; Choi & Bazarova, 2015; Hallam & Zanella, 2017; Liang, Shen, & Fu, 2017; Special & Li-Barber, 2012). Social media users often try to strike a balance between the risks and benefits of sharing personal information. An iconic study conducted by Waters and Ackerman (2011) queried why people share their personal information across SNSs. It is important to distinguish between personal and background information. According to Magolis and Briggs (2016), background information could be age, location, sex, college attended, etc.; personal information could be likes, dislikes, interests, and pictures or videos individuals share across SNSs. Some of the reasons why people share information are to store important and retrievable information, to be known and famous to others, to remain updated with current trends, or simply to have fun (Waters and Ackerman (2011).

Magolis and Briggs (2016) conducted a qualitative study to examine privacy awareness of self-disclosure of personal information among college students. Magolis and Briggs found that students have a myriad of reasons for why they share

information. As an example, students shared details about themselves for self-branding in the hope of seizing a career opportunity or to establish worthy connections. Impression management was another motive for which individuals shared information about themselves. Goffman (1959) defined impression management as the employment of various strategies to manipulate one's identity and stimulate positive responses from others. Much of people's impression management could be seen through examining different SNSs (Proudfoot, Wilson, Valacich, & Byrd, 2018).

Impression management. Self-branding or impression management are not new. Successful technological inventions have capitalized on human nature and emphasized what is naturally innate. It is our nature, as human beings, to create an identity and project it to others living around us (Lecky & Taylor, 1940). Today's SNSs offer just enough space for this innate trait to flourish exponentially. Privacy is no more a matter of face-to-face or a physical presence, as conceptualized by Warren and Brandeis (1860). Today, permissions to know each other need not to be physically given, as most of them occur mostly online (Albrechtslund, 2008; Waldman, 2015).

In their study about why people display their information online, Krasnova, Spiekermann, Koroleva and Hildebrand (2010) identified two key reasons that motivate self-disclosure. First, sharing information about the self appears to be convenient for maintaining relationships; and second, it is fun to know about what others share online. Karsanova et al., (2010) discovered that concern for digital privacy could inhibit social capital formation, i.e., sharing content with others, or having them interested in you; therefore, privacy may strip away the joy of online social validation.

Literature on privacy and SNSs disclosure showed a continuous tension between disclosure and privacy concern (Wang, Duong, & Chen, 2016). Tensions between sharing or not sharing is known as privacy calculus (Dinev & Hart, 2006). Privacy calculus could be explained by using social exchange theory (Blau, 1964). Social exchange theory suggests that people weigh risks and benefits of social interactions prior to engagement or sharing content. As related to the theme of self-disclosure on SNSs, Internet users usually scale privacy risks against immediate gratifications such as new friendships, maintaining existing relationships, impression management, and fame (Brinson & Eastin, 2016; Culnan & Armstrong, 1999; Dinev & Hart, 2006; Hallam & Zanella, 2017; Proudfoot et al., 2018).

Trust and self-disclosure. Self-disclosure on SNSs can increase as a result of an imaginary audience size. If the individual perceives or imagines there is a fair number of followers, i.e., social network users interested in their persona, they may disclose more to maintain the activity of impression management (Proudfoot et al., 2018; Ranzini & Hoek, 2017). The affordances of impression management seem to influence self-disclosure to a high extent. Proudfoot et al., (2018) surveyed 244 college undergrads about their self-disclosure habits and impression management habits. The research focused solely on Facebook as the main SNS platform. The survey was designed to test several hypotheses and aimed at generating a model for self-disclosure and impression management. The results revolved around topics related to privacy concern, trust, and impression management affordances. Trust had two dimensions and two different paths of reasoning. The first reasoning suggested that trust is considered a prime condition to establish privacy and release self-disclosure. If the user trusts the SNS, it leads to a decrease in site-specific privacy (as applied to Facebook), and increases both the social benefits of sharing as well as

impression management affordances. The key takeaway is that high trust in the SNS (whether service provider or the network of users) may reduce privacy concern and privacy measures.

The second path of reasoning is related to third-party data collection agencies and their practices. Knowing that third-party data collection agencies constantly collect data in order to profile users for advertising revenues often shakes users' trust. Peers (e.g., the network of friends) also threaten trust as co-owners of what is shared on Facebook. Peers of the single SNS user might accidentally disclose information that was originally intended for them to another audience that is unintended by the primary owner of the information. In either situations, SNSs usage and disclosure increase as trust increases and the opposite is true. According to Proudfoot et al.,' s (2018) model concerning self-disclosure, high site-specific privacy measures decrease sharing and could be influenced by general privacy concern. Impression management affordances increase as a result of a combination of trust in peers and less privacy concern.

Jeong and Kim's (2017) research was the only study in this CLR that examined sharing and posting on SNSs from a different angle. The study surveyed 216 college students and inquired about whether students have a concern for privacy over the information they share online (e.g., photos, posts, videos, etc.). The students showed concerns about privacy. Jeong and Kim indicated that on Facebook, the students were more fearful of what others might post about them or what others might post on their

timeline[15]. On Twitter, the participants were more concerned about their tweets than what they retweeted, or whether others retweeted them. This concern was justified by the fact that Twitter is more of a public site for information exchange and that the audience is different from Facebook, which often is based on accepting friends who can see posted information.

Privacy clashes, at times, with personal objectives sought by disclosing a piece of information. Choi & Bazarova, (2015) using a mixed-methods approach, compared the responses of 164 undergraduate students with regard to their social disclosure on Facebook and Twitter. Among the main goals of self-disclosure on SNS, the students sought social validation (a form of social gratification), which led them to lower their privacy boundaries. However, those who had relationship goals, such as keeping a limited network of friends or eventually commit to a social relationship, had less disclosure and high privacy boundaries. Regarding the intimacy of disclosure, the students in this study showed more concern for turbulence on Facebook because of invisible audience or due to collapsed audience (Marwick and boyd, 2014). Social turbulence occurs when a member of the audience shares the original post without permission from the original releaser/poster of information (Petronio, 2002).

[15] In this case, I mean a Facebook timeline/wall. It is the interface on which people post their photos, videos, and texts; share content with others, and interact with others' comments and likes.

Select Theories to Study Self-disclosure: Social Penetration Theory, Social Exchange Theory, Communication Privacy Management, and Users and Gratifications Theory

In order to fully understand how theories have informed contemporary research of self-disclosure within social media, I examined four main theories: social penetration theory, social exchange theory, communication privacy management, and uses and gratifications theory. Because some researchers employed a multi-theory approach in their studies to examine privacy literacy, I have clustered these theories (social ecological approach, Quinn, 2014), theory of planned behavior (Fishbein & Ajzen, 1975), and protection motivation theory (Rogers, 1975). Table 16 shows the defining features of each theory and lists key studies that were guided by that theory.

Table 16. *Main theories used to study social networking self-disclosure.*

Theory	Definition	Studies
Social Penetration Theory (Altman & Taylor, 1973).	The theory posits that self-disclosure is an ongoing process of gradually reveling oneself to others and allowing others to slowly access the self.	Osatuyi et al., (2018) Osatuyi (2014)
Social Exchange Theory (Blau, 1964)	The theory suggests that that people weigh risks and benefits of social interactions prior to	Proudfoot et al., (2018) Tsay-Vogel et al., (2018)

	engagement or sharing content.	
Communication Privacy Management (Petronio, 2002)	Privacy management relies on a set of boundaries and ongoing negotiations of ownership, linkage, and permeability, between the user and their audience.	Herrman & Tenzek (2017) Baruh et al., (2017) Baruh & Popescu (2017) Liu et al., (2017) Child & Starcher (2016)
Uses and Gratifications Theory (Levy & Windhal, 1984)	Media consumption could be analyzed in terms of intended uses and obtained gratifications.	Quinn (2016)

Figure 17 shows a breakdown by frequency of studies that were guided by each theory. The percentages were obtained using QDA Miner Lite analysis of 43 selected studies.

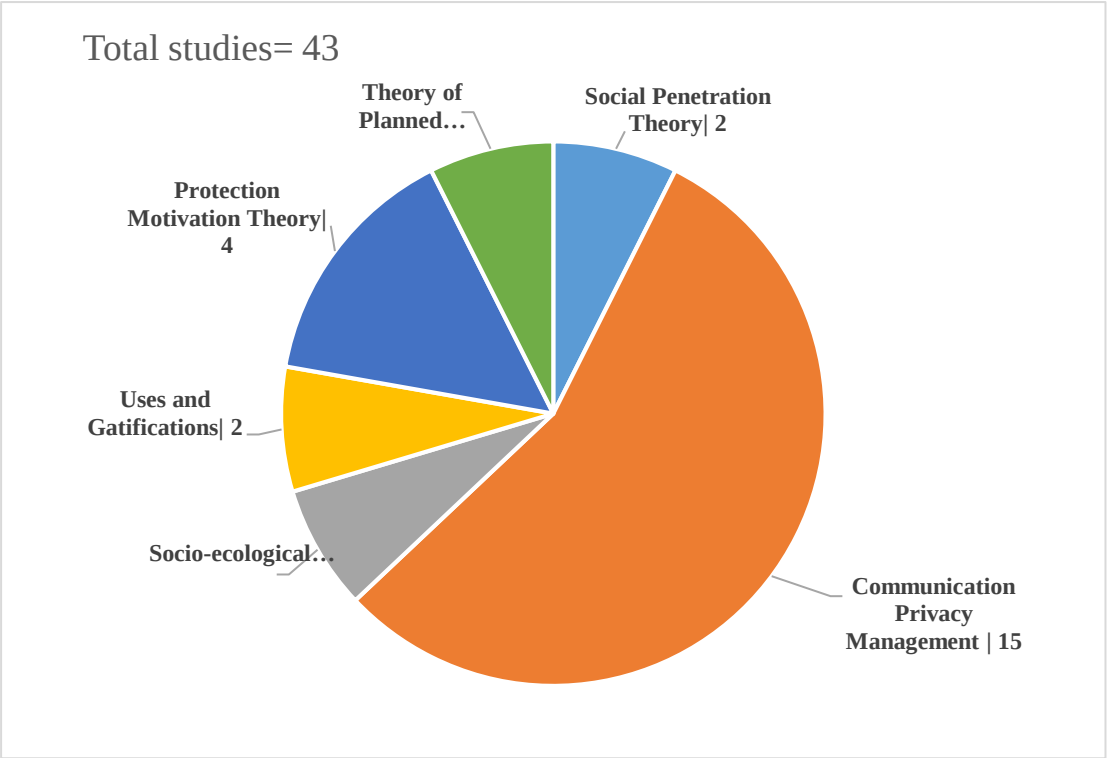


Figure 19. *Main theories used in the study of self-disclosure*.

Social penetration theory. According Altman and Taylor's (1973) social penetration theory, self-disclosure is an ongoing process of revealing oneself to others and allowing others to slowly access the self. In an analogy, it is like an onion where there are layers to every human, and social self-disclosure allows the peeling of the onion. Users control how deep or shallow they could be with individuals of their choice. Social penetration theory treats self-disclosure as a set of rules to follow in order to gain privacy. In a similar way, communication privacy management theory (Petronio, 2002) relies on a set of rules which are: ownership, linkage, and permeability. Ownership means the user who discloses information, enters an ongoing negotiation of content ownership with whomever has access to the shared information. Linkage refers to the reciprocity that exists between people as they exchange information. Permeability represents the application of privacy boundaries and how

much information is made accessible to others. Communication privacy management theory compliments social exchange theory in terms of how deep or shallow the information is, and how much access to the self by others is allowed.

Communication privacy management. As an example of how communication privacy management theory complements social exchange theory, Osatuyi, Passerini, Ravarini, and Grandhi (2018) used both social exchange theory (Blau, 1964) and communication privacy management theories (Petronio, 2002) to study self-disclosure. Doing so, Osatuyi (2014) conducted a study to examine interpersonal communications that occur on SNSs' and users' concern for shared data. Concern happens when a person shares a piece of information with another individual or group under the assumption that it will remain confidential among users or third parties (Baruh et al., 2017). Osatuyi (2014) used exploratory facto analysis and confirmatory factor analysis of SNSs' privacy concerns. He obtained three main factors that are related to data sharing. Factor one was users' concern for unintended use of their data and unauthorized access. Concern of users over errors of misuse and/or storage of their personal data loaded on factor two. Interestingly, collection of personal data loaded in factor three. This is in comply with other studies that found that SNSs' users are more concerned with social interaction and information leak to their immediate networks than data collection by companies or the government (Andrejevic, 2005; Marwick, 2014; Trottier & Lyon, 2013; Shade & Singh, 2016). Comparing the loaded factors to communication privacy management theory (Petronio, 2002), Osatuyi (2014) discovered that three rules of communication privacy management theory match SNSs' users concern for privacy. So, factor one, users' concern for unintended use of their data and unauthorized access is related to linkage and permeability rules; Factor two, errors of misuse and/or storage of users' personal

data are rooted in ownership rule; and factor three, personal data collection is related to permeability rule. Overall, Osatuyi (2014) argued that SNSs' users have a concern of losing their data knowing they actively participate in a space that is accessible by other users and data companies.

Social penetration theory and communication privacy management are theories which have common ground. The theories were also used to study select SNSs' users who experienced a privacy breach or data loss and how that breach affected their privacy behaviors. Osatuyi et al., (2018) surveyed 317 Facebook users and found that those who experienced a privacy breach had a different attitude than those who had not experienced a privacy breach. Those who experienced a privacy breach adopted a shallow sharing strategy, engaged in more self-censorship, and developed more privacy regulations. SNSs users who already experienced a breach appeared to disregard the social benefits of social disclosure.

Osatuyi, et al. (2018) found that users of SNSs who did not experience a privacy breach shared more information about themselves, and their acts of sharing relied on two principles of communication privacy management: ownership and linkage. To illustrate, SNSs' users negotiated the content ownership and relied on mutual peer trust. Privacy across SNSs is the responsibility of the individual, and that is only possible through the afforded privacy settings. However, successfully applying SNSs' privacy setting is a cognitively demanding task (Goel et al., 2011; Külcü & Henkoğlu, 2014; Vishwanath, Xu, & Ngoh, 2018). Because negotiating privacy requires reading and navigating layers of menus, some users cared less about who can access their information, while others preferred self-censorship (Osatuyi et al., 2018).

Usage of SNSs may raise concern for privacy. Tsay-Vogel, Shanahan, and Signorielli (2018) conducted a five-year longitudinal study of Internet users who

spend an average of three hours SNSs per day. The participants (N= 2789) revealed that they have concerns of privacy breaches and fear losing their information to unknown people. The users in their study felt threats to their general privacy, and, increasingly through the years, they showed more interest in government regulations of online privacy. Interestingly, those who used Facebook consistently disclosed more content and their concern for privacy faded with time.

Uses and gratifications theory. Uses and gratifications theory is another lens through which self-disclosure has been researched in the literature. Although it originated in the field of mass media, it is still relevant to scholarship of alternative media formats, such as SNSs. Uses and gratifications theory (Levy & Windhal, 1984) is a positivist theory in the sense that it analyzes media consumption in terms of users' motives and sought gratifications as a result.

Quinn (2016) analyzed students' (N=353) gratifications sought from self-disclosure and the possible threats to privacy. She concluded a list of gratifications for which users of SNSs disclose information: affect, companionship, voyeurism, information sharing, habit, entertainment, communication, professional use, and escape. The participants, however, considered identity loss and the fact that they do not own the shared information, to be among the major threats to privacy. Indeed, what may happen to their information is a question of high privacy concern, since any information shared online is not owned solely by the primary information holder. Any shared content on SNSs is primarily owned by the service provider and co-owned by whomever can see or engage with it—visible or invisible audiences (Herrman & Tenzek, 2017; Velten, Arif, & Moehring, 2017; Wissinger, 2017).

Privacy Calculus and Related Theories

Privacy calculus and its relation to self-disclosure are important concepts, as found by this CLR. Privacy calculus (Dinev & Hart, 2006) is the process of thought about the pros and cons of self-disclosure across SNSs. Some questions related to privacy calculus and self-disclosure are: what if we completely let go of our privacy? What would the world be like without privacy? And lastly, will technology revert to accommodate traditional privacy rules/laws as we know? As sub-theories used to study the influence of privacy calculus on self-disclosure, I discovered two theories that were mainly used: cultivation theory and diffusions of innovation theory.

Cultivation theory. Gerbner, Gross, Morgan and Signorielli (1994) posited that growing up with any type of media often socially cultivates us into accepting it as part of our daily routine and reality. Cultivation theory (Gerbner, 1969) may explain how we agree to share ourselves in online environments, such as SNSs, after hours of exposure to others doing the same. Therefore, does exposure to SNSs cultivate more relaxed privacy attitudes? Tsay-Vogel et al., 's (2018) longitudinal study showed the relationship between how exposure to SNSs and self-disclosure has weakened the individual's concern for privacy over time. Indeed, SNSs, as a software structure, are designed to foster and cultivate self-disclosure among users in order for them to win the social capital, and in order for the service providers to retain data for advertisement and profiling (Nguyen, Bin, & Campbell, 2012; Vitak, 2012).

Diffusion of innovations theory. Diffusion of innovations theory (Rogers, 2003) could also explain why users are comfortable with self-disclosure, as they become experienced users of technology services or as, in Roger's (2003) terms, they are early adopters of technology. Early adopters of technology believe their skills help to mitigate privacy threats and tend to have high privacy optimism (Baek, Kim, &

Bae, 2014)—that risks will not happen to them as much as to others. Privacy optimist individuals perceive SNSs as a positive and meaningful technology and tend to have high information consumption/production profiles.

Table 17. *Theories that explain self-disclosure and feelings about technology and media*

Theory	**Definition**	**Studies**	**Related self-disclosure theories**
Cultivation theory (Gerbner, 1969)	The more time we spend with media or a tech-device, the more we accept it as part of our daily life and routine.	Tsay-Vogel et al., (2018) Nguyen, Bin, & Campbell (2012) Vitak (2012)	Uses and Gratifications (Levy & Windhal, 1984) Social Penetration Theory (Altman & Taylor, 1973).
Diffusion of innovations theory (Rogers, 2003)	Early adopters of technology have the feeling of experts in using tech-devices to share and exchange information.	Baek, Kim, & Bae (2014) Sundstrom (2016).	Uses and Gratifications (Levy & Windhal, 1984) Communication Privacy Management (Petronio, 2002)

Figure 18 demonstrates the relationship among the main theories with regards to self-disclosure scholarship across SNSs. The figure shows the flow of the theories and how they build on each other in self-disclosure research. The theories could be

remixed, and others could be added depending on changes to technology and self-disclosure dynamics.

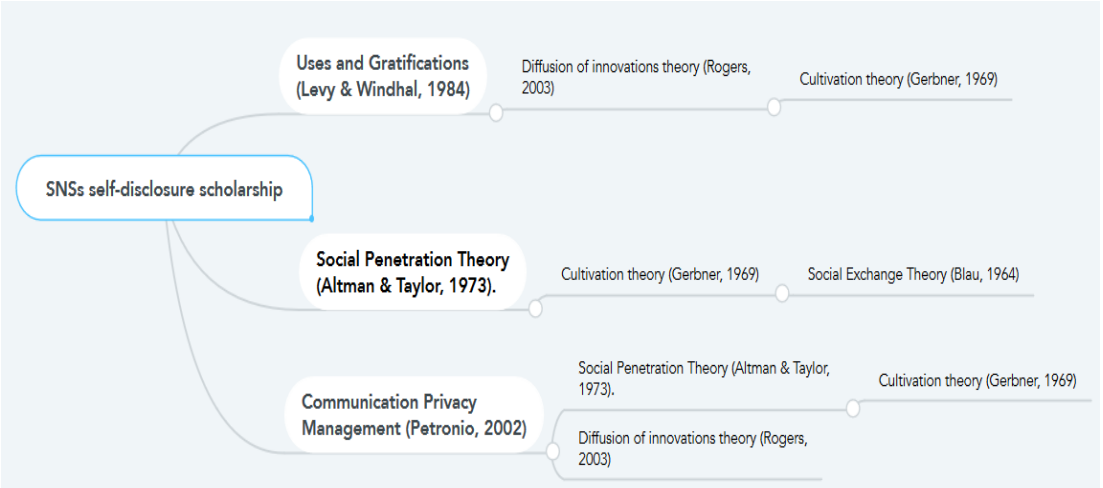


Figure 20. *Theories intersections and relation to self-disclosure scholarship*

Privacy Optimism and Social Turbulence

Perceived benefits and perceived privacy optimism are associated with increased self-disclosure. According to Baek, Kim, and Bae, (2014), SNSs' users who are engaged in highly protective privacy measures usually develop a comparative optimism. Meaning, someone who develops a privacy optimism will think that privacy breaches are more likely to happen to other people. Cheung, Lee, and Chan (2015) conducted a study with 405 college students on their cost and benefit perceptions of self-disclosure on SNSs. The researchers discovered that the perceived benefits mitigated the risks associated with privacy. More importantly, close social relationships exerted a great influence on self-disclosure. In other words, gaining social validation and influence were a byproduct of self-disclosure.

Self-disclosure on SNSs' may have repercussions on day-to-day relationships and cause social turbulence(s) (Petronio, 2002). Petronio explained that social turbulence happens when co-owned information leaks beyond the original owners and becomes public. Turbulence could be self-generated, where someone shares

unwanted content to others mistakenly; as it can also be other-generated when a member of the audience shares content about us without our consent (Cupach & Metts, 1994; Petronio, 2002). Litt and Hargittai (2014), in one of the seminal studies, surveyed 547 undergrads about their online social turbulence experiences. Interestingly, more than a third have had an experience of an online social turbulence. The researchers tested multiple hypotheses and concluded that social turbulence happened with three types of students: those who had high privacy settings; those who had high self-monitoring strategies; and those who overshared their activities online.

In fact, social turbulence could happen for either of these reasons: co-ownership of content (Petronio, 2002), audience collapse[16] (Marwick & boyd, 2014), or the website structure that leaks information to an invisible audience (Lynch, 2015; Litt & Hargittai, 2014). The same way content is co-owned, online social turbulences need co-repairs[17]. According to Litt and Hargittai (2014), avoiding online social turbulence requires technological and social behavioral skills.

Most users of SNSs, or those who share their information online, fear the loss of identity, of health records, of financial information, or just general breaches of privacy (Pereira, Robinson, Peoples, Gutierrez, Majumder, Mcguire, & Rothstein, 2017). A key takeaway from this theme on self-disclosure revealed that users give less attention to privacy when presented with a benefit that is socially important to them. Culnan and Bies (2003) summarized the issue and wrote, ". . . a positive net outcome

[16] Audience collapse is when you disclose information to a many people with different social and professional rankings.
[17] Co-repair is the process of amending and negotiating privacy face to face with whoever causes content to leak on SNSs.

should mean that people are more likely to accept the loss of privacy that accompanies any disclosure of personal information as long as an acceptable level of risk accompanies the benefits (p.327).” In other words, users are able to concede their data as long as the subsequent benefit outweighs the risk.

Summary of Theme 1

Self-disclosure is a complex phenomenon to study. Individuals behave differently on SNSs and privacy means different things to different people. In Theme 1, I tried to showcase the dynamics of self-disclosure, as to why people share content and give away personal clues about themselves. Some of the main reasons for which SNSs’ users disclose information about themselves is impression management and relationship nurturing. Also, the scholarship on self-disclosure followed a number of theories such as uses and gratifications theory (Levy & Windhal, 1984), which examines the motives for using SNSs and the gratifications individuals obtain in return. Finally, this theme has defined some of the core principles that accompany self-disclosure and privacy such as privacy concern (Wang, Duong, & Chen, 2016) and privacy calculus (Dinev & Hart, 2006).

Theme 2: Privacy Concern and Surveillance

In 1982, the *Time Magazine* marked the history of information and communication technologies (ICTs) by awarding a human-made machine the title of ‘the man of the year.’ The article in *Time Magazine* recognized the computer for being the 1982’s year “. . . greatest influence for good or evil” (Brown, 1982, n.p). During that time, the computer competed against great historic and political figures, such as President Reagan and Prime Minister Thatcher of England. In 1982, 80% of Americans projected that the computer will be a necessary home possession just like alarm clocks or air conditioning units (Brown, 1982). The computer was recognized

because the ". . . capabilities of the personal computer can be multiplied almost indefinitely by connecting it to a network of other computers, which can be used to access electronic databases or send electronic mails" (Brown, 1982, n.p). It was the first time a computer received an award since its creation in 1920's. Miller (1969) projected that computers ". . . may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of observers" (p. 1092).

Today, computers have evolved tremendously and have become integral in our life. Computers have blurred the line between public and private, online and offline, and have facilitated the collection, aggregation, profiling, and the de-contextualization of personal data (Nissenbaum, 2010; Sattikar & Kulkarni, 2011; Fallik, 2014; Moll, Pieschl, & Bromme, 2014; Hodkinson, 2017). Computers' advancement, surveillance, data collection and profiling provoked a host of privacy concerns among users (Albrechtslund, 2008; Marwick, 2012; Power, 2016). In order to trace the literature to provide a better understanding as to how all of the aforementioned data streams play into users' and citizens' privacy concern, I mapped this themes and subthemes. Figure 19 maps Theme 2 "Privacy Concern and Surveillance" and shows the connected subthemes. The following narrative will fully explain how the literature and MODES inform an understanding of privacy and surveillance.

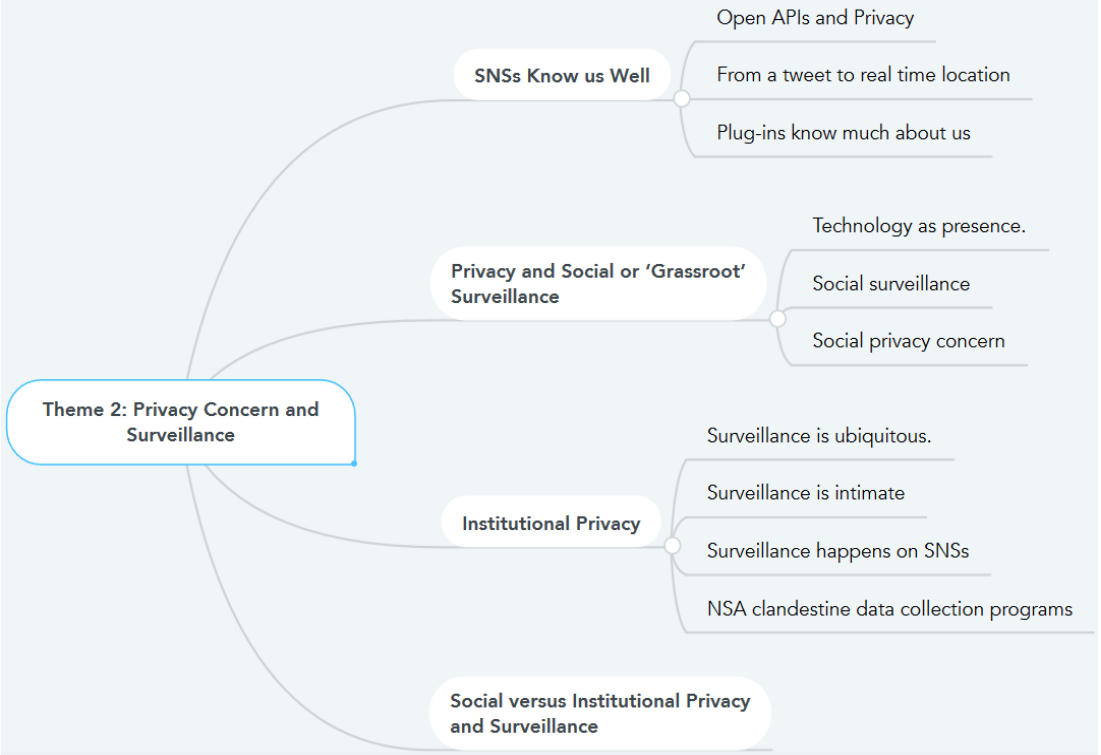


Figure 21. *Mind map of theme two: Privacy concern and surveillance*

To be in a psychological state of privacy concern is when an individual is uncertain about what could happen to the information they share with others, including portable devices and machines, as a daily routine. Today's Information 2.0 technologies, such as social networking sites (SNSs), leave us with difficult decisions to make as whether to participate and share with friends, groups, and others; or to withdraw, control, and enforce privacy settings, which in return, can affect the sociability and reduce the gratifications of SNSs (Altman, 1975; Jeong & Kim, 2017; Vitak & Ellison, 2013).

boyd and Ellison (2007) explained any shared data on SNSs are permanent, searchable, and could be replicated and scaled. Moreover, the social dynamics of the participating audience on SNSs, such as invisible gaze, collapsed context, and the blurring of public and private spheres, are important drivers of privacy concern. Regarding Facebook, Farinosi and Taipale (2018) argued that, "Sociability and

privacy can appear as conflicting needs" (p. 55). Aspects of social participation on SNSs can, indeed, affect interaction and participation in those spaces, and may generate a concern for loss of privacy (Bartsch & Dienlin, 2016; Liu, Yao, Yang & Tu, 2017).

According to Rainie (2018), "People are anxious about all the personal information that is collected and shared and the security of their data" (n.p). Privacy literacy is ignited with a psychological concern for personal information loss. Having concerns over his/her own data is a necessary step to questioning possible ways to protect personal information. Privacy concern then initiates a process of optimization between self-disclosure and withdrawal (Altman, 1975). Kyei-Blankson, Iyer, and Subramanian (2016) found that students, as well as other Internet users, have concerns about their personal data regardless of their gender, ethnicity, or education. In addition to concern over data, SNSs users also worry about being able to connect with one another privately.

Almost three decades before the innovation of SNSs, Bloustein (1976) was among the first scholars to express concern over being able to connect and socially engage with others while maintaining privacy. In addition to government surveillance, there is also social or peer-surveillance (Farinosi & Taipale, 2018). Peer surveillance happens when one lurks on what others post on SNSs and may engage in leaking information to unintended audience. Social network sites and other commercial websites' users are more concerned about social privacy than they are about institutional or government privacy (Baruh et al., 2017; Dienlin & Trepte, 2015; Kyei-Blankson et al., 2016; Tufekci, 2008); however, this particular privacy concern distinction is less researched (Haiyan Jia & Heng Xu, 2016).

SNSs Know us Well

Social networking companies are for-profit companies. The conversations and user-generated content produced (publicly or privately) on these platforms are used for targeting and advertisement purposes through state-of-the-art data-mining techniques (Fuchs, 2012). What if Facebook or other SNSs know more than what we post and share ourselves? In a seminal study, Kosinski, Stillwell, and Graepel (2013) analyzed Facebook profiles of over 58,000 users using researcher-developed machine learning models. The researchers wrote the algorithm model and designed it with an open fashion; i.e., the more the computer receives data, the more it adjusts and becomes accurate. The study population voluntarily provided the research team with access to their Facebook likes, demographic clues, and comments. The model was trained to predict the five big personality traits of Openness, Consciousness, Extroversion, Agreeableness, and Neuroticism. In addition, the model was programmed to predict religious, sexual, and political orientation.

From Facebook likes' analysis, Kosinski, et al., (2013) found high intelligence association between Facebookers and clickable content like 'thunderstorms,' 'the Colbert report,' 'science,' and 'curly fries.' Low intelligence was correlated with clickable content likes of 'Sephora,' 'Harley-Davidson,' and 'Lady Antebellum.' Homosexuality, for instance, was predicted by the clickable content likes of 'No H8 Campaign,' 'Mac cosmetics,' and 'Wicked the Musical.' According to the authors, using such traits can improve marketing services and refine citizen targeting. For example, knowing the Consciousness of a buyer can inform us about his/her purchase behavior and whether he or she is and impulsive buyer. These connections that a

human mind cannot make quickly, machines can make quickly, and with precision, about large crowds and groups of people (Lanier, 2013).

Open APIs and privacy

Sophisticated algorithms do not need so much data to form an accurate impression or predict someone's behavior. Once algorithms are written and embedded in a predictive model/matrix, computers can then use the model to learn and adjust from data, i.e., machine self-learning from available data. These models enable computers to unravel many things about us; from bits of information that individuals leave behind as meaningless or insignificant (Zuboff, 2019). For instance, Kosinski (2017) found that 11 random Facebook-likes are enough data to predict a person's personality better than his/her coworker; 100 likes are enough to predict a person's personality with more precision than his/her friend or family member; and 250 likes can predict someone's personality better than a what a wife can predict about her husband.

The Cambridge University's Center of Psychometrics developed an open Application Programming Interface (API) called Apply Magic Sauce (accessible at https://applymagicsauce.com/demo) to analyze Facebook data. The API can analyze downloaded Facebook or Twitter data or any open texts using natural language processing algorithms. For instance, the API can provide personality (see Figure 20)[18] and other insights based on comments, photos, posts, and open texts. Machine

[18] The personality test in the picture was a result of 100-character text that I typed into Apply Magic Sauce to test natural language processing.

learning models, like Apply Sauce Magic, threaten privacy and the purpose for which we post and share online, i.e., to connect with others.

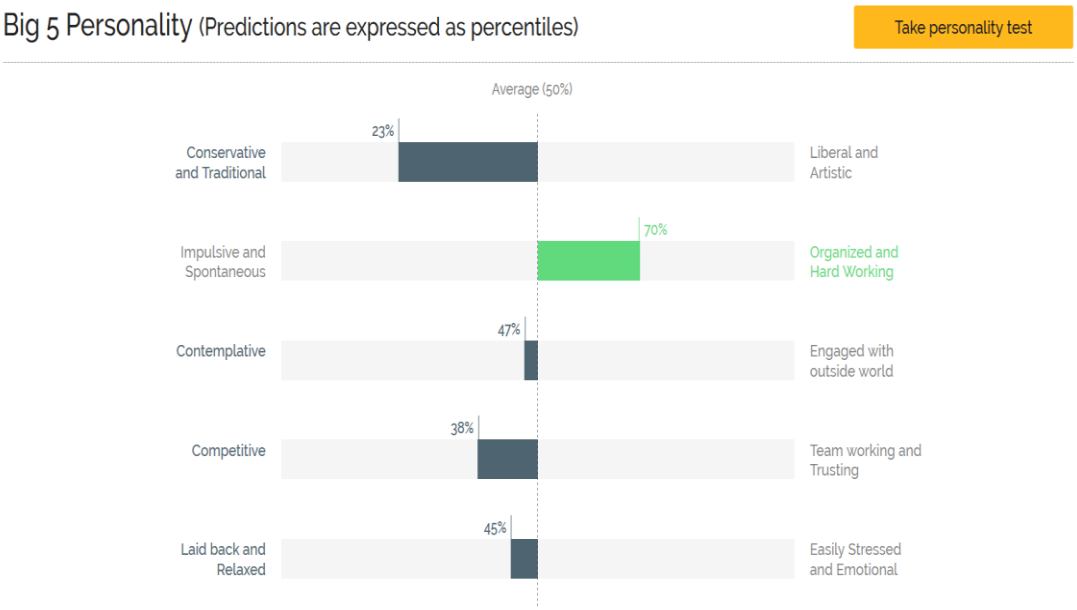


Figure 22. *Apply Magic Sauce API personality analysis based on 100-character text*

Other APIs such as Hoaxy[19] (see Figure 23) can also unveil personal privacy, especially on Twitter. The API works as a mapper of news diffusion/information spread on Twitter and connects news back to specific Twitter accounts, that are clickable, searchable, and retrievable. The API can also track the person's involvement and interaction with news and among friends or communities. The diffusion is automatically clustered around the main actors of news, information, or rumor diffusion. Hoaxy also shows who tweeted what and replied to whom, as well as highlights bots'[20] tweets and diffusions.

[19] I tried the key word "Khashoggi" to be able to track the spread of his killing news.
[20] A bot is an automated system that is designed to interact with users or computer systems.

From a tweet to real time location. Through Hoaxy and using tweets, one can narrow down news interaction to individuals (e.g., using TAGS[21]) and be able to know their location real-time by plugging the Tweets in location APIs such as Geopy. [22]Geopy converts Twitter metadata into real time location. Although Twitter users engage in use of the platform with an intention to express themselves and exchange opinions/news, their content could be used otherwise by third-party companies, such as to profile or study the behaviors and political orientations of users. As a rule of thumb, online data can always be accessed by a third party and be used outside its context.

Knowing about Hoaxy API may engender high privacy concerns within users. Moreover, APIs enable the use of online content outside the context in which it originated to, for example, analyze political orientation, engagement, location, and sexual orientations of citizens. ICTs with their analytic powers have magnified the threats to personal privacy, to self-presentation, and facilitated the de-contextualization of personal data for business ends (Nissenbaum, 2010). Figure 21 gives an example of how data could be decontextualized and used for purposes other than users' intentions, which is to engage with others using SNSs.

[21] TAGS stands for Twitter Archiving Google Sheet. It is and Application Programming Interface that harvests hashtags.
[22] You can read about Geopy here https://geopy.readthedocs.io/en/1.10.0/

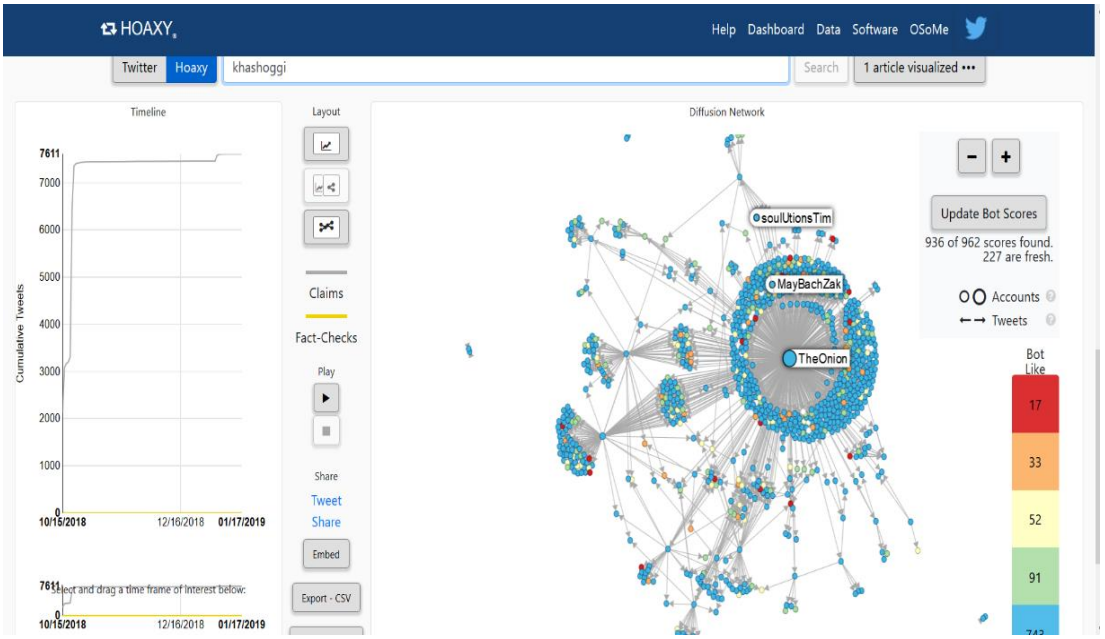


Figure 23. *A screenshot of Hoaxy news diffusion map of public tweets.*

Hoaxy or Apply Sauce Magic use developer API keys (e.g., Twitter, Facebook, etc.) to collect data from Twitter, Facebook, etc. that are then used to analyze and predict the users' behavior and their tendencies. These platforms are open to the public. However, these are not the only platforms using APIs for prediction and analysis of user behavior. In the field of marketing and data analytics, Google Analytics[23] is the place to start investigating about the consumers' trends. Jungle Scout[24] is another data harvesting program that analyzes Amazon purchases, trending products, products people have searched for and could not find, keywords customers

[23] Find more about Google Analytics here: https://analytics.google.com/analytics/web/provision/#/provision

[24] Data analysis machine launched by JS Operating Company, LP (Founded in 2014) as Jungle Scout to analyze data related to consumption and identify gaps in production, marketing, and targeting. See https://www.junglescout.com/lp/brand/?gclid=EAIaIQobChMIpJO3zofA5wIVDlYMCh16nw9AEAAYASAAEgIDm_D_BwE

have typed into Amazon website, and more. It is a par-default knowledge that users leave behind as they browse to shop or visit service websites online.

Plug-ins know much about us. Google Analytics is an HTML code that can be copied and pasted to the webpage of the service provider'. This allows the tracking of users' behavior as they browse. Data collected are meant to inform the website developer about the website sections the users enjoyed the most, their path in website navigation, their confusion(s), time spent on the website sections, when they left (bounce rate), and from where or what section on the website that they left. Such data and more are valuable and free; they can boost businesses and inform customer targeting. Google Analytics delivers a report with the number of visitors (weekly/daily/hourly), the bounce rate, users' countries and cities, language, device used to browse the website, gender, and how users navigated the website.

The same is true about Facebook Pixel[25] plug-in that tracks the number of people who visited a product website but did not buy anything as well as the number of people who placed items in the basket, but did not check out. Facebook Pixel generates a list of those who did not complete the purchase, locates their Facebook profiles and allows the option to re-target them with ads. Facebook Pixel often is attached to a business or organization website that uses Facebook advertising. Facebook Pixel is usually attached to the shopping cart where many customers may fill the cart and then not complete check-out. Facebook Pixel will then identify those

[25] Learn more about Facebook Pixel here: https://www.facebook.com/business/learn/facebook-ads-pixel?ref=sem_smb&utm_source=GOOGLE&utm_medium=fbsmbsem&utm_campaign=G_S_Alpha_Pixel_Brand_US_EN_Acquisition_General&kenid=cd1f46d2-1c37-40da-abe7-eca28770d3ab&product=NoDimensionAssigned&utm_keyword=pixel%20for%20facebook&gclid=EAIaIQobChMIl7XG6onA5wIVyrzACh1ylwapEAAYAyAAEgI3mfD_BwE

customers (if they have a Facebook account) and allow the option to reach out to them with a reminder to finish the purchase.

The growth of targeting tools for marketing or surveillance purposes engenders concern for privacy and loss of data. danah boyd (2012) summarized the issue about privacy concern and argued that,

> Most people are unaware that their data is aggregated with others to construct portraits of individuals that predict their interests based on others' habits. Our interpreted selves aren't simply the product of our own actions and tastes; they're constructed by [recognizing] similar patterns across millions of people. (pp. 348-349)

When privacy concerns are mentioned, two components become important: content and audience. Citizens and users of SNSs prioritize privacy differently. Some are worried about how the content of their SNSs is accessed by friends and other individuals, whereas other people are worried about third-party access to their content and data from companies like Acxiom or government agencies such as the National Security Agency. Surveillance can, therefore, be institutional or social (Marwick, 2012), or what Tufekci (2008) called "grassroot surveillance" (p. 35). Tufekci explained grassroot surveillance to be a consequence of using intertwined SNSs which have raised social curiosity about other fellow humans—what each other is up to; what is new, etc. With SNSs, much of the lurking/curiosity work could be done with a click, especially data that are permanent and searchable.

Privacy and Social or 'Grassroot' Surveillance

Social privacy appeared as a sub-theme of "Privacy Concerns and Surveillance" and as dichotomous to institutional privacy. Social privacy research and

commentary focus on exploring social relationships and the concern of losing personal information to other users, friends, family, or other individuals. Institutional privacy research, on the contrary, relates to privacy concern of losing one's personal data to an institution or company such as Google, Amazon, or the government for surveillance purposes.

Social surveillance. Alice Marwick (2012) wrote extensively about 'social surveillance' and questioned privacy in the age of publicity and self-disclosure. Marwick argued that online users designate a huge importance the human gaze. She commented, "Users monitor their digital actions with an audience in mind" (p. 379). Additionally, Lyon (2018) emphasized the fact that SNSs users engage in activities of watching others all the while also knowing that they too are being watched. It is a reciprocal surveillance which encourages self-branding as well as self-surveillance and monitoring. Reciprocal surveillance is a different type of surveillance apart from government surveillance. Reciprocal surveillance happens among people and each SNSs individual, to an extent, knows that he or she is being watched. However, the government only watches us but we cannot watch back. Reciprocal surveillance is a new layer of surveillance that is different from the panopticon (Bentham, 1790, 1791), or the 'Big Brother' (Orwell, 1949).

Regarding reciprocal surveillance, one of Marwick's (2012) study participants said "With Facebook you know that at that moment a portion of your friends are doing the same things that you are" (p. 390). Marwick and boyd (2011) claimed that users think of other users' surveillance and ignore the commercial surveillance or its impact. Whether it is lateral surveillance through friends (Andrejevic, 2004), or government and institutional surveillance (Greenwald, 2014; Whitaker,1999), the

impact might still be the same. Users of ambient technologies are reduced to pieces of data (Kosinski, 2017, 2019; Kokolakis, 2017). In other words, friends are interested in the data our postings generate, likes and appreciations; companies, on the contrary, are interested in our numeric data that depict our behaviors and orientations. Data are the currency and the drive of privacy, surveillance, business, and more.

Kyei-Blankson, Iyer and Subramanian (2016) conducted a mix-method survey with 302 college students to better understand their privacy concerns while maintaining a SNSs presence. The results showed that female students were more concerned about their privacy than their male counterparts. Similar research found that women expressed more concern over their data than men (Farinosi & Taipale, 2018). Moreover, Kyei-Blankson et al., (2016) noticed that unemployed students expressed more concern over their personal data than did those employed. The researchers did not provide further details, but the reasons could vary per individual. For instance, unemployed students may be under the pressure of maintaining a certain SNSs image to maximize their employability upon graduation. Also, the respondents had various opinions about trusting SNSs users and expressed their readiness to meet people from more serious platforms such as Linked In (Kyei-Blankson et al., 2016). Therefore, trust in the network could influence the trust of its users. Students, in Kyei-Blankson, et al., (2016) study, tended to place varied levels of trust on different networks, which may have impacted their behavior.

Tufekci (2008), in her seminal work "Can You See Me Now?," explained the logic of "...seeing and being seen" (p. 20), and how it moved from a physically lived experience (Brandeis & Warren, 1890) to an online context. Seeing and being seen in the world of fast data and information exchange means thin boundaries between

public and private spheres; information released about ourselves online is co-owned with whomever accesses it. This means that there is no information access control or audience control in the sense that invisible/unintended audience will always be there. These challenges remain the prominent drivers of concern(s) over privacy. Threats to privacy could be many and they can directly affect users' behavior. Building on Altman's (1975) work, Tufekci pronounced a set of threats to privacy, mainly inexistent temporality, audience collapse (see also boyd & Marwick, 2014), and publicizing of personal data.

In Tufekci's (2008) study, of the total participants (N=601), 94% had real names, but they restricted their friending policies to those who they know in real life. The participants expressed concern over unintended audience, but they maintained their names for publicity and future employment opportunities. The author also noted that the more students used SNSs, the less concern they had over their privacy; however, on the converse, those who did not have a SNSs' presence had higher privacy concerns. In the same line of thought, Farinosi and Taipale (2018) found a relationship between time spent on SNSs and privacy concern. The researchers claimed that the more users spent time on social media, the less concerned users were about others lurking in and through their SNSs data and information. However, it is important to note that when users are concerned, they are primarily concerned about human lurkers versus machine learning algorithms (Farinosi & Taipale, 2018).

Social privacy concern. Concern for privacy is one of the most powerful influencers of SNSs users' behavior and relationships. Baruh, Secinti, and Cemalcilar (2017) conducted a meta-analysis of 166 research articles from studies conducted in 34 different countries. In total, the meta-analysis contained 75,269 participants across

all 166 research articles and studies. Baruh, et al., found that when privacy concern is high within SNSs users, intentions to use SNSs or share personal information are significantly reduced. However, parallel to this attitude, privacy-concerned users tended to adopt high privacy protective measures or reduce their participation in SNSs. More importantly, Baruh and colleagues found no significance between privacy literacy and privacy concern mitigation, except that privacy literate users adopted more protective measures. Does privacy concern represent an integral stage of thought for whoever shares information online?

Users of SNSs are concerned more about their information against people they know than institutions or third-party data processors. boyd (2014) remarked that young SNSs users are not as concerned with the government's surveillance as they are with their parents, teachers, and those close to them. Social privacy also extends to privacy concern over the collective or community. In addition to having concerns about individual privacy, SNSs' users are concerned about the privacy of their connections and their immediate relationships, as they share information with friends, parents, and their networks. Jia and Xu (2016) illustrated, ". . . because content shared on SNSs often contains information of multiple individuals, rather than just the original sharer, users of SNSs are concerned about the privacy of their friends being unexpectedly exposed or violated due to their disclosure behaviors" (p. 3).

Concern for social privacy is important to users because of the uncertainty it attaches to the act of sharing. Lyon (2018) argued that ". . . in the world of SNSs, mutual expectations that users might have of each other are often full of uncertainty, shifting and mutable" (p. 33). Hence, protecting one's privacy on SNSs is collective (Petronio, 2002; Marwick & boyd, 2014) and so is privacy concern. As mentioned

prior, privacy concern is a necessary step that precedes privacy measures. The collective norms of a social group also happen to influence their privacy concern (Jia & Xu, 2016). Therefore, it is safe to say that privacy concern is a multifaceted thought about information disclosed online. Privacy concern is contextual; it drives privacy action and it is collective or social.

The context of social surveillance (Marwick, 2012), such as SNSs, is not different than institutional surveillance context, such as at the airport security checks or plane check-in moments. These contexts are complementary and the line between them is thin. Lyon (2018) examined social and institutional surveillance and argued that both types of surveillance may "...feel like quite different contexts, until the U.S. border official wants to check your Instagram account" (p. 115). The motives for either type of surveillances might be different, but the data are the same. It is what citizens generate as a result of interacting with their phones rather than interacting with the devices as useful technological means. Social surveillance, by definition, tracks individuals' behaviors, desires, tendencies, and willingness to compete with others to look good, catch fame, or maintain an online lifestyle (Lyon, 2018).

David Lyon in his book, *The Culture of Surveillance,* explained how surveillance extends from police and government work to lateral or peer-surveillance (social surveillance) and through self-surveillance (Andrejevic, 2005; Marwick, 2014). Social surveillance also happens domestically and is accessible to everybody (Trottier & Lyon, 2013; Shade & Singh, 2016). Lyon (2018) posited that parents track their children and friends across various SNSs. Lateral surveillance is the phenomenon of watching others, those of whom we know or sometimes would like to know about.

Self-surveillance (see for e.g., Biddle, Gorely, Pearson, & Bull; 2011Crowe, 2019) is another concept explained by Lyon as monitoring or controlling ourselves. It ranges from activities related to controlling SNSs privacy settings, friending, and sharing to using ambient technologies to monitor our fitness, calories burnt, heart rate, or else (Biddle, Gorely, Pearson, & Bull, 2011; Bivins & Marland, 2016; Milan, 2015; Morris, 2016). With the age of technology, we have become visible through our phones and the apps we use on a daily basis (see for e.g., Eagle, Pentland, Sandy, & Lazer, 2009).

Technology as presence. Many SNSs users are more concerned about the immediate social surveillance or peer surveillance (Marwick & boyd, 2014) than institutional or government surveillance (Lyon, 2018; Raynes-Goldie, 2010). Part of the problem lies in the fact that individuals are attached to their machines and entertainment technologies. “When so many are immersed in the daily round of sharing, posting, emailing, following, tweeting, and updating their status, it is hard to detach yourself for long enough to get a sense of what this world means,” posited Lyon (2018, p. 156). Immediate gratifications and the social validation SNSs’ users receive as a result of their sharing keeps them attached to their fans/followers and the virtual interaction that they receive from this. In an interview with Paul Eaton, an assistant professor of educational leadership and an expert in social media’s impact on students, faculty, and higher education, explained sharing and self-disclosure as “. . . the way that [people] get a rush from the likes, the shares, or the comment on posts . . . so for some people that's really important (P. Eaton, personal communication, February 10, 2020).

The problem is, as Lyon (2018) coined it, ‘technology as presence.’ He explained that phones or other ambient technologies have entered our lives, and many of us have welcomed and domesticated them at home. It all starts with a device connected to the Internet. Those devices are what Dodge and Kitchin (2011, p. 58) called “Logjects.” Logjects are electronic devices operated by software which enables the device to automatically track and record different operations made by the user. In other words, automatically generate user-data.

On SNSs, information is produced and consumed at the same time. Producers of content also consume data and check on others’ activities and postings. This double function of SNSs “... creates a symmetrical mode of surveillance in which watchers expect, and desire, to be watched themselves... in the absence of face-to-face cues, people will extrapolate identity and relational material from any available digital information” (Marwick, 2013, p. 220). The nature of social connection requires physical cues and news information in order to know about each other (Warren & Brandeis, 1890). Most of the surveillance is between each other online (Lyon, 2018). We watch others and we allow ourselves to be watched by others (Tufekci, 2008). Watching others and being watched is almost a necessary step to either know each other or keep updated about our closed relationships.

Institutional Privacy

The current state of institutional surveillance, which comes from the government (Greenwald, 2014; Whitaker,1999) or from SNSs (Dijck, 2014; Lyon, 2015; Semitsu, 2011) service providers, is inescapable. Whether we accept it or not, we all contribute to the spread and increase of surveillance (Ball, 2017; Park, Shin, & Ju, 2015). Lyon (2018) considered institutional surveillance as “...something that

everyday citizens comply with—willingly and wittingly or not—and desire" (p. 9). Surveillance shadows everybody, especially recently, because individuals are either surfing the Internet or carry a phone in their pockets, which is automated to communicate location and personal data, constantly and without the citizen's knowledge or consent (Fleishman, 2017; Juang, & Juang, 2012). For instance, iPhones are dotted with Places app that automatically locates the pictures taken, even if the camera app location services are turned off. Frequently, iPhones record cell tower connectivity; hence, store a history of our daily displacements and travels (Whittaker, 2017, 2018). Data are everywhere and are amassed without discrimination, just like our airline check-ins that are automatically shared with the National Security Agency and other countries, as part of the Five Eye program (Lyon, 2018). Some of these surveillance activities are known, but an array of surveillance activities remain secrets (see for e.g., Whittaker, 2017).

In the age of surveillance, we almost all have our 'other digital self,' but we may not exactly know what this other digital self looks like. This culture of surveillance sparks privacy concerns (Connor & Doan, 2019; Dinev, Hart, & Mullen, 2008). A recent study (Ledbetter, 2015) about American's top fears showed that almost 50% of Americans feared institutional/corporate tracking of personal information. Additionally, it is estimated that six in ten Americans believe that they cannot go through the day without government watching and collecting their personal data (Auxier, Rainie, Anderson, Perrin, Kumar, & Turner, 2019). Didier Bigo (2011) claimed that the current state of surveillance operates on digital footprints by tracking everything that moves, tangible as a human, or intangible as a piece of information.

Surveillance is ubiquitous. Computers and machines when paired together help create much of today's intelligence and data about people. The Internet of Things (IoT[26]) is a great example of the communication of data among and between portable smart machines. Ubiquitous computing or computer machinery is immersed in every level of life and device surveillance is made invisible to the users (Briggs, Churchill, Levine, Nicholson, Pritchard, & Olivier, 2016; Lyon, 2018). Some surveillance is made visible to people through surveillance means such as CCTVs (Trottier, 2014). However, much of institutional surveillance is unseen (Brown, 2014; Fuchs, Boersma, Albrechtslund, & Sandoval, 2011). Lyon (2018) explained that ubiquitous surveillance ". . . does not involve literal watching at all. You are 'seen' in your bank records, cell phone calls, bus passes, workplace IDs, loyalty cards at the supermarket, passports. . . on Google, Facebook and Twitter" (Lyon, p. 70).

Technology drives societal change and gives voice and power to data collection agencies (Paul, Sarker, Brownstein, Nikfarjam, Scotch, Smith, et.al., 2016; Trottier, 2016, 2019). Ubiquitous computing and ambient technologies gave birth to a surveillance culture and environment where citizens and SNSs users are "...watched in an extraordinary number of ways and contexts, [and although citizens are] increasingly aware that they are watched [they]...in some respect, appear to have made their peace with this" (Lyon, 2018, p. 79). Eaton noted that individuals "...like the convenience of sharing and interacting across SNSs and they don't want the hassle

[26] The Internet of Things is a system interconnected devices with unique IDs and which send and receive data without human interference. Read more about IoT here: https://en.wikipedia.org/wiki/Internet_of_things

that comes along with protecting their privacy" (P. Eaton, personal communication, February 10, 2020).

Some have even adopted machines and purchase services to guarantee themselves a level or surveillance on others. Surveillance is not only a top-down process, but it also goes lateral among people (see also Trottier & Lyon, 2012). Surveillance is becoming a culture and a way of life (Andrejevic, 2005; Marwick, 2014). The software high-tech design (e.g., Facebook, Amazon, Google) has opened doors for a liquefied surveillance that is neither clear nor rigid. Social networking sites exposed a surveillance that is no longer exclusive to the government.

Surveillance is intimate. Many apps have entered our houses to live with us and collect our intimate data. The following quote is posted on Reddit[27] to the community of Fitbit[28] users. It reads,

> My wife's fitbit is showing her heartbeat being consistently high over the last few days. 2 days ago, a somewhat normal day, she logged 10 hours in the fat burning zone, which I would think to be impossible based on her activity level. Also, her calories burned do seem accurate. I would imagine if she was in the fat burning zone, she would burn a ton of calories, so it's not lining up.

The post received 702 comments. The top comment was interesting as it gave the husband a lead on something that would turn out to be reality. The respondent said,

---

[27] For more details, please see https://np.reddit.com/r/fitbit/comments/445ppj/hr_reading_consistently_high_last_few_days/

[28] Fitbit is a sports gadget/watch that is endowed with a sensor to track heart rate, sleep activity, energy, and other sports related activities.

"Has she experienced anything really stressful in the last few days or is it a possibility she is pregnant?" The Husband then replied, ". . . pregnancy is a strong possibility, didnt (sic) know that would jack up the heart rate. I might be a dad, YIKES. now I gotta watch my own heart rate lol." Amanda Jackson (2016), a journalist at CNN, picked the story "Husband and wife never expected their Fitbit would tell them this" and told the story of a husband who thought the Fitbit was defective and needed replacement, before he was swept by surprise from one of the online community members who told him his wife might be pregnant. Talking about privacy, in this situation, Fitbit and the community knew about this user's intimacy prior to he and his wife actually knowing the outcome. There are many apps that collect our intimate data and know more about us than ourselves. Intimate surveillance is a term I borrowed from Leaver (2017) which he used to depict the context of social surveillance monitored by parents over their children, friends amongst themselves, and so on. I am using the term to mean not only that, but also mean the intimate surveillance that companies exercise on their service users.

Another example would be the way we use smart phones, also called 'personal tracking devices' (Lyon, 2018), to capture intimate moments and have those moments monitored by third-party companies that have access to our phone-generated data (Narseo & Srikanth, 2018). Access to our phones any time we use SNSs services collapses space and blurs privacy boundaries (Marwick & boyd, 2014). Technology devices have no such boundaries as privacy in a living room versus a public parking garage. Data collection is indiscriminatory of social and human values and spaces. As an example, Instagram privacy policy reads, "We collect the content, communications and other information you provide when you use our Products...location of a photo or

the date a file was created. It can also include what you see through features we provide, such as our camera...” Instagram[29] collects almost everything and sees through our phones, even if the content is not captured or published.

At another macro-surveillance layer is idea of the ‘big brother,’ as portrayed in George Orwell’s (1949) classic novel, *1984*. Social networking companies are affiliated with government surveillance programs and are vulnerable the State’s intelligence (Payton & Claypoole, 2014). For instance, Facebook’s facial recognition capacities are more sophisticated than the Federal Bureau of Investigation (FBI), because Facebook receives more content then the Bureau; hence, its algorithms of facial recognition are sharper and its repertoire is more diversified compared to the FBI, which has a limited dataset of people’s faces (Lyon, 2018). Therefore, although the government has a big basket of data, these data are simply information debris from telecommunication companies such as voice communications traffic, cell tower and Wi-Fi tower phone-communications, stored photos and videos, Internet based conferences (Skype, Apple’s Facetime, etc.), online purchases and money transfers, and the list goes on (Payton & Claypoole, 2014; *Samuels*, 2019) versus the more robust and targeted data collected by Facebook.

As of June 2016, Google was granted a U.S. patent to manufacture smart baby cribs. The smart crib stands as a great example of intimate surveillance and private space intrusion. The crib is equipped with sensors that monitor the baby’s movements at all time. The crib can be linked to the parents’ phones so they receive alerts of, for

[29] Instagram data policy could be accessed here: https://help.instagram.com/519522125107875

instance room temperature drops; if the baby is awake when it should be sleeping; or if the baby needs new diapers; or makes them aware if the baby is coughing or sneezing unusually. The crib can also respond to baby cries and put on entertainment video or music. The crib is built with an algorithm that collects babies' cries and works on interpreting them as cries for hunger, aches, or diaper change (Muoio, 2016).

Surveillance happens on SNSs. The rise of SNSs, participatory data sharing, and surveillance enforced 'dataveillance.' According to Clarke (1988), Dataveillance is the "...systematic monitoring of people's actions or communications through the application of information technology" (p. 500). In a later publication, Clarke (1994) made distinction between personal dataveillance and mass dataveillance. The former is when an individual is being surveilled or inspected as he/she uses Web services. The latter surveils a group of people or an entire community. For example, Trottier and Lyon (2012) explained the anatomy of Facebook surveillance where users construct their identity and reputation in collaboration with others. The different community groups and personal friend-to-friend relationships allow for data exchange, social ties establishment, and even data leaks. Because of instant and multiple interactions, surveillance and digital presence on SNSs are fluid. This fluidity is further enhanced with lateral or social surveillance, as in a peer leaking information about another peer. Moreover, any exchanged information among SNSs users is a commodity owned by service providers, like Facebook, and is passed on to advertisers and police (Trottier & Lyon, 2012). In addition to the aforementioned features, Trottier and Lyon argued that the constant changes and updates of SNSs structures and policies encouraged "...unanticipated visibility…enhance[d] the scope of peer-to-

peer sociality and scrutiny, all while facilitating the commodification of these exchanges" (p. 93). The commodification of SNSs participants supported Foucault's (1977) definition of surveillance as when someone "...is seen, but he does not see; he is the object of information, never a subject in communication" (p. 200). In this world of massive surveillance, we are points of data, content, and a sum of behavioral traces and clues that once aggregated, can sharply reveal everything about us (Zuboff, 2019).

Data requests about individuals are common among the world's countries. In the U.S., such requests are protected by the Electronic Communications Privacy Act (ECPA) of 1986. Under this act, the U.S.' Federal government compels information companies, such as Google or Facebook to supply information (e.g., email, address, alien's name or identifier) within a certain time and without alerting or informing the user. This type of surveillance is another example of undercover surveillance that happens without the user's permission[30]. Institutional surveillance is done as routine control or as part of a criminal investigation or other unknown reasons. For instance, Ira Gus Hunt, the former Central Intelligence Agency' s chief technology officer said at the GigaOm's data conference (2013) in New York:

> The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time. . . Since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang onto it forever.

[30] As an example, see Appendix.1: a letter of request from the Bureau of Federal Investigation (FBI) requesting data about a Facebook user

Sometimes, the government collects data, even meaningless, to keep for probabilistic needs in the future. Payton and Claypoole (2014) stated that the U.S. government aggregated its citizens' data without asking permission nor offering the opportunity to opt in or out of data collection. The researchers said, "Most citizens . . . are already in the mix without even knowing it" (p. 34). In my discussion with Paul Eaton, he posited that we do not "...have any privacy anymore are even if you were to do everything in your power to remove yourself from the system, you actually can't escape it because the system now is so ingrained into everything we do" (P. Eaton, personal communication, February 10, 2020).

Changes in technology and the fast growth of data sharing services and collection make it difficult for law to remain updated. Today's world of technology still operates under laws from the 1980's. Under what is called the 'Digital Due Process Coalition'[31], many companies, advocators, and Non-Governmental Organizations (NGO's) have criticized The Electronic Communications Privacy Act for lacking individual privacy protection. Among the main aspects the coalition were transparency and consent. Under ECPA, the government with its agencies do not need a warrant to retrieve individuals' private information, such as emails, cloud documents, or geographical location information the phones generate. The appeal called for a warrant before the government agency investigate or collect any individual's private information.

[31] Check https://digitaldueprocess.org/ for more information on the updates suggested to appeal ECPA and the sheer number of advocates.

In this context of stagnant law and legislation, technology continues to develop, and software updates continue to change SNSs structures and policies. As of 2012, the Federal Bureau of Investigation launched a request for proposals for the development of a SNSs application that ". . . must have the ability to rapidly assemble critical open source information and intelligence that will allow Federal Bureau of Investigation strategic and information operations center (SIOC) to quickly vet, identify, and geo-locate breaking events, incidents and emerging threats"[32](n.p). The request for proposals also stated that ". . . social media has become a primary source of intelligence, because it has become the premier first response to key events, and the primal alert to possible developing situations" (n.p). Regarding SNSs, the U.S. topped the list of countries that send account investigation requests with 134,150 requests to Facebook[33] and over 23,000 request to Google[34] in 2018.

National Security Agency clandestine data collection programs. The National Security Agency continues to monitor data and people's moves. It may not be as obvious as it is in China with measures such as the social credit score (Marr, 2019), but it is still a "...broader regime of security and commodification" (Giroux, 2015, p. 108). In 2013, Edward Snowden, ex-National Security Agency employee, exposed the state of surveillance and its depth. Snowden contacted Glenn Greenwald and Ewen MacAskill, two journalists from the *Guardian*[35], and handed them files

---

[32] Excerpt from the application offer by the SIOC. See appendix 2 for the full application offer.
[33] For more Facebook requests archives, check the reports here https://transparency.facebook.com/government-data-requests
[34] Check more Google requests archives here https://transparencyreport.google.com/government-removals/by-country?hl=en
[35] The Guardian is a UK-based newspaper. Read more here: https://en.wikipedia.org/wiki/The_Guardian

about the National Security Agency practices. Some of the files' screenshots are presented in their article, "NSA Prism program taps into user data of Apple, Google and others" (Greenwald & MacAskill, 2013, n.p). In simple words, the PRISM has direct access to saved and collected data from Facebook, Apple, and Google. In other words, National Security Agency knows about any person or device that is connected to the Internet. Precisely, the agency "...allows officials to collect material including search history, the content of emails, file transfers and live chats" (Greenwald & MacAskill, 2013, n.p).

The PRISM program started its collection of data from Microsoft in 2007. It then expanded to other major information companies, such as Google and Facebook in 2009 and Apple in 2012. The program cost the government about 20 million USD a year. The collection of data involved emails, video chats, voice chats, videos, photos, stored data, voice over IP,[36] file transfers, video conferencing, logins, and SNSs details[37]. The database is grandiose, as it contained data from Microsoft (with its products Skype, Hotmail, etc.), Yahoo, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.

However, the National Security Agency does not stop there. The data collection range extends to smartphones data and calling patterns. According to Free Snowden Foundation[38], location data mapping allows the agency to locate previously unknown relationships between citizens using a system called 'co-traveler.' The

[36] Internet Protocol address is a unique numerical label that is assigned to every device that is used to browse the Internet. Voices recorded on a device are stored under the IP address of that device.
[37] Copy of the PowerPoint leaked by Edward Snowden accessed June 30th, 2019 from https://archive.org/details/nsa-prism-13-1021/page/n3
[38] https://edwardsnowden.com/surveillance-programs/

National Security Agency tools also collect cookies and other data from mobile apps as well as text messages. As of 2016, bipartisan efforts were still working and pressing the agency to define the scope of its data amassment and espionage (Reuters, 2016).

Cohn Marjorie (2017), a professor of law at Thomas Jefferson's School of Law commented on Snowden's revelations and compared them to Orwell's classic novel, *1984*, saying,

> Orwell never could have imagined that the National Security Agency would amass metadata on billions of our phone calls and 200 million of our text messages every day. Orwell could not have foreseen that our government would read the content of our emails, file transfers, and live chats from the social media we use. (n.p)

The swamp of raw data people leave behind on SNSs encourages surveillance. Social networking sites made the individual a center for constant surveillance and data-harvesting (Crary, 2013). The revelations of Snowden are a small window into the workings of the government security agencies (Giroux, 2015). After Snowden's revelations of many classified documents, there is no reason for individual citizens not to inquire about privacy and surveillance (Eubanks, 2014). Skinner and Marshall (2013) argued that if an agency can read a citizen's emails and conversations; then it is not just a loss of privacy, but also a loss of liberty, as the agency has the power to reread the conversations at choice. The power the state has over people's information is indifferent, indiscriminate, and a direct threat to liberty and freedom; consequently, this power shakes the core values of democracy and human rights (Eubank, 2014; Giroux, 2015).

Institutional surveillance, which is not as threatening to the individual as is social surveillance, happens to be the dominant norm of socialization, where "...the state and corporate cultural apparatuses now collude to socialize everyone into a surveillance regime, even as personal information is willingly given over to social media" (Giroux, 2015, p.108). Government watch is the spider net that traps citizens' data permanently and indiscriminately, whether in an intimate bedroom or at a work desk, just like to a hammer, everything is a nail.

Social versus Institutional Privacy and Surveillance

This theme showed that the different populations in the reviewed studies may or may not know about institutional surveillance, may or may not have a privacy concern, but they certainly have concerns about social surveillance. Trottier and Lyon, (2012) remarked that, "Yet for many social media users, surveillance, and especially surveillance-as-control, does not seem to flicker on the horizon. Indeed, it seems that for them, control is in their hands as they choose whom to accept or deny as friends and build their networks of like-minded acquaintances" (p. 91). Payton and Claypoole (2014) emphasized that social surveillance and institutional surveillance may have the same response-behavior, and wrote:

> When a person understands that everyone will hear his opinion, then his opinion tends to be expressed in a way that is more acceptable to his neighbors, his boss, or the local police. If your living room is being watched by video, you are less likely to walk around in your underwear or eat that block of cheddar on the couch in front of the television, even if that' s the way you like to spend an evening. (p. 3)

It is about the freedom of choice, opinion, and liberty of expression. Surveillance, as it is today, we might start thinking, is a direct threat to our democracy and liberty.

Summary of Theme 2

Theme two focused on individuals' concern for privacy and surveillance. Surveillance, as discussed prior, can be social or institutional. Social surveillance happens informally among people, friends, peers, or even within families. Institutional surveillance is carried out by the government agencies or for-profit companies. In theme two I discussed the power of ubiquitous data from SNSs as well as IoT technologies such as Fitbit. Finally, the available means of data collection and public back-end data harvesting are abundant and can reveal quite intimate data about us, such as our psychological traits. All these practices are somehow open, but a many of them remain classified and inaccessible. The state of uncertainty about omnipresent surveillance is at the heart of concern for losing privacy.

Theme 3: Privacy Management and Literacy

This theme focuses on how SNSs' users (e.g., college students) manage their privacy. It also features studies on privacy literacy and how they relate to privacy concern, self-disclosure, and feelings about data collection. In order to trace the literature and provide a better understanding of how all of the aforementioned data streams play into users' and citizens' privacy management, I mapped my themes and subthemes. Figure 21 maps Theme Three "Privacy Management and Literacy," and shows the connected subthemes. The following narrative will fully explain how the literature and MODES I used to inform an understanding privacy management.

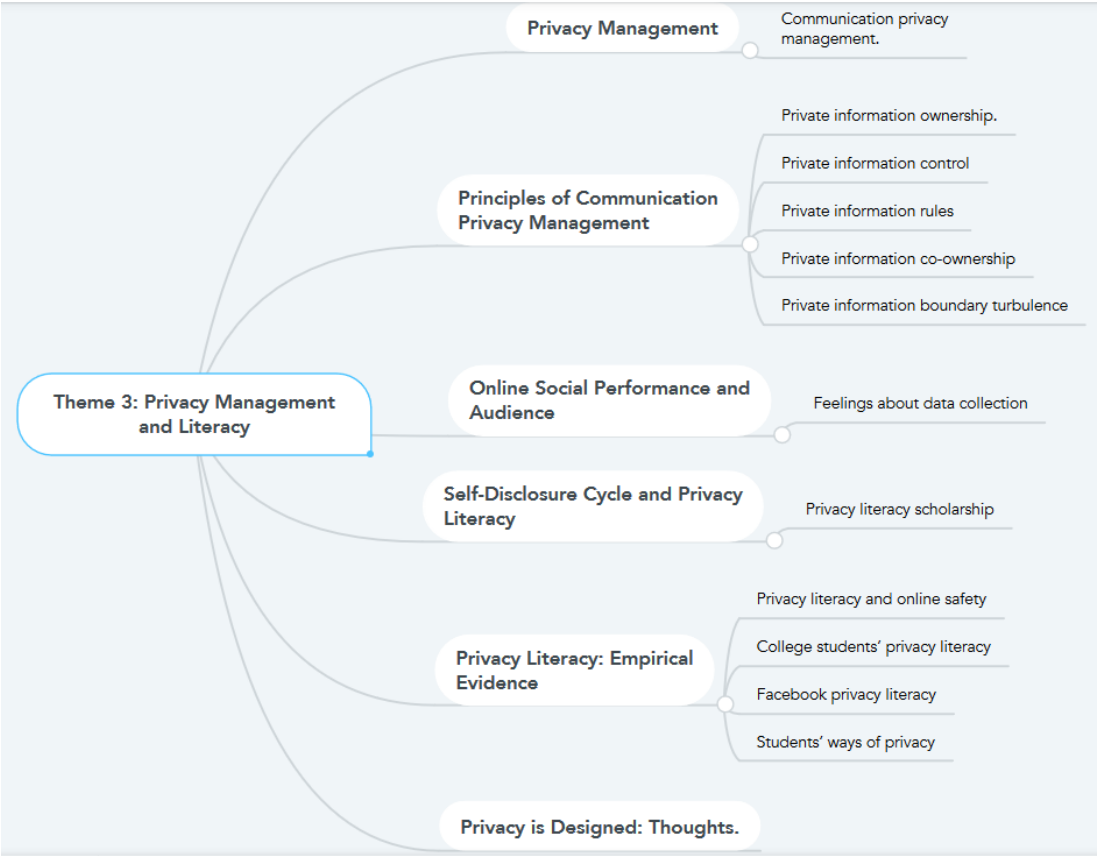


Figure 24. *Mind map of theme three: Privacy management and literacy*

Privacy Management

Social networking sites are arenas for people to connect with each other, share, and exchange a variety of information, including about themselves and others. Self-disclosure feeds relationships and scales them from basic acquaintance to intimate encounter. Altman and Taylor (1973) and Baxter (1988) were among the first scholars to highlight the dichotomy of openness versus closedness among individuals to maintain a relationship. Burgoon, Parrott, Le Poire, Kelley, Walther, & Perry (1989) noted that while this dialectic notion is important in developing and maintaining relationships, equally critical is establishing a threshold for privacy. In other ways, it is important to not disclose everything about ourselves. In this context of privacy literacy research, Petronio (2002) advanced the theory of communication privacy

management and posited that individuals manage their privacy boundaries according to a pre-determined rule-based system.

Scholarship on privacy literacy could be traced back to when Jourard (1964) coined the practice of 'self-disclosure' in the book *The Transparent Self*. Jourard (1971) defined self-disclosure as "... the act of revealing personal information to others" (p. 2). Altman and Taylor (1973) argued that ongoing self-disclosure nurtures and solidifies relationships. This is also true about SNSs' relationships (Henderson & Gilding, 2004). How do different Internet users manage their privacy?, has been one of the main questions asked in literature (Bartsch & Dienlin, 2016; Fortier & Burkell, 2018; Liu et al., 2017; Romo et al., 2017). Communication privacy management (Petronio, 2002) was the most used framework in privacy literacy research and scholarship. Figure 22 shows a QDA Miner Lite frequency analysis of the selected studies for this CLR. Fifteen studies used CPM as their theoretical framework.

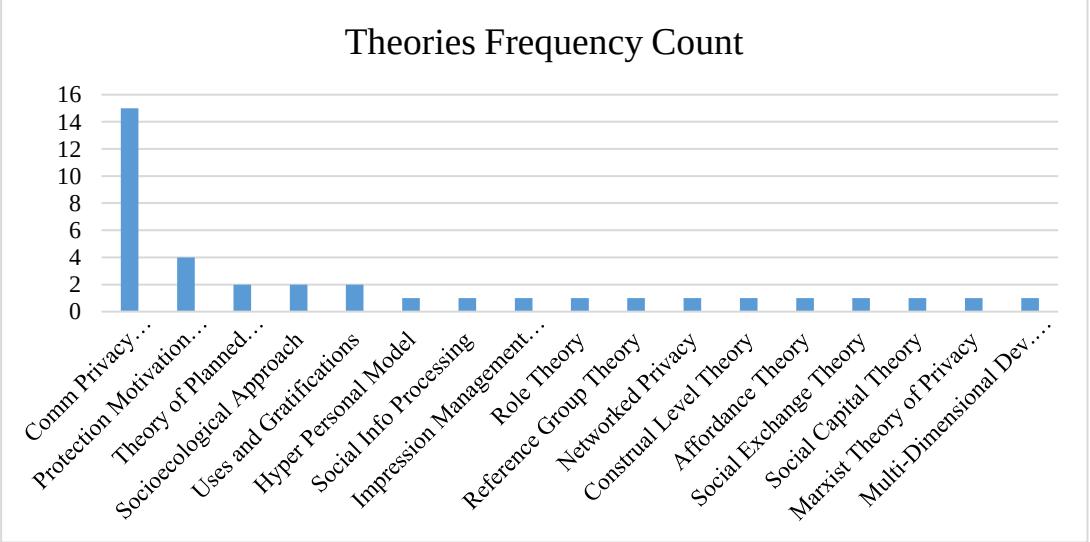


Figure 25. *Frequency count of the theories used in privacy literacy research*

In order to better understand self-disclosure as it relates to privacy literacy, I will discuss communication privacy management theory in addition to other frameworks and strategies that are frequently used in privacy-related studies.

Communication privacy management. Communication privacy management theory posits that information disclosure rests upon tensions of openness and closeness. Like Baxter (1988, 2010), Petronio (2002), prior to SNSs invention, argued that self-disclosure creates a juxtaposition of two needs: to open to others, and to remain private. Additionally, the dialectical tension highlights the interplay of self-disclosure between the individual and others. The existence of such tensions is important as it gives individuals a sense of information ownership and initiates a process of decision making for disclosure. Furthermore, to disclose or not disclose largely depends on the recipients' role in securing the privacy of any disclosed information.

Principles of Communication Privacy Management

Understanding communication privacy management is important to understand disclosure decision making and the consequences of privacy fails and breaches. Communication privacy management also helps explain the individuals' perceptions of privacy and partially explains the privacy paradox, where what individuals claim about privacy regulation misaligns with their actual behavior. The theory is built on five principles: private information ownership, private information control, private information rules, private information co-ownership, and private information boundary turbulence.

Private information ownership. Being able to own information about ourselves is pivotal to privacy as a right. In other words, we have privacy if we ascertain information ownership (Petronio, 2002). Additionally, ownership of information grants people the prerogative of managing their information as they please. Petronio argued that ownership of information is perceptual; therefore, in real life, individuals experience confusion regarding their ownership right. Social

networking sites are an example of a structure that pretends to afford self-managed privacy settings, but the potential for information leaks is abundant (Child, Pearson, & Petronio, 2009).

Private information control. All SNSs afford self-managed privacy setting menus. Controlling the flow of information is especially necessary when information needs to be kept private or secret. The ability to keep the information secret happens with the establishment of a boundary system that requires constant management from both the author of information and the receiver. One of the questions Petronio (2009) raised was whether control would still be possible if a person with firm privacy boundaries established a relationship with another individual who has loose privacy boundaries.

Private information rules. Based on the individuals' ownership and control of information, disclosure follows a certain number of rules that are particular to everyone. In other words, to be able to control the flow of private information, Internet users develop a set of criteria that are important to them and their information disclosure context(s). Factors such as gender, culture, context, privacy calculus, and type of information tend to influence the rules of disclosure and make them frequently amendable. Additionally, the motivation for self-disclosure influences information-sharing rules. For example, disclosure of information to nurture a friendship may affect information rules differently than disclosure of one's financial information.

Private information co-ownership. Co-ownership, also referred to as collective ownership, happens when an individual discloses his/her information to another person or entity (e.g. a financial institution, a school, etc.). The individual or entity that receives the information becomes the co-owner, confidant, shareholder, or guardian (Petronio & Reierson, 2009). Both parties, the owner and the person with

whom the information is shared (i.e., the receiver) work collaboratively to secure the shared piece of information. A break of the mutual rules of disclosure may result in privacy beach or social turbulence. Disclosure rules may be implicit (e.g., "I tell you this news, but I am sure you will not repeat it to anybody") or explicit (e.g., "please keep this secret between us and do not tell anybody"). Negotiations of these rules are ongoing and constant between owners and receivers/co-owners to preempt inadvertent privacy violations and mishaps. When information is co-owned, privacy rules extend, according to Petronio (2002), to three conditions that are necessary to manage privacy: (a) linkage rules, (b) permeability rules, and (c) ownership rules.

(a) Linkage is the decision the owner of information makes to extend their relationship links to other individuals. Said differently, who else may have access to the information at stake?

(b) Permeability explains the degree of openness the owner of information can have with other information receivers. Decisions about how much others should know and how much depth and breadth could be shared with others.

(c) Ownership is the negotiation of how much independence the co-owners/receiver of information can have over information disclosure. Sometimes information is shared with individuals as a privilege, and they may be given no permission to disclose information (Golish, 2003). In this case, the co-owner/receiver of information has no right to share anything further than themselves—the opposite of this situation is also true.

Private Information Boundary Turbulence. The rules for information co-ownership and self-disclosure expectations do not always apply. Sometimes co-

owners of information opt to violate ownership rules for many reasons. The principle of boundary turbulence assumes that mistakes of information leak, misunderstandings, intentional violations, or any mishaps that take place in information privacy management may result in turbulence.

Online Social Performance and Audience

Social networking sites encourage users to engage in self-display. Scholars have described SNSs as exhibition display (Hogan, 2010) or a stage to perform the self (boyd, 2007). Display on SNSs is "…ubiquitous and psychologically valuable, and participants in these spaces engage in the practice because they benefit from it" (Fortier & Burkell, 2018, p. 3). Posting is also encouraged by audience interaction and response, i.e., social validation (Phua, Jin, & Kim, 2017; Quinn, 2016). Moreover, as Litt and Hargittai (2016) posited, users of SNSs also have imagined audiences. Eaton mentioned that ". . . audience is really important to how all of this plays out because some people will try to perform or set up a certain image on themselves for their workplace people. Some people will do it for their families, etc..." (P. Eaton, personal communication, February 10, 2020). Therefore, SNSs' users differ in their ways of release and control of self-display.

Petronio's (2002) communication privacy management is an exemplar framework that explained a rule-based system that people apply to their self-disclosure. The nature of the audience impacts the way users manage their privacy. Audience could be the network of friends or the platform itself (e.g., Facebook). Most SNSs require some personal information release in exchange for having access to their services. Knowing who the audience is, who can see the shared information, and what happens to the shared data is crucial to privacy management (Petronio, 2002).

Feelings about data collection. Morton and Sasse (2014) conducted a study using Q methodology to segment individuals' feelings about their personal data collected by information companies such as Google, Apple, Facebook, etc. The participants ranked statements such as "The technology service will tell me if it is tracking my behavior or location" or "The organization will completely delete all the information it holds about me when I ask it to." Morton and Sasse found most of the participants loaded in each of these categories: (a) information controllers, who want to control their personal data collection and dissemination; (b) security concerned, who expressed a concern over their security and personal information; (c) benefits seekers, who use technology services for the gratifications they receive; (d) crowd followers, who are inspired by what others do; and (e) organizational assurance seekers, who expect guarantees from the technology institutions in exchange for personal data collection. This research was the first of its type to examine participants' points of view about privacy and personal data collection. Internet users act according to their beliefs and perceptions, and this research inspired privacy management and tried to understand why individuals protect, disclose, or simply disregard privacy.

In extension to Morton and Sasse's work, Fortier and Burkell (2018) conducted the same research using Q methodology on Facebook. The goal was to create a typology of Facebook users' feelings about what they share and how they control their audience. The statements were written as, "Before posting photos on Facebook, people should get permission from anyone who appears in them," or "I can use information I find on Facebook in any way I want." The results from 48 participants loaded in three profiles: (a) image control, (b) relaxed display, and (c) personal use. Each of the profiles had a privacy classification and orientation. In other words, the participants who loaded in these profiles managed their privacy differently.

Their perception of privacy guided their behavior. Overall, their perceptions centered around issues related to the complexity of disclosure and participation in the social sphere with friends, family, or even public posts and personas. Image controllers loaded in factor (a): those who had moderate to strong privacy control skills. For instance, these individuals controlled their posts, who could see them, and carefully posted on others' walls. These individuals rejected anybody's access to their postings, except those whom they friended or friend. Interestingly, the individual's used Facebook to lurk around others without leaving traces.

Relaxed displayers loaded in factor (b): these individuals have low privacy control skills. They are 'laissez-faire' individuals on SNSs. They used Facebook to invent themselves and they brand their image carefully. Relaxed displayers trusted SNSs to regulate posted content and they considered Facebook a sharing space. Factor (c) loaded participants with strong privacy expectations—The fundamentalists. They only used Facebook to keep in touch with friends. They had a restricted access to their profiles and did not share identifiable information.

This typology by Fortier and Burkell (2018) is important in beginning to understand some of the perceptions underlying privacy literacy, mainly of Facebook participants. In other words, not every user has privacy control as his/her priority. Also, it is important to know that privacy is challenged by the socialization gratifications SNSs offer people. Not giving up privacy for the socialization gratification of SNSs is a difficult challenge (Blank, Bolsover, & Dubois, 2014).

Self-Disclosure Cycle and Privacy Literacy

Social networking sites' cycle of sharing is multi-faceted. It has four main aspects (Fortier & Burkell, 2018) that influence the user's decision-making and privacy management. Information sharing depends on display, benefits of sharing as

well as the cost, risks, and privacy control skills. To illustrate, *display* reveals the self to others, and this has a *benefit* of relationship building and publicizing of the self. However, the benefit is tagged with a *cost*, that of the possibly of losing privacy. The potential of losing privacy is the *risk* that may result from self-disclosure, context collapse, audience collapse, or unintended audience (Litt & Hargittai, 2014; Marwick & boyd, 2014). The risks could be mitigated with strong privacy literacy skills, i.e., control of personal information (also see Fortier & Burkell, 2018).

Sharing is often driven by culture, motivation, and socialization (Nissenbaum, 2010; Petronio, 2002)—including software socialization (Manovich, 2013). The information sharing cycle sets the ground for understanding privacy literacy and why it is important. Although Fortier and Burkell's (2018) research was based on analysis of SNSs' self-disclosure preferences and intentions, it still helps mapping the profiles of those who use SNSs and their privacy management orientations.

Privacy literacy scholarship. A key dimension of privacy literacy research pertains to how users manage their private versus public personas and how they set the boundaries of self-disclosure to achieve a midway point between accessibility and retreat (Taddicken, 2014; Trepte et al., 2015) or how to achieve a balance between concealing or revealing personal information (Petronio, 2012). For instance, as communication privacy management theory posits, the establishment of boundaries between SNSs users, the boundaries are not meant to be fixed or to keep others outside. The boundaries are points of entry and negotiation among users (cf. Taddicken, 2014).

Privacy literacy has been researched from different perspectives. One perspective posited that privacy problems could be linked to lack of experience with privacy breaches, which may consequently lead to underestimating the risks of losing

privacy (Dienlin & Trepte, 2015). When contacted for a comment, Eaton suggested that ". . . people care less about privacy and personal data protection, because there has not been any major ramification of data breaches yet" (P. Eaton, personal communication, February 10, 2020). The other perspective argued that the lack of declarative knowledge (e.g., knowledge of risks, privacy rights) and procedural knowledge (e.g., protection skills) may reduce the chances that individuals' concern for privacy will transfer to concrete privacy management skills (Debatin, Lovejoy, Horn, & Hughes, 2009; Park, 2013; Trepte, et al., 2015). The third perspective claimed that being savvy about privacy literacy and protection may increase disclosure and reduce the fear of a privacy breach (Turow & Hennessy, 2007). I asked Caitlin Fennessy, the Research Director at the International Association of Privacy Professionals about her opinion on data transparency and she responded, "I think transparency is positive, and from my perspective, the more transparency there is, more likely individuals will call for and demand greater protections in that realm, which I see as positive" (C. Fennessy, personal communication, September 5, 2019).

Baruh, Secinti and Cemalcilar (2017) conducted an extensive meta-analysis of survey studies from 1990 through 2016 on topics related to privacy concern, privacy literacy, information sharing behavior, and privacy protective measures. The list of literature-search keywords pertaining to privacy literacy was exhaustive and contained terms like 'privacy knowledge,' 'knowledge of online security tools,' 'institutional practices online,' and 'social privacy literacy.' Among the seven questions posed for the meta-analysis, four of them measured the relationship between privacy literacy and intentions and behaviors regarding (a) the use of online services and SNSs; (b) information sharing and adoption of privacy protective measures; and (c) privacy concern.

The results indicated that the more SNSs' users were concerned about their information, the weaker their intentions were to share personal information. This category of users had strong sharing intentions and frequently used privacy protective measures. Regarding privacy literacy and the subsequent SNSs behavior, Baruh et al., (2017) found inconclusive results due to the scarcity of studies; however, they noted that high privacy literacy skill may lead to stronger intentions to use SNSs. Due to the lack of research studies, the same inconclusive results were obtained regarding the relationship between privacy literacy and intentions/ behaviors to share information and adopt privacy protective measures.

The last question asked about the relationship between privacy literacy and privacy concern. The answer was that individuals with high privacy literacy tended to have high concerns for the privacy of their information. The meta-analysis was inconclusive in examining privacy literacy and individuals' intentions to use SNSs or to adopt privacy protective measure. The inconclusiveness of the results was due to the lack of scholarship in privacy literacy. Baruh and colleagues' (2017) research was considered "...the first study to systematically evaluate the associations between online privacy concerns, privacy literacy, online service use, and adoption of privacy protective measures" (p. 45).

Privacy Literacy: Empirical Evidence

Privacy literacy and online safety. Bartsch and Dienlin (2016) claimed that privacy literacy is a new lead of research with few studies that examined the underlining principles of the concept and its application. Bartsch and Dienlin researched the relationship between experience with privacy regulations and SNSs' behavior on Facebook. Additionally, the researchers examined the relationship between the experience of using SNSs and the user's perceived degree of online

safety. The results indicated that the more the individual user was engaged with updating the safety measures, the more they acquired privacy literacy skills. Interestingly, the more time the user spent on Facebook was found to enhance his/her social privacy literacy skills. Bartsch and Dienlin concluded that when users applied high privacy literacy skills to their SNSs accounts, they exerted more control over their information; however, the researchers noted that more privacy control may reverse the benefits; therefore, increase privacy concern.

College students' privacy literacy. As an example of college students managing their privacy online, some research focused on college drinkers and their information management to maintain a boundary between formal professional reputation and its informal counterpart (Ridout, Cambell, & Ellis, 2012; Westgate, Neighbors, Heppener, Jahn, & Lindgren, 2014); and how posts of dinking on SNSs can lead to a loss of employment opportunity or job (Brandenburg, 2008).

College students are among the most engaged population with SNSs (Osatuyi et al., 2018). A Pew Internet report showed that about 75% of Facebook users attended or have had some college education (Smith, 2013). It is important to know, however, that little research was conducted in regards to college students' monitoring of self-disclosure and boundaries on SNSs (Romo, Thompson, & Donovan, 2017). In the same vein of argument, scarce research has been dedicated to study college students' concern for privacy and their privacy management skills (Child & Starcher, 2016). For college students, it is important to manage social networking content about themselves and carefully polish their reputation, as they bear a social responsibility towards their friends, family members, as well as a professional responsibility towards their future employer(s). Hence, SNSs reputation management, i.e., management of the self on SNSs requires privacy literacy skills.

Romo et al., (2017) conducted a study to explore how college students established rules and criteria about their SNSs (also called 'social privacy' by Raynes-Goldie, 2010), boundary management, and social turbulence management—following communication privacy management of Petronio (2002). The researchers found that students followed smart posting as the fundamental rule to self-disclosure. Smart posting invokes principles of data permanency and reinforces principles such as pausing and reflecting before posting on SNSs. Students engaged in preserving the permeability, ownership, and linkage of privacy by setting implicit and explicit posting rules with friends and peers. For instance, students concealed alcohol containers whenever around cameras or picture-phones.

Also, posting content was done smartly, as students only posted to select SNSs or agreed upon site between themselves and their friends/peers, i.e., audience. For example, several students used Snapchat when partying or posting alcohol related content, as it faded instantly and sharing was restricted to select friends. At times, friends posted pictures of others, and that created a privacy breach, i.e., social turbulence. Victims of the breach usually untagged themselves to preserve their reputation or sometimes they activated the Facebook review option and simply declined posting the picture on their wall. However, this did not mean the post was removed from the online sphere. Students, in this case, took offline action and negotiated content deletion with the content owner. To practice face-saving in face-to-face negotiation and remediation of turbulences, some students employed strategies such as negative politeness—jokingly or indirectly mentioned the incident. Other students failed to resolve their social privacy breach and their turbulence turned into long-term stress, social vulnerability, and relational strain (Romo, et al., 2017).

Facebook privacy literacy. Based on a year-long digital ethnographic study, Raynes-Goldie (2010) investigated the methods Facebook users took to protect their social privacy. The author defined social information privacy as actively engaging in protecting and controlling personal information on SNSs. Some participants used a real last name paired with an adjective as their first name (e.g., Jackson the Great). Others used their first name with a middle name initial, while others used a completely made-up name. The adoption of a random name was a strategy to avoid appearing in public searches or being located by others. Another strategy to enforce privacy was to delete photos or tags that users knew were public and permanent. Some users had two accounts, one real account and one fake account, and would use the fake account to stalk and check others' activities, exchange links to photo albums about others, and else.

Discussing overly sensitive issues on SNSs could be a real threat to privacy. This discussion often carries out a mixed feeling about needing to share with friends and fear that information is not kept secret. For that, some users adopted strategic ambiguity. Strategic ambiguity (Bavelas, 1983; Raynes-Goldie, 2010) is a communication tactic that happens when individuals intentionally utter what they mean in a vague and ambiguous way with cues that only their peers/friends could use to help decipher the message or attribute multiple meanings to the message. Other researchers (Child & Starcher, 2016) have found that Facebook users also used coded online language that could only be deciphered by their intended audience them in order to exchange sensitive information.

Similar to Child and Stracher (2016), Marwick and boyd (2014) discovered how teenagers use different ways to conceal sensitive and personal information. In

Marwick and boyd's research, students used subtweeting and steganography. A subtweet happens when an individual posts sensitive information or aggressively insults another user without mentioning any personal identifiers, name, ID, location, etc. The assumed idea is that the receiver knows the tweet is addressed to them. In response, the receiver may respond with the same fashion, but adding the hashtag #subtweet. Steganography, a Greek word that means covered script/code, is a method that involves hiding or encrypting the message. For instance, Marwick and boyd (2014) showcased an example of a participant who broke up with her boyfriend. In this example, Marwick and boyd (2014) explained that the participant posted about her break-up on Facebook in order to garner support from her friends, doing so without the knowledge of her parents. She engaged in steganography by posting lyrics from a song that expressed her sorrows, which allowed her to successfully draw her friends' sympathy. Strategies like steganography often happen on SNSs when the structure of the network, or the collapse of audiences and contexts, is used to increase social secrecy (Marwick & boyd, 2011; Nissenbaum, 2010).

Scholars such as Marwick and boyd (2014), boyd (2014), Nippet-Eng, (2010), and Petronio (2002) all considered privacy as a social practice that is based on ongoing context-related negotiations that happen inside networks of individuals (e.g. evidenced by practices of subtweeting and steganography). Altman (1977) was among the first researchers to claim that privacy is contextual and found through his ethnographic meta-analysis that, although privacy is universal, it manifests itself differently in different cultures.

Regarding communication privacy management principles of Petronio (2002), Palen and Dourish (2003) also posited that privacy is an ongoing regulation of rules.

Palen and Dourish argued that “Privacy is not about setting rules and enforcing them; rather, it is the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres” (p. 3). Users of SNSs practice privacy differently and manage their information flows in various ways.

Students’ ways of privacy. To some college students, managing privacy is a matter of who sees their profile and accesses their information. Special and Li-Barber (2012) investigated graduate students’ privacy settings as an indicator of self-disclosure. With 127 graduate students, the researchers found a variety of privacy-related behaviors. Some participants allowed only their personal friends to access their content (54.2%); about a quarter of students allowed their friends from different networks to access their profile, as they had an open/public profile. Additionally, Special and Li-Barber discovered that female students had more privacy settings than males.

In one of the seminal works in the field of privacy literacy, Tufekci (2008) surveyed 601 college students about their privacy settings. She found that although students had concerns for unwanted gaze or audience, 94% used real names on Facebook and 62.8% did the same on MySpace. Most students in the study only allowed their friends to access their content. According to the students, using a real name was a strategy for publicity and job marketing rather than visibility.

Tufekci reported that the students cared more about spatial (i.e., immediate) audience privacy rather than temporal (i.e., future) audience privacy. They restricted access to ‘friends only’ to manage spatial audience. This strategy helped reduce concern for temporal audience or hidden audience (Armerding, 2018). Vishwanath, Xu, and Ngoh (2018) found another dichotomy of privacy management and strategy:

social versus institutional privacy loss. Based on a survey research with 513 students, Vishwanath and colleagues discovered that students activated the settings geared to protect content from leaking to friends and immediate audience more than the settings geared toward protecting information from leaking to institutions i.e., government or SNSs companies. Initiatives like the 'literacy enhancing project launched by Kaspersky Lab (Perekalin, 2019) invites people to mostly care about the social, immediate audience versus the government or SNSs companies themselves.

Using a media ecology lens, Quinn (2014) interviewed a purposive sample of 23 students about their interactions across different SNSs and how they adapted to the interconnected environment while enforcing their privacy management skills. On the ecological perspective, Quinn wrote, "An ecological approach emphasizes the interdependency between individuals and environment, and focuses on behavioral adaptations as a means to surface how valued outcomes, such as privacy, are accomplished" (p. 563).

The study focused on Facebook and Twitter as the outlets for interaction and the researcher asked the participants about their adaptive behavior regarding three ecological layers: Technology, social, and discursive. For each layer, the participants had an adaptive behavior that was motivated by the will to protect and manage their privacy. Concerning the technology layer, the participants knew that Facebook operates on data mining for advertisement and allows third party companies to access the data. Moreover, the participants were aware of content scalability or virality. For this, the participants practiced silence, i.e., to browse without interaction with content or other Facebookers. Additionally, the participants enforced the privacy measures available through the websites to restrict access and mitigate the risk of virality.

The social layer was composed of adaptive measures to filter and select audience. The discursive layer was the communicative option where content travels among users of the same network. The participants suggested less creation of content that may leak and cause them trouble. In other words, they practiced wise content creation and exchange. According to Quinn (2014), wise content management was realized through wise posting, faking profile information, and masking any location-related signs. In this research study, privacy management was interactive and dependent of the ecology in which the user is situated.

Privacy is Designed: Thoughts

The management tips and strategies learned from this literature survey seemed to be limited and are supplied by the SNSs. In other words, users can only protect their privacy through the protection options that are available to them by-design. Privacy depends on the structure of the website or the SNSs in use. This casts away the user's view and application of privacy and imposes the website-creator's view of what privacy is and how it could be managed. Bossewitch and Sinnreich (2013) commented that "The scope and functionality of these privacy settings is limited, unclear and frequently revised" (p. 227).

According to Quinn (2014), some students were aware of the underlying structures of SNSs, the dynamics of privacy available settings, and had issues of continuous mistrust in the network, which then led them to silently interact with services as Facebook. Similar to silent surfing, some users of SNSs engaged in face

painting[39] (Bossewitch & Sinnreich, 2013) or obfuscation[40] strategy (Brunton & Nissenbaum, 2011). Obfuscation occurred when users junked the network with misinformation about themselves, while enjoying the affordances of the tech-service. Similarly, face painters worked by,

> Reintroducing chaos and noise back into the system...[and] protect their identities with a campaign of disinformation and spoof the corporate profiling technologies with odd juxtapositions and preferences. These campaigns also aim to raise awareness around omniscient surveillance, and in particular to critique Facebook's problematic privacy policies. (Bossewitch & Sinnreich, 2013, p. 236)

Hacking Facebook algorithms by intentionally clicking and share content across diverse and conflicting sites and profiles could also be a promising strategy against advertisement profiling and mass surveillance. However, the question is: will these strategies prevent data profiling in aggregate? Will the individual citizen be able of obfuscate every SNS or online space they happen to interact with?

Summary of Theme 3

Theme three addressed the theme of privacy management. Managing privacy has attracted a great number of scholars who attempted to unpack SNSs' user behaviors and privacy literacy habits. The main theoretical framework used for these studies is communication privacy management framework (Petronio, 2002), however,

---

[39] Face Painting is internet slang for the practice of sprinkling a social networking profile with embellishments, fantasy, and satire, often with humorous or political intentions. Retrieved from: https://www.urbandictionary.com/define.php?term=face+painting

[40] Obfuscation is when someone hacks the SNSs algorithm by random clicks, junk posts, and random shares of content.

I explored some of the sub-theories that informed the communication privacy management theory. In this theme, I also discussed types of audiences, and demonstrated privacy literacy as a rule-based skill. In other words, much of the research works included here have investigated methods of data control through co-ownership of content, and negotiations of social turbulence. I closed the theme with some thoughts about how privacy is designed and how software engineering interferes with individual's privacy literacy skills.

Theme 4: Privacy and Law

In today's information age, privacy is an issue of paramount significance for individual freedom, human rights, and democracy (Cohen, 2012; Fuchs, 2012b; Preneel, Rogaway, Ryan, & Ryan, 2014; Westin, 1967; Witzleb, Paterson, & Richardson, 2019; Zuboff, 2015). At the center of privacy debate are concerns of the power relationship between the government, commercial enterprises, and the individual's autonomy in decision making (Gillis & Simons, 2019; Kerber, 2016; Norman, Pepall, Richards, & Tan, 2016).

In order to trace the literature to provide a better understanding as to how all of the aforementioned data streams play into users' and citizens' privacy, I mapped my themes and subthemes. Figure 23 maps Theme 4 "Privacy and Law" and shows the connected subthemes. The following narrative will fully explain how the literature and MODES inform an understanding of privacy and law.

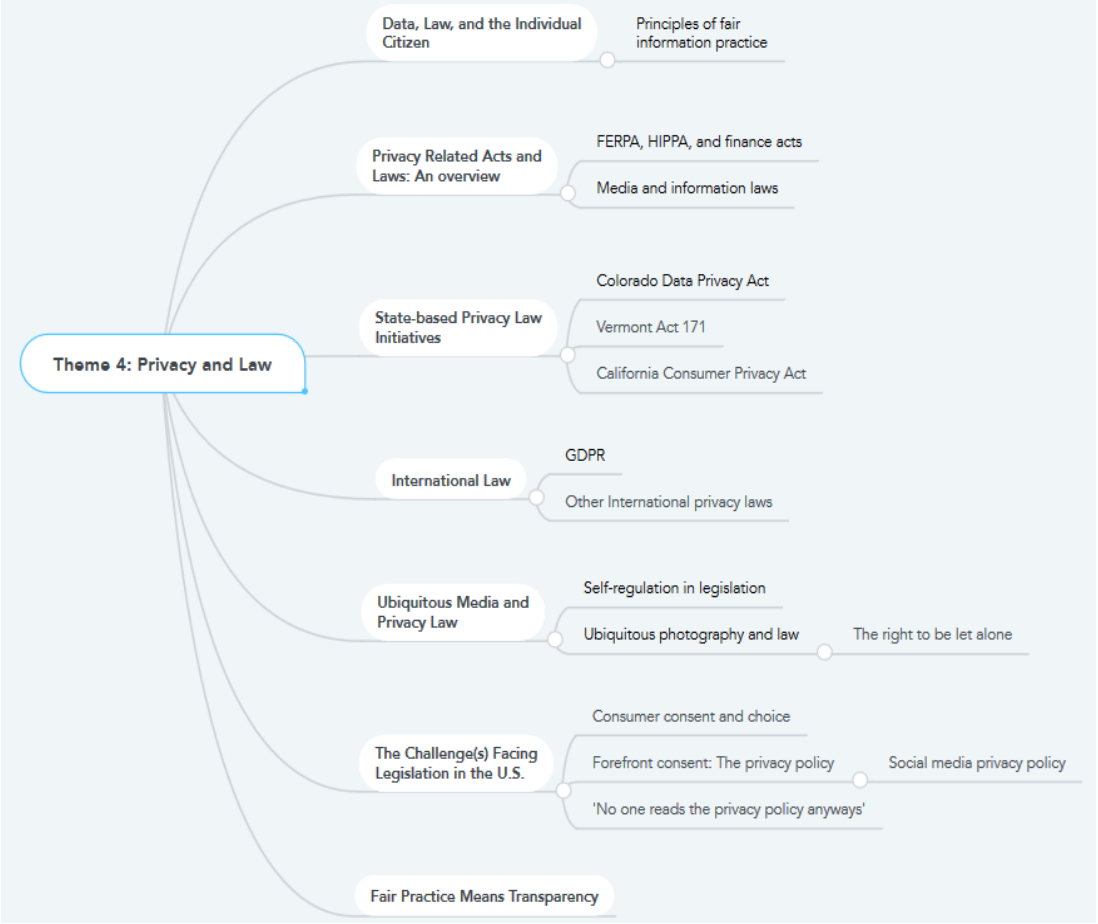


Figure 26. *Mind map of theme four: Privacy and law*

Theme four focuses on privacy law and legislation, but also poses the question of whether the consumer or the individual citizen is (a) protected, and (b) knows the law. Solove and Schwartz (2018) theorized that privacy laws and regulation could restrain individuals' freedom and allow the government and commercial businesses to access and control personal big data. Overall, privacy plays an important role in today's new media age, which is characterized by the desire to be seen (Tufekci, 2008) and the urge to evade public gaze (Altman, 1975; Igo, 2018).

Additionally, the citizens' increasing concern over privacy through grassroot movements, such as the California residents who initiated the California Consumer Privacy Act with over 600,000 signatures (OneTrust, 2018), are spurring companies and businesses to address privacy policies and ascertain compliance with laws and

regulations. Positions such as the Chief of Privacy are now mainstream in many corporations. The Chief of Privacy often develops programs of data literacy and compliance for the workforce that the corporation employs. The leading organization for developing privacy officers is the International Association of Privacy Professionals (IAPP), from which I received training on the California Consumer Privacy Act (CCPA) and the General Data and Privacy Regulation (GDPR) laws. Hence, companies, media platforms, and other service providers need to ensure that their privacy structure and policies are compliant with information privacy laws.

As for now, privacy is taking momentum in legislation and is on Congress's agenda. Many states have already written laws (e.g., Colorado, California) and others (e.g., Texas, Nevada) have consumer data laws awaiting legislation. The other major challenge of privacy application and protection is the individual's privacy literacy and how much data self-protection strategies that they know.

Data, Law, and the Individual Citizen

To understand how law works, as well as where and how it should be applied, one needs to picture the flow of information cycle. Figure 24, as inspired but The National Science and Technology Council's *Privacy National Strategy* (2016), demonstrates the positioning and importance of law and regulation in today's technology-based world. Citizens interact with technology and generate data in giant amounts that are permanently stored for services' optimization. Data storage and management created players called analytic providers, such as Amazon Web Services. Analytic providers work on creating systems empowered by algorithms and software to help collect, store, and manage data. Data processing and commercialization has created a chain of data players in the information-ecosystem: data collectors who collect data; and data brokers, who clean, repackage, and resell data.

The individual customer/user/citizen of technology is the primary generator of data. The interaction of the citizen with the machine and the service provider creates a dynamic and fluid information ecosystem. The fluidity of the space raises issues related to privacy and data safety. For this, law and regulation need to be present within the transactions that are related to individuals' data. According to The National Science and Technology Council (2016), ". . . U.S. legislation has provided specific privacy protections to consumers in an expanding set of areas. However, the progress of privacy literacy and protection has not kept pace with the exponential increase in data collection, processing, and storage, and the resulting risk of privacy" (p. 2).

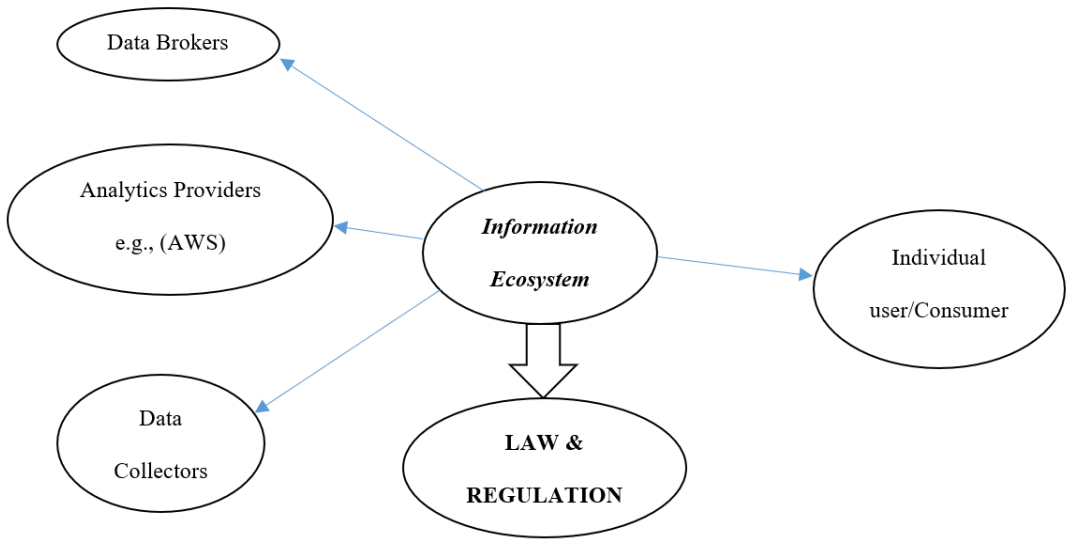


Figure 2741. *Information ecosystem of data players and Law*

Principles of fair information practice. Fair Information Practice Principles (FIPPs) have a long history in the legislation and regulation of privacy. They continue

[41] Notice the customer is in the opposite side to major data players and companies. This is one of the main findings of this literature review: The individual citizen is not a major player as many happen to think.

to influence today's privacy policies and self-regulatory practices of websites and SNSs. The Fair Information Practice Principles developed as a result of the raising concern over data collection practices and the consequences of storing personal data in the 1970's. The Fair Information Practice Principles were first proposed by the U.S. Secretary's Advisory Committee on Automated Personal Data Systems in a report entitled, *Records, Computers and the Rights of Citizens* (1973).[42] The following excerpt from the report pictures the problem of today's privacy law:

> Although there is a substantial number of statutes and regulations that collectively might be called the 'law of personal-data record keeping,' they do not add up to a comprehensive and consistent body of law. They reflect no coherent or conceptually unified approach to balancing the interests of society and the organizations that compile and use records against the interests of individuals who are the subjects of records. (n.p)

Presented with this problem, the report discussed legislation and legal possibilities as well as redefined the concept of privacy. The report had an action agenda which contained many items such as the Congressional necessity to establish ". . . a code of fair information practice for all automated personal data systems maintained by agencies of the Federal government or by organizations within reach of the authority of the Federal government" (n.p). This seminal report laid the ground for the

[42] Record, Computers, and the Rights of Citizens could be accessed here, https://aspe.hhs.gov/report/records-computers-and-rights-citizens

introduction of the Fair Information Practice Principles (FIPPs), which continue to guide today's laws and SNSs' policies.

The Federal Trade Commission published another report, *Privacy Online: A Report to Congress* (1998)[43], in which the five Fair Information Practice Principles were introduced as: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, Enforcement/Redress. *Notice* is a fundamental principle and means the consumer needs to know when a service collects his/her personal data, the amount of data, and the possible uses of data. *Choice* allows costumers control over the options as to how their data are used, including secondary uses inside the company or by third parties. *Access* enables the consumer to access data files about themselves and contest any accuracy or incompleteness. *Integrity/Security* means that service providers take the necessary steps to keep data safe and anonymous. The last core principle, *Enforcement/Redress* happens by creating a body that enforces the above-mentioned principles.

The Federal Trade Commission report of 1998 suggested three ways to enforce privacy laws: self-regulation (e.g., website policies and terms of use), legislation (e.g., state-based legislation that would protect consumers; and/or government enforcement of law through civil and criminal sanctions). Today's online privacy policies are driven, to a greater extent, by the FIPPs. In addition, other privacy statutes were legislated both at the federal and state level.

---

[43] Find full report here, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

Privacy Related Acts and Laws: An overview

FERPA, HIPPA, and Finance Acts. Soon after the Fair Information Practice Principles were initiated in the 1970's, a number of acts and laws were passed to further protect the privacy of individuals. The Privacy Act (1974) was developed by the U.S. Department of Justice's Office of Privacy and Civil Liberties (OPCL). The act established a code that regulates the collection, storage, use, and dissemination of individuals' information (e.g., Social Security Number) that are gathered by any federal agency. Givens (2015) posited that this law did not regulate the private sector; it overlooked the private companies' data collection and processing practices.

Family Educational Rights and Privacy Act (FERPA) of 1974 is the golden standard that enforces data privacy in educational settings such as schools and universities. Family Educational Rights and Privacy Act grants full authority to access educational records to students and parents; it also grants the right to mandatory consent for any third party to access students' educational data; and, lastly, the law allows for the amendment of the records before sharing them with a third party.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established national privacy standards to safeguard identifiable health information of patients. Health Insurance Portability and Accountability Act is the standard of privacy enforcement in medical field nationwide. The Children's Online Privacy Protection Act (COPPA) of 1998 was passed to protect children's data and behavior online. The law prohibits online service providers from collecting, using, or storing data of children under the age of 16 without a parental or legal guardian's consent. In the same line of argument, the Electronic Communications Privacy Act (ECPA) regulates overall information collection, use, and dissemination by businesses. EPCA is consisted of three sub acts: (1) The Wiretap Act, which codifies the interception of

communications; (2) the Stored Communications Act, which regulates the storage of communications and records; and (3) the Pen Register Act, which regulates the use of pen register and tracking devices (Solove & Schwartz, 2018).

In the field of finances, the Financial Modernization Act or Gramm-Leach-Bliley Act of 1999 regulates the circulation of individuals' financial information. Regarding marketing and data harvest, the only existing acts are the Telephone Consumer Protection Act (TCPA) of 1991 and the CAN-SPAM act of 2003. The TCPA protects the privacy of consumers and their right to not receive solicitation calls from businesses to which they object. The CAN-SPAM prohibits soliciting through emails.

Media and information laws. In the field of media and entertainment, the Video Privacy Protection Act of 1988 prohibits the disclosure of identifiable information of consumers' media and video rentals. The same principle requires television cable providers to obtain a consumer's consent to release any personal information under the Cable Communications Privacy Act of 1984. However, Payton and Claypoole (2014) contested that online media providers, such as YouTube, do not abide by the same rules. Givens (2015) explained that the U.S. does not have a federal law that regulates data and online services.

The most relevant act to the regulation of SNSs' data practices is the Social Networking Online Protection Act (SNOPA) of 2012. The Act is supposed to protect employees from submitting their SNSs information, such as log-in credentials, to their employers in the course of a job recruitment. The Act also protects students from submitting similar information to their institutions. The Act is not yet enforced at the federal level, however, as of 2019, SNOPA has been acted in 15 states according to

the National Conference of State Legislatures[44]. Regarding citizen data privacy, there are a few successful initiatives in the U.S. which could be compared to the General Data Protection Regulation (GDPR) law of Europe. As an example, the California Consumer Privacy Act (CCPA) of 2018. The law was signed in June 2018 and became effective in January 2020.

State-based Privacy Law Initiatives

Colorado Data Privacy Act. When this CLR was first conducted, there were three states leading data privacy legislation. First, Colorado with the Colorado Data Privacy Act (enacted Sep. 2018). The act requires that businesses and governmental entities based in Colorado develop and maintain a written policy explaining the handling and disposal of personal data. Additionally, businesses that store, own, or license personal information shall show security mechanisms to protect consumers' data. Coloradans, i.e., citizens of Colorado, should be notified of any unauthorized acquisitions of their data and/or data breaches.

Vermont Act 171. Second is the state of Vermont with the Vermont Act 171, which was enacted in January 2019. This act focuses more on data brokers, collection, packaging, and reselling of consumer/citizen data. The act has four main tenets:

1- Provide consumers information about data brokers and how they handle data.

2- Require data brokers to have adequate security measures to protect consumer/citizen data.

[44] See more details on the bill at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx

3- Prohibit acquisition of consumer/citizen data with intent to fraud.
4- Remove the financial barriers institutions impose to freeze consumer data/account.

California Consumer Privacy Act. The third law, and the most comprehensive of all, is from the State of California with the California Consumer Privacy Act (CCPA), which was enacted in January 2020. Under the CCPA, California residents/consumers have the right to request that businesses disclose data collected about them, the source, and purpose for collection. California residents can request that a business deletes their personal information. Lastly, Californians can opt-out of a businesses' collection and sale of their personal information without retaliation.

Table 18. *Key features of the new privacy laws and their relation to privacy literacy*

Law Initiative	**Key Feature**	**Date Enacted**	**Privacy Literacy Engagement**
Colorado Data Privacy Act.	Businesses need to show data handling and disposal, and ways to protect consumer data	September 2018	Residents are required to be familiar with the various laws. Remain updated about the newly added updates and companies' practices as long as they use their services.
Vermont Act 171	Regulates data brokers, checkups of data security protocols, and	January 2019	Citizens need to understand data practices, brokers' roles, and the trajectory of data processing that is

	citizens can freeze their data/account any time.		usually hidden away from individuals.
California Consumer Privacy Act	Residents of California can request their data file(s); can request data to be deleted; and can request to opt-out from the service data collection.	January 2020	Knowledge of what data points are being collected from various service providers. Individuals need to know how they are opted-in data collection and how they can opt-out.

Federal and International Privacy Law Initiatives

Federal Law. At the federal level, there is not a comprehensive law that regulates data generated by U.S. citizens or connected devices, data processing, dissemination, and exchange—i.e., privacy. Compared to Europe, which has one of the most comprehensive privacy laws, the U.S. has initiatives, laws, and state-laws that together may reach a comprehensive information and privacy law in the future. As of now, a federal data privacy law regulating all personally identifiable information is absent, and the U.S. has minimal restrictions to the management and processing of consumer data (Forrester, 2019[45]).

In the U.S., it is important to note that privacy is articulated in the constitution, but the law enactment of the constitution does not cover the technological advances and human interactions with technology. As technology proliferates, one may pose the

[45] Check the privacy heat map here to obtain an idea about administrative restrictions to privacy regulation: http://heatmap.forrestertools.com/

question of whether these laws are responsive to the current and future dangers of information privacy (Solove & Schwartz, 2018). Several amendments in the constitution referred to privacy:

Table 19. *U.S. constitution Amendments and their relation to privacy*

Amendment	**Amendment text**	**Relation to privacy protection**
First Amendment	Protects the right to speak anonymously, the right of belief, and religion.	This protects the physical privacy of people as well as the moral capital.
Third Amendment	Protects citizens' homes against unauthorized uses (mainly by soldiers) without the owner's consent even at times of war.	It provides privacy of the home, property, and allows for the freedom of consent.
Fourth Amendment	This amendment protects people and their homes and belongings from unjustified searches and seizures.	This amendment is the closest it could be to the protection of personal identifiable data.
Fifth Amendment	The amendment protects against self-exposure and grants people the right to remain silent.	The amendment it limits the government in forcing individuals to divulge things about themselves.

Ninth Amendment	says that the "Enumeration in the Constitution of certain rights shall not be construed to deny or disparage other rights retained by the people" (FindLaw, 2019, n. p).	This amendment, according to Sharp (2013), is interpreted as a protector of privacy in ways that are not clearly stated in other amendments.

The U.S.' constitution does not specifically mention the word privacy or consumer data (Solove & Schwartz, 2018), but through the aforementioned amendments, it guarantees, to a certain degree, personal privacy.

Currently, there are comprehensive legal proposals under negotiations; these proposals may lead to a comprehensive law that shall govern big data, data exploitation, citizen targeting, and extensive data collection of individuals. Debates on privacy in the U.S. intensified more since Snowden, the ex-NSA worker who leaked unclassified government document in 2013 about invasive, real-time, and abusive surveillance practices on American Citizens. As of 2018, several privacy law proposals were introduced to congress: The CONSENT Act, Social Media Privacy Protection and Consumer Rights Act, DATA Act, Information Transparency and Personal Data Control Act, Consumer Data Protection Act, and Innovative and Ethical Data Use Act (OneTrust, 2019). In the present time, information privacy is regulated within states; through the federal constitution; through some information and telecommunication acts in addition to self-regulation policies that technology providers write and impose on consumers.

Fennessy, mentioned that "… I actually do think we will see it. And I think we'll see it, in my personal view, when industry feels enough pain from divergent state laws to demand action from Congress. The more state laws we have, I think the more likely we'll get to a federal law" (C. Fennessy, personal communication, September 5, 2019). Renee Williams, attorney-at-law extensively elaborated on the issue and said to me, "One of the biggest concerns that I have as an attorney in privacy is that there's no uniform federal legislation. Every state does something different. Every state has its own privacy initiative or law." She then examined the California Consumer Privacy Act (CCPA), one of the U.S. most comprehensive privacy laws, and said, "... let's take the California privacy law, which is somewhat similar to the GDPR...It doesn't have the teeth that I feel like privacy legislation should have." When I asked her about a possibility for a federal legislation, she responded, "What I'm hoping for is somewhere down the road, we will have federal legislation that all the states have to comply with. Something that is not industry specific, you know, but it needs to address privacy altogether. However, I think we're a long ways from getting there" (R. L. Williams, personal communication, February 24, 2020).

The government may impede privacy laws. The previous theme mentioned the National Security Agency clandestine surveillance and mass data collection. Speaking of law, most acts relevant to data protection were passed in the beginning the 1970's, with the growth of computer use and development of data storage techniques. However, it is also important to know that there are laws that limit the privacy of U.S. citizens. Specifically, the government impedes the development of privacy protection through acts that mandate data storage 'in case' of presumed future investigations. For instance, the Bank Secrecy Act of 1970 mandates banks and

financial institutions to store detailed reports of citizens' financial transactions to assist in government investigations, if needed. Communications Assistance for Law Enforcement Act of 1994 requires phone and cable providers to facilitate government interceptions of communications and surveillance (Solove & Schwartz, 2018). Moreover, the U.S. PATRIOT Act of 2001 has many sub-acts that regulate electronic surveillance and facilitate law enforcement access to information.[46]

International Law

Regarding international law, the U.S. is a member of the Asia-Pacific Economic Cooperation (APEC) since 2004. APEC includes China, Japan, the Russian Federation, Australia, New Zealand, Peru, Indonesia, Mexico, Singapore, Thailand, and Vietnam. The agreement was signed to protect personal information of citizens across borders and guarantee the security of personal records (Solove & Schwartz, 2018).

The General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) is a law applicable to the European Union. It regulates the collection, processing, and distribution of personal data. The law became effective on May 25th, 2018. According to the *Official Journal of the European Union*[47], the GDPR is much inspired by the Charter of Fundamental Rights of the European Union, which states that every individual is entitled to the protection of his or her personal data. The GDPR protects natural persons regardless of their nationality or residence.

---

[46] For more insights about privacy and information law check Solove & Schwartz (2018).
[47] The entire text of law from the official journal of the European Union could be accessed here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

The law is intended to protect freedom, security, justice, and the well-being of natural persons (i.e., anyone who lives in Europe or EU citizens outside Europe).

The GDPR law has 11 chapters and 99 articles. The law outlines the possible ways of processing of data; it requires transparency, consent; and it allows the consumer to limit their data processing, amend and/or delete their records. Additionally, the GDPR has laws prescribed to regulate the course of data processing and to impose that data is securely stored and completely anonymized. Lastly, the GDPR also regulates the transfer of data both nationally and internationally, and imposes penalties and fines on violators.

The GDPR regulates U.S. businesses that operate in Europe (e.g., Facebook, Google) or E.U. citizens that travel for work or schooling in the U.S. The California CCPA applies the same requirement on California residents, whether inside California or outside. For this reason, current training on privacy law is mostly focused on the GDPR and CCPA as they are the two most comprehensive privacy and information laws within the U.S..

Other international privacy laws and initiatives. In addition to the E.U.'s comprehensive GDPR, there is the Brazil Lei Geral de Proteção de Dados (LGPD) data protection law that was enforced as of February 2020. The data protection law applies to any business that processes personal data of Brazilians. The main goal of this law is to guarantee that personal data are protected and anonymized. Also, the Brazilian citizen has the right to rectify data, delete, give, or refuse consent (Brook, 2019). In 2001, Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) to regulate all businesses or government agencies that collect personal information on Canadians (Solove & Schwartz, 2018). Future laws include the possibility of the European Union ePrivacy, the Indian Personal Data

Protection Bill, the Chile Privacy Bill Initiative, the New ZEALAND Privacy Bill, and the U.S. Federal Privacy and Information Law (OneTrust, 2019).

Ubiquitous Media and the Context of Privacy Law

In the U.S., the race for data and information processing created a monetary value and attached power to human digital footprints. As citizens, almost everything we do generates data. These data, in aggregate, have become a prized commodity. West (2019) in her article, "Data Capitalism: Redefining the Logics of Surveillance and Privacy", shed light on the power of online networks, big actors of data, and inspectors of human behaviors, i.e., surveillance actors. West posited that data capitalism started in the 1990's with the Internet turning from a place of selling and exchanging goods and services to a place of harvest of behavioral traces and personal data. According to West (2019), "Data capitalism is, at its core, a system in which the commoditization of our data enables a redistribution of power in the information age ...[and in a way that is]... asymmetrical and weighted toward the actors who have access and the capability to make sense of data" (p. 23). Big actors such as Google, Facebook, and Amazon have the power to influence behavior and opinion as they control information (Zuboff, 2015). Not only that, but they also influence legislation (Fujisaki & Kang, 2019).

Self-regulation in legislation. Self-regulation is one of the key foundations in the U.S.' consumer privacy law and legislation (Papacharissi & Fernback, 2005). Self-regulation happens in gray areas of current law, or when new practices emerge outside the law scope. As of now, social networking companies operate in a realm of law that is not fully regulated yet (Papacharissi & Fernback, 2005). Hence, this means company's self-regulation through policies and terms that are posted on different websites (Celeste, 2019). The privacy policies are considered as legal notices that

describe the information collected; how it will be processed and shared; and how it will be secured if stored (Solove & Schwartz, 2018).

Within the U.S., the perception of privacy and how citizens petition for it to be legislated may be in direct conflict with the capitalist intentions of the main technology and marketing leaders. Caitlin Fennessy, commented that, “Historically, industry has been opposed to federal legislation worrying that something too prescriptive or too similar to GDPR would really thwart innovation. Industry’s reticence was a major hold up. Now, I would say industry is largely supportive of federal privacy legislation, in part because of the plethora of state laws that create additional compliance burdens and potentially conflicting requirements” (C. Fennessy, personal communication, September 5, 2019). Fuchs (2012b), a capitalism and privacy scholar, commented on business orientation of U.S. companies and privacy. He wrote,

> privacy under capitalism can best be characterized as an antagonistic value that is, on the one hand, upheld as a universal value for protecting private property, but is, on the other hand, permanently undermined by corporate and state surveillance into human lives for the purpose of capital accumulation. (p. 141)

Data are also beneficial. For instance, Google Maps user-data helps suggest the best routes for drivers to take; this helps reduce fuel consumption, manage traffic, and save time (Kosinski, 2019). The availability of information about a consumer’s behavior and interests may be used to generate powerful holistic behavioral trends of consumers to benefit businesses and improve service (Acquisti, 2004; Turow, 2012). Consequently, failure to optimize and develop new services could occur should data become unavailable for businesses to use (West, 2019).

Ubiquitous Photography and Law

In modern democracies, privacy is a primordial value and a universal right[48] that establishes individuals' freedom of choice and privacy. Warren and Brandeis' (1890) seminal article, "The right to privacy", is considered the cornerstone of common law: the 'right' to be let alone (Joyce, 2015; Solove & Schwartz, 2018). Warren and Brandeis' (1890) work came in the context of ubiquitous access to photography and the introduction of the camera lens to the lives of public figures. In the 1880's, communication technology advanced enormously; lithographic print was introduced; and yellow journalism[49] and institutionalized gossip started to spread, which resulted in a blur of the public and private boundaries (Shapiro, 1998). Beginning of the 19th century witnessed a growth of paparazzi photographers and investigative journalists who challenged the boundaries of the sacred domestic. New media progressively granted the grand public access to previously private places and information; this therefore inspired Warren and Brandeis (1890) to write their landmark article that laid out the ground for a the 'right to be let alone' common law.

The right to be let alone. Warren and Brandeis (1890) argued that a common law should protect life, property, feelings, intellect, as well as any of the human possessions, tangible or intangible—all this is regardless of the social and economic changes. The two legal scholars expressed their concern regarding emerging media in the 1890's and posited that photography has intruded the private space and that ". . .

---

[48] See art 12 of the *Universal Declaration of Human Rights* ('*UDHR*') and art 17 of the *International Covenant on Civil and Political Rights* ('*ICCPR*').
[49] Yellow journalism was a term coined mid 1890's to depict newspapers that write less-research news and use eye-catching headlines.

numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops" (p. 195). Warren and Brandeis suggestion of the right to privacy against media came before the computer or Internet were introduced to the public. They concluded their reasoning stating that law should "... protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds" (p.206).

The Challenge(s) Facing Legislation in the United States

The current challenge in law and regulation in the U.S. lies in the complexity of the new mediated environments, such as SNSs or the Internet of Things tools such as Alexa of Amazon. These smart devices enabled private information to be communicated in networked spaces and be aggregated across spaces, making it complex for laws to adjust to such fast moving technologies (Bast & Brown, 2013; Waldman, 2019). Additionally, lack of consensus over the concept of privacy and what it means in practice continues to increase complexity for legislation (Solove & Schwartz, 2018). Examining laws and state-based initiatives, a number of legal law scholars and practicing professionals agreed that technology has caused privacy erosion (Bast & Brown, 2013; Joyce, 2015; Solove & Schwartz, 2018; Waldman, 2019). In Bast and Brown's (2013) words, "Federal and state statutes may very likely be found by courts not to apply to many types of advances in technology, leaving the individual with an increasingly shrinking realm of privacy (p.19)". Or as Waldman (2019) argued, "Privacy law—a combination of statutes, constitutional norms, regulatory orders, and court decisions—has never seemed stronger (p. 1)".

In addition to the incomplete law coverage of privacy erosions, Waldman (2019) added that ". . . privacy law's most important tools—including, privacy by

design, consent requirements, and Federal Trade Commission consent decrees—are so unclear that professionals on the ground have wide latitude to frame the law's requirements (p. 4)". Lack of clarity and lack of comprehensibility on the current information privacy law has left several gaps unfilled. The gap in law is filled by third-party practitioners and software engineers who then apply their own understanding and interpretation of law to software (Waldman, 2019; Solove & Schwartz, 2018).

Consumer consent and choice. Law and technology are two sides of the same privacy coin and operate interchangeably. People acquaint privacy laws through legal notices and privacy policies on different websites. Some questions are important for the analysis of privacy policies and information law enforcement. How are privacy policies used by corporations to interpret law and protect the consumer? How are consent and choice guaranteed by privacy policies?

The Future of Privacy Forum and Data Guidance (2018) have released a new report[50] that compares the GDPR of Europe to the CCPA of the United States. Both laws decree that the individual consumer must be informed prior to or while data are being collected by businesses and consent must contain elements such as type of information, purpose of collection, and data processing. Compared to the GDPR, the CCPA further obliges businesses to include a link, "Do not sell my data," on their websites allowing customers to opt-out of data selling. Both laws grant customers the

[50] Full report is available at https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

right to opt-out of data collection and the right to data erasure. Renee Williams, an attorney at law specializing in healthcare law posited that companies work with a fashion that "...we're going to opt you in automatically, but if you tell us you don't want to participate, then we will opt you out and we won't share your information." She added that, "Most people don't even know what opt-out means or even how to go about doing it, because they don't even know that option exists." When I asked her why companies mask these options away, she commented, "...these companies are relying on the fact that you don't know what your rights are, and that enables them to continue to use your information; it is more marketable and more profitable for them" (L.R. Williams, personal communication, February 24, 2020). With that said, data consent is about transparency and clear communication of what data are collected, why, and what will be passed on to third parties. Additionally, an essential part of consent is to offer choice and ability to control one's data and personal information, as well as, choice to opt-in or out without service disturbance(s).

Forefront consent: The privacy policy. Cate (2006) criticized the Fair Information Practice Principles (FIPPs) and described them as unsuccessful. Cate explained that, "Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice" (p. 343). This quote highlights the main criticism researchers have made about privacy policies. For instance, Papacharissi and Fernback (2005) and Silverman (2015) posited that online privacy policies do not fully adhere to the principles set forth by the Federal Trade Commission. Cate (2006) added that the notice principle i.e., privacy policy, does not give choice to the users and is often written in technical and complex language.

Social networking sites privacy policy. Ideally, SNSs' privacy policies inform users about how information is collected, stored, and shared with third parties (Givens, 2015; Waldman, 2016). There is, however, another reality to SNSs' privacy policies. For example, Fuchs (2014) claimed that Facebook's privacy policy is focused on privacy for the company's benefit and offers little protection to the individual users. Fuchs added that SNSs' policies could not be considered as offering consent, since they do not ask the users if they want their data sold to third parties. Personal data as defined in the GDPR (Chapter 1 Article 4) is "Any information relating to an identified or identifiable natural person ('data subject')." In light of this definition, privacy policies should require consent from users on anything they collect, store, or sell to third parties.

The GDPR, as well as the CCPA, account for the protection of two types of data that are relevant to SNSs. The first type is the content individuals generate share, such as posts, comments, likes, videos etc., and the other is the one that companies generate to profile and study people's behaviors (Wahyuningtyas, 2017). However, the way are SNSs' engineered influences law interpretation and application (Waldman, 2019).

The core problem about the privacy policies, as summarized by Papacharissi and Fernback (2005), is that "Privacy statement formula follows in the tradition of self-regulation prevalent in the U.S. which is founded on a lack of government involvement in regulating consumer privacy" (p. 719). Waldman (2019) added that privacy engineering may add complexity to the role pf privacy policy and compromise a larger amount of citizens' data. The researcher declared that "Outsourcing privacy law compliance to engineers can further erode traditional paradigms of expertise, including those taught in law school, that ensure social and pro-consumer values at

least have a seat at the table in practice" (p. 5). In other words, SNSs' self-regulated privacy engineering and policy writing may promote business profitability and innovation advancement, but may also put citizens' privacy at risk.

Privacy policies as they are written and designed require at least a reading level of a college sophomore-student (Garber, Alessandro, & Johnson-West, 2002). Privacy policies, are often designed to support the firm's business model versus the needs of the end user (Fuchs, 2012). Waldman (2019) further posited that privacy policies assure people about privacy protection, while hiding the true protection of their data.

'No One Reads The Privacy Policy Anyways'

The individual citizen, in addition to being the primary actors in the technology and privacy law ecosystem, are also reluctant readers of privacy policies and notices (Monteleone, 2015; Obar & Oeldorf-Hirsch, 2016). In their survey research with 543 SNSs users, Obar and Oeldorf-Hirsch (2016) discovered that 74% of users skipped the privacy policy as well as the Terms of Service (ToS) for a quick join of the service. The researchers found that it required the participants 73 seconds on average to read the privacy policy and 53 seconds to go over the ToS. The counted seconds were deemed enough for the participants to skip the terms and hit 'join' button. Among the takeaways from this research, according to Obar and Oeldorf-Hirsch, was that information load and lack of choice were factors that pushed the users to join the service without any further readings. Researchers also found that most Americans find the privacy policy lengthy and difficult to understand; hence, most of them skip it or spend less time skimming its content (Turow, Feldman, & Meltzer, 2005; Reidenberg, Breaux, Cranor, French, Grannis et al., 2015)

According to Brandimarte, Acquisti and Loewenstein (2013), users of SNSs and other online services usually disclose information about themselves when they feel in control of their privacy. In a Pew Internet survey, Smith (2014) discovered that the American public overestimates the privacy and data protection afforded by the privacy policies documents, especially when a company uses phrases that contain words, such as confidentiality or data security. Brandimarte, Acquisti, and Loewenstein (2013) further investigated the idea of user control and found that SNSs' users disclose more data if they feel they have control over how their data are collected and managed.

Solove (2007), the chevron researcher of information and privacy law, explained that as long as people feel in control of their information, they self-disclose data regardless whether their control is real or not. He added that users of SNSs and other online services underestimate privacy risks when they feel in control of their information. Privacy policies and privacy settings are tools commercial companies use to make users feel in control of their data (Solove & Schwartz, 2018).

Fair Practice Means Transparency

The principles of fair practice as advanced by the Federal Trade Commission, as well as privacy laws, requiring businesses to provide notices about data collection practices and allow individuals to have control over those practices (Cranor, 2012). The standard engineering of the Federal Trade Commission principles has been through privacy policies, pop-ups, and added clickable button such as "Do not sell my data" –with the California Consumer Privacy Act Research (e.g., Cranor, 2012; Monteleone, 2015; Papacharissi & Fernback, 2005; Turow, Hennessy, & Draper, 2018) showed that privacy policy is a poor way to alert the individual citizen of how personal data are collected and processed. These policies are often written by lawyers

and are meant to match the business' profit objectives rather than protect citizens' privacy (Papacharissi & Fernback, 2005). Moreover, most people skip reading privacy policies and spend little time reading in-depth (Obar & Oeldorf-Hirsch, 2016). Cranor (2012) posited that "These policies are long, complicated, full of jargon, and change frequently" (p. 274). McDonald and Cranor (2008) estimated that it would cost an individual, in average, 244 hours per year and an average of 40 minutes a day to read privacy policies of websites.

Social networking sites, such as Facebook, give users no bargaining power on their data. Hence, the policy informs the consumer and protects the company in case of a law suit instead of offering the individual user a legitimate and transparent consent (Wahyuningtyas, 2017). The no choice but 'I agree' model of SNSs' is not an informed consent. The "...user consent per click does not always represent the real intention of the respective user to give [his or her] agreement to the terms being offered" (Wahyuningtyas, 2017, p. 795). Monteleone (2015) agreed that privacy notices fail to provide the necessary protections for Internet and SNSs' users. There are a plethora of examples of data breaches and violations of privacy policies, terms of use, security protocol, as well as legislation (e.g., Yahoo, Equifax, and Cambridge Analytica), which show that privacy policies are not a guarantee of data security.

Data breaches that are declared to the public have received fines from the Federal Trade Commission. However, not all data breaches are announced. As an example of Federal Trade Commission fining process, in September 2019, YouTube, a product of Google, received one of the biggest fines a tech company has ever received with $107 million. The Federal Trade Commission fined the company for knowingly and illegally collecting children's data and using these data for ads (Singer & Conger, 2019), which violates the Children Online Privacy Act (COPA). In 2017,

Equifax was found guilty of the largest breach of all time, as it exposed 147 million American financial records[51]. The Federal Trade Commission settled the case with a fine of $425 Million in order to help people affected by the breach.

Turow, Hennessy, and Draper (2018) conducted an archival data analysis with a large U.S. demographic using the 2009, 2012, and 2015 Annenberg public surveys. In their analysis, the researchers focused on the trust users have in privacy policies. They discovered that young adults who misunderstood privacy policies believe that the protection regulations mentioned in the policies are solid. Additionally, Turow et al., summarized the situation about privacy policies, and posited that "Thirteen years of research show consistently, though, that the label [privacy policy] is deceptive. A strong majority of Americans thinks it means that firms will not use their information without their permission (p. 476)." Privacy literacy could be a powerful beginning towards understanding the structure of media and technology as well as corporate practices.

Amidst these breaches, lack of comprehensive legislation, no bargaining power on the part of the citizens with the giant companies, and lack of transparency on the part of service providers, the individual citizen is left with scarce options to protect their privacy. Among those choices is privacy literacy that brings awareness of institutional practices, legislation, and context-savvy self-disclosure (Trepte, et al., 2015). Data will continue to fuel technology and life, as the next theme will show. Additionally, the law is unable to maintain pace with technological advances (Solove

[51] More details about the Equifax breach are available here https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

& Schwartz, 2018; Payton & Claypoole, 2014). Noticeably, innovations in technology are so helpful for society's well-being; however, that comes with a price tag on an individual's privacy. This debate leads to the questions of whether privacy has ended, and whether there will be a federal privacy law in the future.

Summary of Theme 4

Theme four was an opportunity for me to branch outside of software, technology, and education to the field of law. The major theoretical framework of the comprehensive literature framework advocates for the 'right to be let alone' (Warren & Brandeis, 1890). Theme four discussed recent law developments and companies' law practices and how they are informed by Warren and Brandeis (1890) seminal work in privacy. For instance, the theme synthesized discussion related to privacy policies and companies' self-regulation and discussed how these policies and self-regulation principles should be informed by 'the right to be let alone'. In this theme, I also interviewed key experts in the field of legislation and research. Their insights were hopeful as to the possibility of moving issues related to citizen privacy in SNSs use into U.S. federal law in the near future. Amidst all these law changes, the theme posed questions relevant to the individual citizen' knowledge of law, and whether law and technology will come to a consensus.

Theme 5: Big Data and Future of Privacy

Six-in-ten Americans, about 60%, would like to learn more about how to protect their privacy, and about 67% agree that current laws do not suffice to protect their privacy (Rainie, 2018). A Pew Internet survey (Auxier, Rainie, Anderson, Perrin, Kumar, & Turner, 2019) reported that seven in 10 Americans believe that their personal data are less protected than it was five years ago. What does the future of big data and privacy look like? This question is the focus of the current theme.

A Pew Internet and Elon University survey of 1,021 information experts inquired about the future of large data sets and yielded mixed results, where 53% predicted that the future of big data is likely to be beneficial for society at almost all levels; and 39% of the respondents deemed big data will have a negative impact on society (Anderson & Rainie, 2012). Technology is marching forward with haste, and, with the massive data it generates, it poses various threats to privacy. With that, some scholars think that privacy is officially dead, and that future society will benefit more from transparency of data (Aldritch, 2015; Kosinski, 2017; Webb, 2019). In order to trace the literature to provide a better understanding as to how all of the aforementioned data streams play into users' and citizens' data sharing, I mapped my themes and subthemes. Figure 25 maps Theme 5 "Big Data and Future of Privacy" and shows the connected subthemes. The following narrative will fully explain how the literature and MODES inform an understanding of data and the future of privacy.

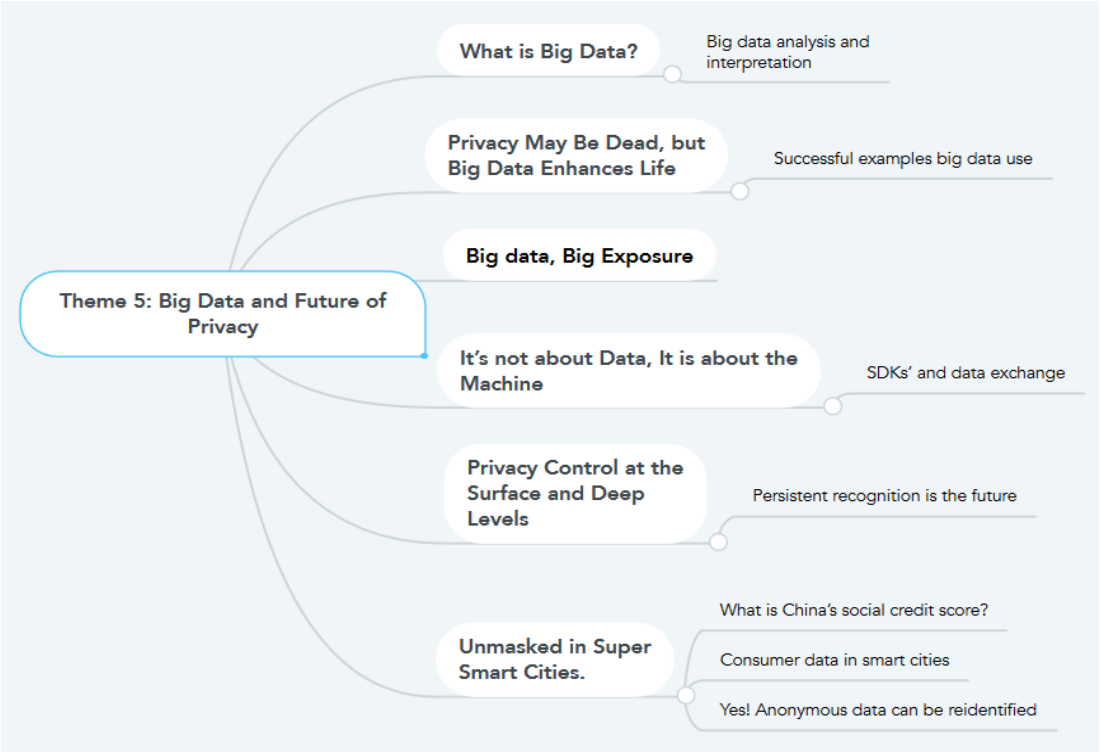


Figure 28. *Mind map of theme five: Big data and future of privacy*

What are Big Data?

Big data are data that a human brain cannot process and they require sophisticated machines for analysis and packaging. As an example of big data, YouTube users upload 500 hours of new content per minute; Google processes 3.8 million searches per minute (Warzel, 2019); and Facebook users upload 300 million new photos daily and reach eight billion video views a day (BroadbandSearch, 2020). These are numbers and data-bytes that we can only think about in the abstract. Big data come from the ". . . widespread diffusion of digital devices that have the ability to monitor our everyday lives" (Newell & Marabelli, 2015, p. 3).

Big data require sophisticated software and machine. In another example of big data, Facebook stores about 111 megabytes of photos and videos per user (Tucker, 2013), who now make up about 2.2 billion monthly active users (BroadbandSearch, 2020). That is more than 100 petabytes of personal information. Like Facebook, Acxiom is another massive data company. Acxiom has a database that is growing rapidly. As their website indicates[52], the company covers over 62 countries with 2.5 billion reachable consumers i.e., about 68% of the world's active Internet users. In the U.S., Acxiom has more than 1500 piece of information per individual. The size of Acxiom's database is huge and is used for audience research, marketing, and business enhancement. The company, for instance, holds various pieces of data about individuals and families/groups, as shown in the figure below. According to the

[52] https://www.acxiom.com/

company, the data have been curated from information that people have entered in surveys and censuses around the world.

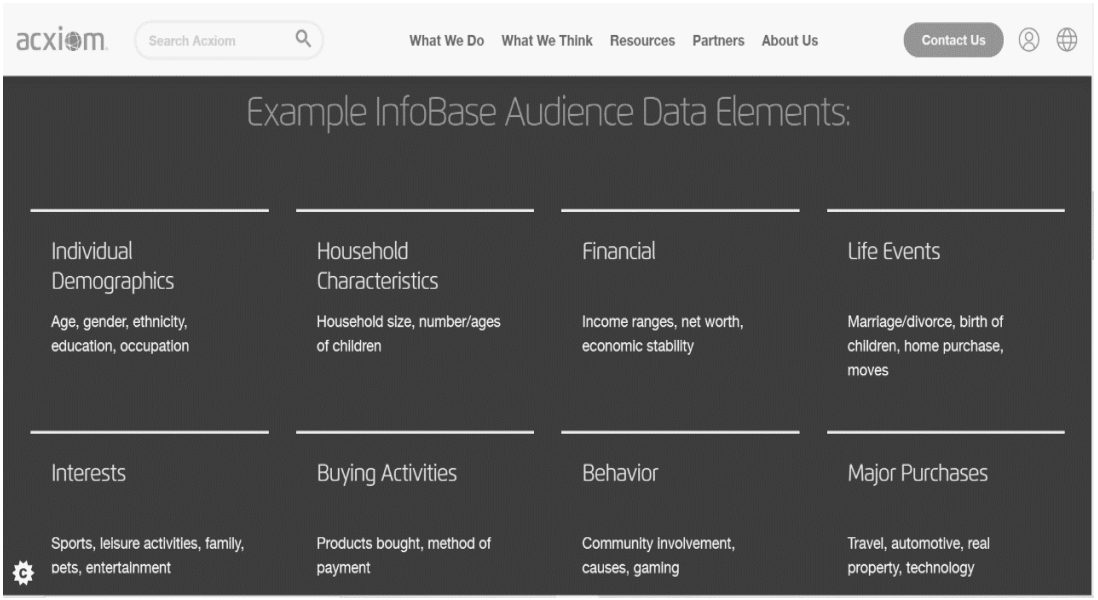


Figure 29. *Snapshot of audience data elements provided by Acxiom data management company*

Big data analysis and interpretation. Big data, as in raw or aggregate data, may or may not mean anything about the population from which they were drawn. However, the ability to access, mine, and engineer powerful machines to clean, process, and draw predictions and insights is what makes big data powerful and a privilege (Lanier, 2013). Just like privacy, definition of the phrase ‘big data’ is yet unclear, as the concept envelops a range of applications and concepts such as information load; easy access to subsequent bits of information just with the touch of a finger, metadata, the digital traces people leave behind, and software engineering work to handle data in huge amounts (De Mauro et al., 2015). Susan Hauser, a former vice president of Microsoft's corporation stated in a 2012 interview (Wash, 2012) that the world holds twice the amount of data as it does water in its oceans, and analyzing

it can create accurate predictions and insights of trends and things before they even happen.

The policing tool Predpol [53] is a great example of using algorithms to analyze past crimes in order to predict new ones, hot areas for crime, and much more, therefore, efficiently guiding police and patrolling to predictive crime areas. The movie *Minority Report*[54] (2002) is an interesting piece of drama and mystery, where people are arrested by a 'precrime unit' before they, themselves, know they were going to commit a crime. Among the big data folkloric stories is that of the retail giant, Target, when the company figured out a teen was pregnant and sent her advertisement mails before her dad knew. The computer analyzed purchase data from Target database and concluded a through a pattern of pregnant females' unscented cosmetics purchases that the teen was pregnant (Hill, 2012).

Just as Predpol works on crime data to predict crime, the same algorithmic structure might start working on SNSs data and data from Google about individuals and generate patterns of suspicious events, gatherings that may go out of control, home child abuse, sexual abuse, and other happenings before they occur (News & Events, 2018). There are a plethora of examples about big data and its predictive power, which makes living with technology convenient, while also a threat to privacy. Lanier (2013) argued, "This state of affairs means that unless individuals can protect their own privacy, they lose power. Privacy has become an essential personal chore that most people are not trained to perform" (p. 66).

---

[53] https://www.predpol.com/
[54] Read about Minority Report here: https://en.wikipedia.org/wiki/Minority_Report_(film)

As it relates to literacy, it is important to inquire about big data in terms of its application and analysis; how much of a person's personal information is exposed; and how much of the individual is known unintentionally by unintended audiences. In other words, as Newell and Marabelli (2015) pointed out, users are often unaware of how much data are produced by their digital devices; what data are used; by whom; and with what consequences. Therefore, living in a sea of data that are big, how much can individual users do to protect themselves (i.e., privacy literacy). This makes privacy literacy on par with a survival set of skills.

Privacy May Be Dead, but Big Data Enhances Life

Any interaction with or among electronic devices—smartphones, fitness gadgets, tablets, laptops, smartwatches, smart homes—generates data about operating systems and individual users. These data are informative to businesses aiming to enhance their services and targeting skills. Michal Kosinski (2017) mentioned that when we stop battling for privacy and move into an era of no privacy, but collectively focus on organizing our future (law, society, culture), we then live in a healthier, safer, and fairer society. Regarding big data, many scholars think that privacy is dead (Hubaux & Juels, 2016; Mims, 2018; Rauhofer, 2008; Webb, 2019; Zibuschka, Kurowski, Roßnagel, Schunck, & Zimmermann, 2019). But is it really dead?

Even though privacy may be considered dead by some scholars, the analysis of data still enhances life and pushes innovation further. As an example of the benefits of big data, McKinsey Global Institute (2011) advised that by using the big data available in the healthcare sector, the U.S. Department of Health could save more than $300 billion yearly by reducing national health care expenditures. The current system with always-on devices needs data and strong software to operate. Data about us are necessary and so is sharing these data. Tucker (2015) advised that it is a mistake to

demand that technological progress reverses itself by trying to avoid or contest its power. A better solution might be to teach ourselves how these technologies work and understand how technology can be abused (Wissinger, 2017). Lanier (2013) and Tucker (2015) added that the future will lack privacy and will be dependent on our knowledge of the software and how it operates.

Successful examples big data use. Data fuels today's economy and businesses. In the field of healthcare research and development, technological wearables are making their way to revolutionize diagnosis and treatment. Wearables are devices endowed with sensors, which the patient wears to cull data on their medical profile. Glucose monitors are already approved by the Federal Drug Administration (FDA) for patients to wear and the app on their portable devices registers the glucose levels throughout the day (Schadt, 2015**)**. Ai Viz is another success of the use of big data in healthcare. The app is now available on Apple and Google play stores, and is Federal Drug Administration approved. The app works on preventing strokes by identifying large vessel occlusion indicators and prevent strokes. The app will then notify the doctor on-call, call an emergency ride, and transfer data to the patient's main doctor all within six minutes[55]. The app is linked to a scanner data with a trained algorithm that learns from the performed scans of others who have shown similar symptoms. With more data comes accuracy. The model keeps learning infinitely from the massive amounts of scans available, and whenever a

[55] For more information visit, https://www.viz.ai/

new patient is scanned, the algorithm will quickly determine if there are any indicators of a stroke.

The Apple watch hard fall[56] feature works similarly to Ai Viz. It is equipped with motion sensors that detect hard falls, dispatch GPS location, and call an emergency ride. It has saved many lives of bikers and mountain hikers, for instance. In the world of sports such as soccer, computers could be trained to indicate where defense players should position themselves when the opponent team is attacking, and suggest other positions depending on what the opponent team is doing (Le, Yue, Carr, & Lucey, 2017).

In another example, Ocado is an online grocery-delivery company. It has built the largest Customer Fulfillment Center today—it is located in southern England. The center uses 700 robots running on a grid as large as three football stadiums and are managed by an air traffic control system[57]. The above-mentioned success stories rely primarily on citizen information and data in addition to Artificial Intelligence (AI) or machine learning.

Big data, Big Exposure

Citizens consider their right to privacy violated when they can no longer control their social or physical interactions (Laufer, Proshanskey, & Wolfe, 1976). Payton, Claypoole (2014) stated that,

> When we know we are being watched and listened to. . . the resulting change in behavior is simply a loss of freedom. . . the freedom to allow the less

---

[56] See how it works here, https://support.apple.com/en-us/HT208944
[57] https://www.ocadotechnology.com/

> socially careful branches of our personalities to flower. Loss of privacy reduces the spectrum of choices we can make about the most important aspects of our lives. (p. 3)

Folks who oppose the extensive collection of data and behavioral profiling defend personal privacy and the right to be let alone. They argue that with big data comes big exposure (Chirita, 2018; Price & Cohen, 2019).

The developing technologies have taught us new norms about privacy and shareability. As Lanier (2013) argued, software is political and is made to make people behave a certain way. Software is a set of thoughts with an objective and ideology that are embedded in a written code (Lynch & Gerber, 2018). A recent U.S. White House report concluded that whoever has more data has power, and much of today's data is in the hand of few others (White House, 2014). Data creates and generates value; however, data profit relies on the citizen's interaction with a device and with others. Despite being the main actor, the citizen remains absent from the equation of data and privacy. As Kosinski (2017) argued, using a service for free makes the user a commodity.

In her book, *The Age of Surveillance Capitalism,* Zuboff (2019) spoke about what she calls 'behavioral surplus.' As it relates to algorithm and predictability, behavioral surplus are the little details we publish here and there across online spaces, such as on SNSs, through which algorithms can make accurate predictions about us and know things we initially thought were private. The behavioral surplus phenomenon is what Artificial Intelligence and facial recognition softwares exploit to accurately profile us. For instance, Wang and Kosinski (2018) developed a machine learning model that analyzed pictures with high accuracy. From one face shot, the model predicted people's sexual orientation with about 81% accuracy. The accuracy

increased to 91% as the model was provided by as little as five face shots. In Wang and Kosinski's research, the model was trained on 35,000 human face shots with sexual orientations, and from there on the model would predict new images and new intimate traits. One can imagine how much SNSs can know about the users by harvesting their behavioral surplus. In other words, information users put out there and think has no significance has great significance in the age of surveillance capitalism.

It's not about data, It is about the machine. In my conversation with Tom Liam Lynch, an educational researcher and software theorist, he stated that the companies that lead software engineering have a great amount of power to regulate and influence people's behavior (T. L., Lynch, personal communication, February 18, 2020). Lanier (2013) posited that "Because software is the way people connect and get things done, then what the software allows is what is allowed, and what the software cannot do cannot be done" (p. 70). Because software is human authored (Lynch & Gerber, 2018); fundamentally it has imposed privacy trade-offs for service or convenience (Payton & Claypoole , 2014; Lanier, 2013). Many forget that software controls what users can do and shapes, in a way, their behavior (Manovich, 2013).

The future is, more than ever before, in the hands of software engineers. According to Lanier (2013), the future is determined by who harvests big data in addition to operating with powerful computer systems that the regular citizen do not own. Waldman (2018) followed along and argued that web-design is similar to public

space design and architecture[58]. Web-design can be designed to restrict our behavior, influence our understanding of privacy, and even coerce us into acting against our true intentions. Waldman analyzed 191 privacy policies from different websites and concluded that they are designed to ignore the users' comprehension and protect the company's services.

Software runs our phones and allows the phones to follow a precisely scripted function and automated behavior. Our phones talk and communicate with other connected devices on our behalf. Apps in our phones continuously exchange data about us. Tom Liam Lynch illustrated this by saying, "So if you own an iPhone and you sign up with your Facebook account with company x. Now, company x has your data; Facebook has access to certain amount of it; Apple has it; and depending on who you are connecting to in terms of your network, they may or may not have your data as well." And when I asked him whether the general public knows all this, he responded, "When you talk about software space or layers, there's like five layers to it, and folks just aren't used to thinking about it that way… and it's by design, they're [the end user] kept from thinking about it as well" (T. L., Lynch, personal communication, February 18, 2020). The machine can be programmed to do whatever the computer programmer wants it to do. The giants of information system production have capitalized in this field of machine and software engineering through Software Development Kits (SDKs).

[58] Also see unpleasant design architecture at https://99percentinvisible.org/episode/unpleasant-design-hostile-urban-architecture/

SDKs' and Data Exchange: Another Level of Unconsented Big Exposure

If you are a coder or a software developer, it would be a daunting task to have to write every app's code from scratch. One may ponder, why doing so if there is so much in common among most apps: the coding language, the functionalities, or the artistic layout. Many apps use the hamburger drop down menu, for instance (e.g., Facebook, Instagram) other apps use other structures. However, it should be noted that most apps have similar setting structure and sections. Recoding the same features from scratch is inefficient. The answer to this issue is the library of SDKs (Software Development Kits) just like the library available in the Unity 3D game engine in videogame design. These libraries contain ready to go designs or shortcuts that developers use as their app basis/foundation and then add on their touch.

Facebook[59, 60], Amazon, and Google each have their own SDKs libraries that help developers build apps that are compatible with their service(s). Apps such as Tinder, Grindr[61], and others use Facebook SDKs to develop the software to interface their applications. In return to using SDKs for free, the apps report data directly to the tech giant often unbeknownst to the user. Such data include the device, IP address, time of usage, health data, religious affiliation, and the advertising ID unique to every user (Warzel, 2018). Data then becomes available as Facebook, for instance, can easily match advertiser's ID with the user, if he or she used the same device to log into Facebook before (Warzel, 2019).

---

[59] Facebook SDK for IOS https://developers.facebook.com/docs/ios
[60] Facebook SDK for Android https://developers.facebook.com/docs/android
[61] Tinder and Grindr are online dating apps.

Apps built with Facebook SDKs, such as KAYAK, an app that compares flight prices, will still send data to Facebook even if the user does not have a Facebook account (Privacy International, 2018). Such information includes departure city and airport, departure date, arrival city, arrival airport, arrival date, number of tickets (e.g., adults or children), and class of flight (e.g., first, business, or economy).

Apps communication with the owner of the SDKs happens automatically without alerting the user. A report by the German security initiative Mobilsicher (Ruhenstroth, 2018) claimed that about 30% of all apps[62] in Google's Playstore automatically send user data to Facebook once the app is opened. The report mentioned that dating apps such as Tinder, Curvy[63], or Grindr, apps that help with therapy of quitting smoking such as 'Kwit,' or apps which help with depression such as 'Moodpath' all send user data to Facebook. Apps that monitor the pregnancy cycle 'Pregnancy +' or reminder and calendar apps such as 'Bible+ Audio' or 'MuslimPro' all send data to Facebook once the user opens them. The reason being is that these apps and many more others used SDKs that are initially released for compatibility by Facebook. Ruhenstroth (2018) added that Facebook pairs these data with data the company already has about the user. Facebook can then tell its data customers who the users are, with substantial details, just from the apps they open and close daily.

AppCensus[64] is a security initiative that analyzes real time usage of apps and the type of data the app transmits to third parties. This transmission is hidden from the

---

[62] Statista, as of June 2019, Google store has more than 2.7 million apps. Details are found here https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[63] Curvy is an online dating app

[64] To try the website visit https://search.appcensus.io/

individual citizen (Binns, Lyngs, Van Kleek, Zhao, Libert, & Shadbolt, 2018; Privacy International, 2018; Ruhenstroth, 2018). AppCensus analyzed more than 80,000 apps for what they call 'privacy analysis,' which focused on what type of data the app transmitted to third party without the user's knowledge. Using the AppCensus, I investigated some of the apps I use on my phone and found out secret third-party data collectors such as Crashlytics, a software development company owned by Google.

Unuchek (2018), a researcher at Kaspersky Labs, shared results of the security lab report and reveled that "...4 million Android apps were sending unencrypted user profile data, such as names, ages, incomes, phone numbers, and email addresses—and, in one example, dates of birth, user names and GPS coordinates" (n.p) to advertisers such as Facebook and Google. In their study, Binns et al., (2018) analyzed 959,000 apps from the U.S. and U.K. Google Play store to identify third-party trackers. They found that 88.4% of apps send data to Alphabet, the mother company of Google, and in second to Facebook with 44.5%.

Privacy Control at the Surface and Deep Levels

Software structure controls the individual's choice more at the deep level, but also allow the user a surface level control known through privacy-setting buttons and links. Privacy settings are an important component of any phone app or website that collects personal data. For instance, Facebook privacy settings are programmed around content exposure—who can see my stuff—and location services. Google focuses mainly on location to optimize its services and customize its content. The overall question is, to be able to have full control over privacy, would surface level privacy setting control be enough?

A recent report by Associated Press (Nakashima, 2018) showed that Google tracks users' location even if they turn it off on their phones. Moreover, the report

demonstrated how Google stores a snapshot of the user's precise location once the user opens the Google Maps app. In other words, before the user starts using the app or changing any settings, a precise location snapshot is recorded permanently. Even if location services are turned off, daily weather apps and searches on Google search engine, for instance, about food or car wash services pinpoint the user's location and send it to Google.

Android is a Google product and Android phones were found to collect cell tower locations and send them to Google regardless of whether the user has turned on their location or not (Collins, 2017). Current Google privacy terms[65] state that Android phones send data to "...Google servers about device and connection to our services. This information includes things such as your device type, operator name, crash reports and which apps you have installed" (Google Privacy Policy, 2019). The list of data the phone sends to Google servers is neither clear nor is it exhaustive. The same policy mentions that Google collects data (e.g., browser, application, device) about users even if they use Google products without signing in with an account. This is privacy setting at a deep level, which the user does not control. Opt-out may be an option. Google, Facebook, or other SNSs and information websites do offer opt-out options, although partially, but doing so requires skill and privacy literacy. The opt-out options are often embedded in multiple-step menus and require reading of the policies and terms.

[65] https://policies.google.com/privacy#intro

Devices smart enough to know and recognize people. Device intelligence has developed tremendously. Tech Trends 2019 mentioned the development of drones for surveillance (Webb, 2019). The drones are endowed with facial recognition technology and can take full High Definition (HD) pictures from 1000 feet. They are used to monitor concerts, traffic, and more without the consent nor the recognition of people on the ground. Voice recognition is another technology that is developing at an unprecedented speed. Smart speakers, like Alexa, are owned by 1 in 10 Americans (Future Today Institute, 2019). Amazon is currently working on enhancing the powers of its smart speakers to recognize our voice and note if we are sick or moody, and pair the information with data the company has on us to enhance its marketing tools (Webb, 2019).

Persistent recognition is the future. The super retailer, Walmart, is working on developing facial recognition tools at checkout that would determine customers' satisfaction and any potential help they may need. Store associates would then receive alerts to help the customers based on the customers moods and satisfaction levels (Anderson, 2017). An article issued by the Walmart Corporate (Smith, 2019) showed how Walmart's Kepler project is changing retailers' management and customer experiences. The project uses AI to identify low stock, product spills, empty shopping carts and alert the store associates. Walmart, while managing its stock and efficiently managing the inner-store associates, also tracks shoppers' moves, time spent in the aisle, and any confusion or mood change while inside the store (Collins, 2017; Sisson, 2018).

Kroger, another grocery and food retailer, started testing cameras in shelves which recognize age, sex, and mood in order to display ads and store discounts accordingly (Pisani, 2019). While doing this permanent AI tracking and recognition,

Walmart and Kroger's philosophy stems from the age-old marketing golden standard that it is less expensive to retain existing customers than to recruit new ones.

In testing these intelligent retail stores, both privacy and law are at stake (Webb, 2019). As of 2019, the U.S. does not yet have a holistic law that governs the fast-growing arena of artificial intelligence and facial recognition. In the year of 2019, the U.S. Congress has held multiple hearings about artificial intelligence and facial recognition to regulate the exploding field[66,67].

Unmasked in Super Smart Cities

China dwarfs other countries in the race to develop and implement Artificial Intelligence in the daily life of its inhabitants. Many of AI and its use in society has been part of fiction books and movies for a long time. For example, *Black Mirror*, the British science fiction series that airs on Netflix, has an episode that features people rating each other based on 'good' societal behavior. The rating the citizens obtain affects their socio-economic status. The episode is called *Nosedive*[68] and it shows a world of always-on citizens that watch each other, rate each other, and are all connected to a perfectly designed grassroot surveillance (see also Tufekci, 2008) system. Software coding, i.e., software at a deep layer (Lynch, 2015), is what made the citizens in *Nosedive* act a certain way and show great caution when in public. Noteworthy, *Nosedive* is no longer science fiction. It is becoming a reality in China. Like the financial credit score in the U.S., where loan repayments indicate financial

[66] https://science.house.gov/hearings/artificial-intelligence-societal-and-ethical-implications
[67] https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=657
[68] https://en.wikipedia.org/wiki/Nosedive_(Black_Mirror)

risk(s) and are predicted by an algorithm and sent to the lender; China's social credit score predicts good behavior and citizenry based on social interactions and is also funneled through an AI algorithm.

What is china's social credit score?. China, in an unprecedented race towards the future, has already installed 200 million sophisticated surveillance cameras with enhanced facial recognition capabilities. Both the government and private companies collect big data on every citizen as well as visitors e.g., surveillance cameras data, purchases, SNSs' data, health records, financial records and more (Marr, 2019). The collection of data are funneled through an algorithm to indicate someone's credit worthiness based on social actions alone. The social credit score is be applied in full by 2020, according to the State Council 2014-2020 road map[69], although it already is in effect in smaller scales throughout China. Under this system, citizens' data are shared across State Departments in China and other Chinese governmental agencies to notify them of citizen compliance or non-compliance with law (Horesley, 2018). Incompatible citizens are then subject to economic and social sanctions. The violations and sanctions are publicly published on a state website called *Credit China*[70]. Marr (2019) commented that the system tracks all deeds, and the trustworthiness score could fluctuate depending on behavior. Marr added that those who score high will receive social perks such as discounted utility bills, no deposits to rent a bike, or skip the line to see a doctor at the hospital, those who score

[69] https://www.chinalawtranslate.com/socialcreditsystem/?lang=en.
[70] https://www.creditchina.gov.cn/xinyongfuwu/shixinheimingdan/

poorly could even be confined to staying in one small area and not receiving any discounts or perks.

Similarly, the U.S. has started using faceprints and facial recognition for its border control, but there is a danger that faceprints could grow out of control and people's faces will be scanned and tracked everywhere (Future Today Institute, 2019). As an example, for some U.S.-based airline companies, such as Delta, boarding the plane requires the boarding pass and a faceprint, as shown in the picture below taken from a recent international flight that I took. The picture below was taken from a research trip I took to Belgium where I was obliged to leave a face biometric to board the plane. Moreover, there was no consent request or information about the device or the data it collects.

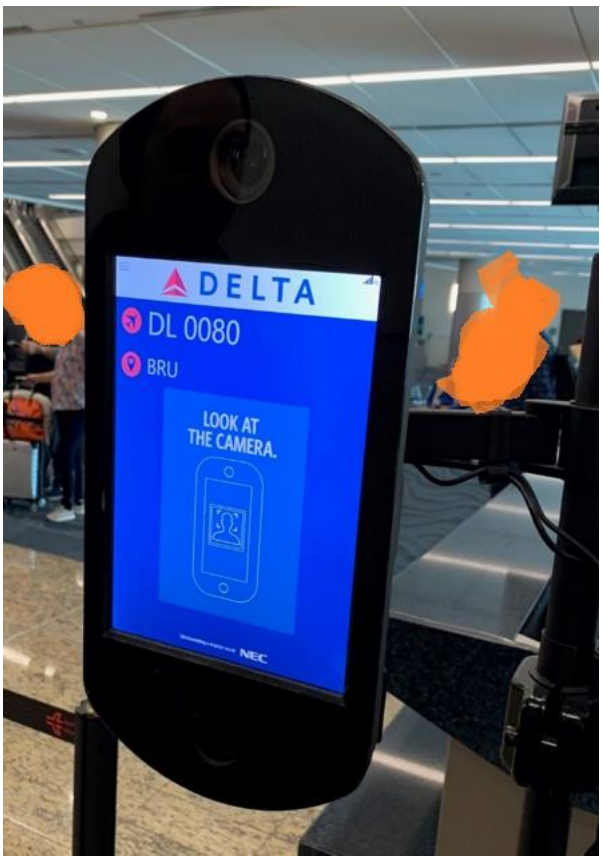


Figure 30. *Delta Airlines boarding facial biometric camera*

Consumer data in smart cities. Technology advancement is behind our data exposure. Considering AI development, facial recognition devices, and the use of nanotechnologies, how could we remain private and protect our personal data? The future of smart cities is energy efficient, healthy, and less polluted than regular cities. Sidewalk Labs[71], the Google urban technology spinoff has launched a project to build a smart neighborhood in Toronto, Canada. The smart city would open opportunities to third parties to build and establish an efficient digital infrastructure. Ubiquitous, fast, and secure connectivity is a priority, according to Sidewalk Labs. Moreover, the company published on its website that data will be open to third parties as a foundation to optimize the services offered and, therefore, enhance life quality (Side Walk Toronto, n.d)[72]. The Lab did not mention details about data privacy, but it alluded to security by establishing ". . . an independent entity called Urban Data Trust [which] will be charged with balancing the interests of personal privacy, public interest, and innovation" (n.p).

Sangdo, in South Korea, is another smart city that is half built. As an example of the city functionalities, it will employ radio-frequency identification technology to monitor citizens' trash disposing behaviors. The city will have pressure-sensitive floors in homes and select public areas to detect hard falls and automatically alert emergency (O'Connell, 2005). Regarding data and privacy and, according to Tech Trends (Future Today Institute, 2019), currently there are 50 world smart cities

[71] https://www.sidewalklabs.com/
[72] Read about the project of Toronto Smart city here: https://www.sidewalktoronto.ca/outcomes/#innovation

projects around the world, and they will have common amenities, such as abundant 4G, and soon 5G, connectivity, public Wi-Fi hotspots, and digitized government data that will be open to everyone. Data will be floating everywhere, and the future holds questions about data and privacy, such as who will own the data? Who will own the right to access self-generated data? Especially knowing that with big data, it becomes hard to keep data anonymous anymore.

Yes! Anonymous data can be reidentified. De Montjoye, Radaelli, Singh, and Pentland (2015) from MIT media lab studied purchasing activities of 1.1 million people for a period of three months. The researchers found that the availability of four metadata points can expose the person with 90% accuracy. They added that just knowing the price of purchase can expose the customer with 22% chance of accuracy. Acxiom, the giant data broker, teamed with Facebook to merge their data and create a giant marketing database. As of February 2013, Acxiom declared that its data matched 90% of Facebook SNSs profiles (Tucker, 2013).

Questions about privacy are usually answered with ‘data are anonymous.’ Research showed that this is a relic of the past. Another study by Kondor, Hashemian, Montjoye, and Ratti (2018) from MIT showed how a matching algorithm is able to handle big data sets of 1,319,524 daily commuters through train or bus. The program was able to uncover the identity of individuals who make 3 to 4 trips daily at an accuracy of 16.8% after just a week. The accuracy then jumped to 55% after a month and to 95% after 11 weeks. Campbell-Dollaghan (2018) noted that as “...urban planners, tech companies, and governments collect and share data, we now know that ‘it’s anonymized’ is never a guarantee of privacy” (n.d).

Regarding privacy literacy, some teaching initiatives cautioned learners that data anonymity is not possible with the sophisticated data mining softwares and machine learning models that can learn and trace individuals' habits. A privacy literacy project at TeachingPrivacy.org is an example of a cross-disciplinary group of researchers from the International Computer Science Institute and the University of California-Berkeley[73] who engage the public in dialogue about how privacy works. On their website they wrote "...data mining and inference techniques can be used to match anonymized users to their real identities with a high degree of accuracy, including through language models, speaker identification, facial recognition, location correlation, activity modeling, and other retrieval techniques" (n.p).

Data brokers such as BeenVerified can spill records of people using single identifiers such as name, address, phone number, etc. The records come in pages and clear sections such as family members, addresses, mortgage, owned properties, felonies and more. Using tech devices, we, as citizens, presume our data are anonymous; whereas in reality, data we leave behind can lead to other discoveries about us. Been Verified is an example of a system that operates on 'surplus behavior' (Zuboff, 2019), i.e., things we assume are insignificant or think we have control over them.

Summary of Theme 5

Theme Five was a mixture of current data practices and a projection to the future. Big data are good and big data are bad. It depends on how one uses them and

[73] https://www.icsi.berkeley.edu/icsi/

for what purposes. So much is yet to be unraveled about the black box or what happens behind the interface and the screen. Big data have opened venues for human life betterment, while also opened a gate to massive surveillance and scrutiny. The regular citizen is more and more in need of maintaining knowledge about the technology ecosystem that they use on a daily basis. Whether we agree or not, the individual human remains the main player in the equation of technology, big data, and surveillance. In this theme, I also tried to unpack some aspects of software and the future of privacy. It remains inconclusive and unknown to whether the citizen will be able to have their privacy and personal data under control.

Chapter Summary

In this chapter, I presented the themes I found in my literature analysis as well as the MODES. Additionally, I have sought expert opinions from a variety of perspectives, such as law, policy, and educational technology. The five main themes were (a) Self-disclosure Dynamics; (b) Privacy and Surveillance; (c) Privacy Management; (d) Privacy and Law; and (d) The Future of Privacy. In the next chapter I will present the public opinion, discuss Facebook data in light of the literature, and conclude with a map of the CLR and the privacy literacy skill i.e., privacy literacy 2.0.

Chapter V

Public Opinion Findings: Social Networking Data

Chapter Overview

In Chapter IV, I presented the main findings of my quest about privacy literacy. I presented the themes I found, as well as their respective sub-themes. The findings in Chapter IV were synthesized from a mix of (a) the scholarly work and (b) expert opinion with (c) media and secondary data. In Chapter V, I investigate (c) public opinion on privacy as noted on social networking sites, in particular, the public discourse on Facebook during the Zuckerberg Senate hearing in April 10, 2018. This chapter describes the data I pulled using Facepager API. Additionally, in this chapter, I discuss the ontological imperative (Lynch & Gerber, 2018) of the digital tools I used to collect and analyze data. The findings are presented with emphasis on public opinion about the privacy of personal information.

What Does the Public Think?

It is important to bear in mind that the current analysis of public opinion was collected from a sample of publicly available Facebook comments of Facebook users during the Senate hearing of Mark Zuckerberg, CEO of Facebook[74], on the Cambridge Analytica scandal. I collected a sample of 10,000 comments using Facepager, a tool developed by Till Keyling[75] from the University of Munich, Germany.

---

[74] The hearing took place on April 10th, 2018. For a summary of the hearing, visit https://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senate-hearing-highlights-cambridge-analytica

[75] Read about Facepager here https://www.alumniportal-deutschland.org/en/science-research/news-from-science/facepager-till-keyling-social-media/

Before engaging in analysis, I selected my analytical framework for the aforementioned SNSs data. Lynch and Gerber's (2018) ontological imperative framework addresses five key philosophical principles for scholars to think through when they engage in using digital tools for digital data collection and digital data analysis. As they argued in their seminal work on this method, "A critical understanding of the ontology of the digital (*what digital is*) has direct methodological implications that can help the field avoid epistemological pitfalls associated with conducting research in the digital age" (p. 112). Simplistically, this means that if data are digital (i.e., from Facebook data) and are collected with digital instruments (i.e., Facepager), and analyzed using digital tools (i.e., Voyant Tools), then researchers must engage in a critical analysis of these tools, systems, and services in order to ensure transparency, replicability, and ethical oversight.

When researching digital spaces, researchers must exercise extreme caution in making assumptions in their analysis due to potentially biased or incomplete data. Data may be incomplete because the nature of the digital is inherently unstable, and so are the products and coded software systems (Lynch & Gerber, 2018). Hence, the data that the researcher thinks is complete or bias-free, may actually not be, because data are algorithmically generated or black boxed by tech companies; therefore, if a researcher is not careful with the digital data collection and analysis process, this could possibly lead to highly biased and faulty findings (i.e., epistemological pitfalls).

As Lynch and Gerber (2018) posited, "Researchers, as well as the public, must continuously rupture common associations between the digital and qualities like objectivity, ephemerality, and neutrality. Rupturing such assumptions requires exploring the ways theorists have grappled with notions of digital and computationality…and its linguistic and ideological constructs" (p. 113). This means

that researchers must unpack all facets of their digital data and tools to ensure that there are no unfounded biases associated with 'the lure of objectivity', 'the power of visual evidence', and the 'black-boxing' that SNSs data and its analysis often gloss over (Gerber & Lynch, 2017; Gerber, Lynch, & Onwuegbuzie, forthcoming; Lynch & Gerber, 2018). Thus, the ontological imperative analytical framework helps researchers to engage in this critical analysis and allows readers a transparent view of the process and findings.

Employing the ontological imperative (Lynch & Gerber, 2018), I addressed the five main guiding principles of the framework in order to provide readers with layers of transparency regarding the data collected and the tools, systems, and services used to both collect and analyze the data. In this case, the parties at play in this study's dataset were Facebook, Facepager, and Voyant Tools. The five principles that guide the ontological imperative analysis of these tools, systems, and services are:

> (1) What digital tools, systems, and services are at play in my study? Who created them and why?
>
> (2) What data do these digital tools, systems, and services render?
>
> (3) What hidden limitations might there be to the data rendered via these digital tools, systems, and services?
>
> (4) What are the epistemological implications of this ontological analysis?
>
> (5) What are the axiological implications of this ontological analysis? (Lynch & Gerber, 218, p. 119)

Facepager: Ontological Imperative Analysis

Principle one. What digital tools, systems, and services are at play in my study? Who created them and why? Facepager was the tool I used to scrape Facebook back-end data. Facepager enables you to harvest publicly available data

from SNSs such as Facebook and Twitter. The tool will only collect what is made available to third-party developers by Facebook and Twitter through their Application Programing Interface (API). Facepager is a free open source tool, meaning that it could be used at no monetary cost. Facepager was developed by Till Keyling from the University of Munich, Germany. The tool was initially developed to enable research scientists to access digital data and study new media ecologies such as SNSs. Facepager requires no coding skills and its application steps are easily traceable, which increases research transparency.

Principle two. What data do these digital tools, systems, and services render? Facepager restricts the data points that the user can request in order to access data made available to third party developers by Facebook. Accessing Facebook data depends on the API key that the company used to develop the application (most SNS have dozens of API keys, each one makes very different data available). Restrictions are usually imposed by SNSs companies on third-party developers and interested individuals. This means that the data returned are generally nowhere near the exhaustive types of data collected by the SNSs on its users. For example, with the Facepager API, I did a data pull on February 4th, 2019 at 10:42 p.m., from the public Facebook webpage of CNN[76] International. The data I was able to return was as follows: level; "id"; "parent_id"; "object_id"; "object_type"; "query_status"; "query_time"; "query_type"; "name"; "message." The data were available in multiple formats such as.tsv or .csv, which was opened using Excel.

[76] A media company based in U.S. and is specialized in news broadcasting and other television programs.

Principle three. What hidden limitations might there be to the data rendered via these digital tools, systems, and services? Examining the Facebook Developer documents allows one to see the hundreds of metadata points that could have been collected if the developer of Facepager had used a different API key. For example, the Facebook Developer documents note data points such as geolocation, likes, and connections which could have been useful in my analysis, but which were not returned with the Facepager data pull. Additionally, as Lynch and Gerber (2018) pointed out, SNSs (i.e., Facebook) could also change or restrict access to the API at any point in time, and therefore, completely changing the metadata points that I might receive for a secondary confirmation pull. In other words, if I try to make an exact pull of this data in the future, I may or may not obtain the same data points.

Other similar apps, as documented[77] by Facebook, are able to return up to 60 points of data, however, this does not mean that they make all 60 data points available at one time, and as I have experienced, that is almost never the case. When I used Facepager, I was able to retrieve nine points of data only. I was hoping to retrieve location coordinates so I could have more variables for research and discussion. However, even the nine items mentioned prior are not always returned by Facepager. This is due to the regulations imposed by SNSs. Moreover, data returned in this case, (i.e., Facebook comments) came back padded in one single-space text or Excel file. The researcher needs to do so much cleaning before data could take shape.

[77] https://developers.facebook.com/docs/graph-api/reference/user

Principle four. What are the epistemological implications of this ontological analysis? Data collected from SNSs are usually determined by the tool we use. Harvesting SNSs data might yield a promising return of data, or it might return a restricted sample of data. The user of Facepager is rate limited[78] by the Facebook API. Moreover, as Gerber and Lynch, (2018) pointed, data are temporal and exist in the moment that they were produced. Therefore, replication of the process is often tedious, if not an impossible task. In this research, the comments I used would have been difficult to spot amongst other comments had I gone to manually surface Facebook to retrieve a sample of comments. Hence, the selection of comments Facepager collected is what researcher am bound to as the primary sample. This means that I must consider the data I collected as not only incomplete, but also temporally restricted to April 2018. This could change if I did the data pull today in February 2020 for the same conversation that occurred in April 2018. In other words, replication of this exact sample may not feasible.

Principle five. What are the axiological implications of this ontological analysis? The axiological implications (i.e., ethical considerations) are the fact that data are text (i.e., Facebook comments) and are bound to a permanent Facebook ID. I had to make sure the texts cannot be traceable back to the participants. Although data were open to the public, ethically speaking, the purpose for which I collected this

[78] API owners, in this case Facebook, can enforce limitations on how much data could be collected by other APIs as well as the quantity of data clients can request. This is also called Application Rate Limiting.

information was to gain insights and not harm anyone. Data concealment may be necessary in this case, since written data are easily searchable and traceable.

Concealment of Publicly Available Data

When harvesting publicly available SNSs data, there are a set of ethical considerations the researcher needs to follow, such as not causing harm or stress to the participants (Kraut, Olson, Banaji, Bruckman, Cohen, & Cooper, 2010), and concealing the data, especially data that are public. Gerber, Abrams, Curwood, and Magnifico (2017) posited that anonymity is of utmost importance to researchers collecting data from online spaces. Gerber et al., (2017) added that researchers need to practice anonymity when analyzing and reporting online data, because "… a simple search on any public search engine might highlight identifying information about research participants" (p. 149). Since text is searchable and retrievable as SNSs data are permanent (boyd & Ellison; 2007; Collins, 2017; Lanier, 2013), I chose to practice a maximum concealment level (Bruckman, 2002). A maximum concealment level involves changing all identifying information; use of fictive language for pseudonyms; and the rephrasing of participants' quotes. Therefore, the comments I collected from Facebook will undergo a maximum concealment level.

After engaging in the ontological imperative and ensuring maximum concealment levels to understand the nature of the data that I was dealing with, I processed the comments as explained in Table 20.

Table 20. *Levels of public data concealment and treatment*

Data Returned from Facepager	**Concealment Level**	**Data Treatment**
Facebook numerical ID E.g., 123456789123456789	Maximum	Delete Facebook IDs

Facebook post ID, e.g., 123456789123456	Maximum	Delete Facebook Post ID
"Data on Facebook, if not protected, it will be harvested."	Maximum	Rephrased: Anything you post on Facebook is collected unless you manage to protect it.

Facebook: Ontological Imperative Analysis

Principle one. What digital tools, systems, and services are at play in the study? Who created them and why? The platform was launched in February of 2004 as The Facebook (Boyd, 2019). It was launched by Mark Zuckerberg to enable people to connect with a visible network of friends. Visible means that you not only have a messaging channel, but you also get to see the pictures, videos, and updates of people you connect with on Facebook. The concept started as a rating service, known as Facemash, and soon turned to be one of the worlds' top information processing companies. Facebook revenues stream from data processing and marketing.

Principle two. What data do these digital tools, systems, and services render? Facebook is a platform that is rich in data and insights about people, their interests, opinions, feelings, and life in communities. The platform restricts data access to researchers and other third-party developers and only allows for the harvesting of small samples of people's data. The data I obtained from Facebook were insightful, but also restricted. For instance, I wished to obtain the location of the commenters in order to produce a geographical map of privacy thinking. As mentioned in the aforementioned ontological analysis of Facepager, this could have been possible, as Facebook does occasionally make these geolocation data available;

however, one needs extensive knowledge of programming languages in order to program an API call with the API Key to retrieve the data points that they wish to use (see also Gerber & Lynch, 2017; Lynch & Gerber, 2018). Given I used a pre-built tool, I was restricted only to what that developer had deemed important to collect.

Principle three. What hidden limitations might there be to the data rendered via these digital tools, systems, and services? Examining Facebook Developer documents, the company can grant access to hundreds of metadata points depending on the API key and access token used by the researcher. I tried other APIs (e.g., Facebook Graph and QDA Miner Lite), but several steps are put in place by Facebook to restrict access to data. Even publicly available data is returned as a sample that is incomplete; therefore, it is hard for researchers to paint a complete picture of SNSs behavior. Importantly, researchers need to bear in mind that using APIs to access Facebook data may yield samples of data that the researcher did not design or control. In other words, sampling is restricted by Facebook on data requested through the API.

Principle four. What are the epistemological implications of this ontological analysis? Data collected from SNSs are usually determined by end-point API, and in this case, it depends on the Facebook API and what it allows us to do. Usually, returned data from SNSs are samples. The key limitation is that the researcher does not control the sampling process; hence, the researcher may not have a full idea about what is left unsampled. Regardless, data are temporal and are bound to context and time. A big missing piece is that the researcher does not have direct contact with the users, and social norms suggest that directly contacting users from disaggregated data is unethical.

The analogy is that you would not go lurking, hidden behind a one-way glass wall at an AIDS support group or an Alcoholics Anonymous support group, and then locate the names, home addresses, phone numbers, and emails from these individuals and contact them to be in your research study. That is a violation of social norms and trust on many levels. Therefore, data from SNSs are simply aggregated insights about groups of users. Levels of micro and macro insight, through interviewing, focus groups, and surveys should only be sampled from aggregated insights to population, location, and other demographics, not specific users, because they were part of an initial data pull (Gerber, 2016; Gerber & Lynch, in press). Generally speaking, there is a missing layer of member-confirmation and clarification, if needed by the researcher, which can be refined through a multi and mixed method approach (Gerber, 2016). Because data returned by the Facebook API is spatially and temporally sampled, the possibility that another researcher could replicate the process and obtain the same sample is unlikely to happen.

Principle five. What are the axiological implications of this ontological analysis? The axiological implications (ethical considerations) are the fact that Facebook returns public data with several identifiable pieces of metadata such as post ID and user ID. These IDs could be retrieved using Find my Facebook.[79] For this reason, data cleaning prior to analysis is of utmost importance.

[79] https://findmyfbid.com/

Voyant Tools: Ontological Imperative Analysis

Once I treated the data for anonymity, I then transferred the comments to Voyant Tools, an open-source web-based application for text mining, statistics, text analysis, and data mining. I adhered to five principles of the Ontological Imperative, as developed by Lynch and Gerber (2018).

Principle one. What digital tools, systems, and services are at play in my study? Who created them and why? Voyant Tools was developed in 2003 by Sinclair and Rockwell (Sinclair & Rockwell, 2012). According to Klein, Eisenstein, and Sun (2015), the tool "… was conceived to enhance reading through lightweight text analytics such as word frequency lists, frequency distribution plots, and KWIC displays" (p. 138). The tool was designed to assist researchers in mining corpus texts with no prior computer coding knowledge/experience.

Principle two. What data do these digital tools, systems, and services render? Voyant Tools does not harvest any data; however, it analyzes data and provides insights from the text. When the text is plugged in, the tool automatically conducts a frequency analysis, correlation, collocations, and trends. The researcher is then free to select any type of analysis and further mine the text.

Principle three. What hidden limitations might there be to the data rendered via these digital tools, systems, and services? Using Voyant Tools, I was not able to modify the word clouds, a type of analysis that the tool does automatically. Also, the tool only reports high frequency words. In order to obtain low frequency words, which may be insightful, the researcher needs manual mining. Lastly, the tool does not keep the text format as inputted initially. Consequently, the researcher needs to develop a system of tracking of the text portions.

Principle four. What are the epistemological implications of this ontological analysis? Using Voyant Tools allows for discovery and mining of the text. The tool shortcuts several steps for the researcher; however, it guides analysis and the researcher's options. The researcher is limited by the choices the tool offers. In my case, it was convenient to use Voyant Tools, as I only worked on text and needed an anecdotal analysis versus a systematic analysis.

Principle five. What are the axiological implications of this ontological analysis? The axiological implications are the fact that data are a text (i.e., Facebook comments) which are bound to a permanent Facebook ID. I had to make sure the texts were clean, before uploading to the tool for analysis. When the data was returned, I changed the order of comments in the text and rephrased all direct quotes findings.

Voyant Tools Analysis

The following is the analysis of the comments, frequencies, trends, and word clouds that emerged from my study of public discourse on Facebook. The comments were retrieved from the 2018 Zuckerberg-Senate hearing. Additionally, I will support the analysis with select Facebook comments about the topic of privacy.

Word Frequencies I anecdotally analyzed a corpus of 8,926 Facebook comments i.e., a total of 98,104 words. As relevant to this research, Voyant Tools enabled an analysis of the most mentioned words and their frequencies, collocates, a word cloud visualization, and allowed a trends comparison.

Figure 31. *A snapshot of Voyant Tools interface*.

Table 21 shows the most recurrent words and their frequency counts. The Voyant Tool classifies words in a ranking order from most frequent to least frequent. The top 20 words are the center of discussion, as they give a clear idea about the corpus.

Table 21. *Word frequencies from Facebook Comments*.

Words	**Frequencies**
Facebook	1605
Mark	852
fb	649
People	501
Like	486
Just	426
Zuckerberg	391
Know	371

Data	329
Senators	324
Want	318
Use	288
Government	286
Senator	279
Lol	267
Don’t	261
Social	226
Questions	222
Information	212
Info	206

It is important to remind the reader that the Facebook discussion happened around the Facebook data breach scandal, known as Cambridge Analytica. Analyzing the word frequencies, provides an overview of public understandings and feelings about the data breach. In keeping with the focus of this research about privacy literacy, I chose to concentrate on the following words: Facebook as an example of the SNSs; Data as the fuel of the problem; Government or Senators as the legislation body; and privacy, although not a top frequency word, remains worth mentioning.

Facebook. The most frequently mentioned word was Facebook, which is the company at stake. The three words of ‘people, just, and like’ came in the top word frequencies to show an ongoing conversation among people that used quite a few of illustration words (see Table 13). For example, this comment stirred much conversation and argument based on people’s likes and threaded discussions, “No one

forces you to use Facebook, right? You are free to join. If you do not agree to it, then do not join." Or this comment from another individual, "You all are commenting aggressively about Mr. Zuckerberg. Did you forget that you are complaining about him and yet continue to use Facebook?"

Most comments that contained the word 'Facebook' were superficial; elicited conversation and argument; and highlighted a diversity of opinions between maintaining a Facebook account, deleting it, or supporting Mark Zuckerberg and showing love for his company.

A commenter who wanted Facebook to close down sarcastically commented on SNSs' social relations saying, "Imagine Facebook runs out of business, you all will start having organic face to face interactions." Another individual praised Facebook for helping them to enrich their business and argued, "Facebook has helped me advertise for my business at a low cost. I do not want to use highly expensive newspapers or TVs again". In the same line of argument, another citizen praised the power of connectivity Facebook offers and said, "Facebook has helped me find family members in the past. I love it."

A Facebook user summarized one of the main problems that is relevant to this research and highlighted the problem of consent. The user said, "So I consented to use Facebook and own an account. Now, if things go wrong, data gets stolen, it is Mark the escape goat. People!! You consented to have Facebook." This comment sparked discussions surrounding the consent users give tech companies. A participant replied and stated the Equifax breach and said, "We gave it all to Equifax while we are here watching Mark getting smoked. What did Equifax take? Did anybody receive a notification? This was about money, right? You guys consented to the company to take time and not inform you about any breach. Delete Facebook and sue Equifax."

The public enriched the conversation as one mentioned how Facebook should have the same regulations as HIPPA, and thus, protect the people's SNSs records. Overall, discussion around Facebook was split among total supporters of Facebook, opponents of Facebook, and those who accepted the company and suggested regulations.

Data. Personal information protection, predictive algorithms, and data selling for advertisement and surveillance purposes were my key thoughts as I approached the Facebook data corpus. My objective was to obtain the pulse of the public perceptions about data processing. As a foundational piece of information, a commenter said, "Every app on your phones tracks you somehow. Google tracks you at all times for marketing." However, some people showed a lack of understanding that data are not confined to only what they post. Data are collected in an aggregate fashion, and every post, has another layer of data related to it, such as time of post, id of post, location of post, etc. Additionally, processing-algorithms can reveal things we have always thought were private. For example, someone said, "Data? Huh? If you want to know my favorite food, just see my posts. No brainer. We all know what it is." Another one added, "I would like to ask these companies which collect my data if they need more selfies of my dog?" In the same vein of argument, a Facebooker said, "Oh no!! Cambridge Analytica leaked photos of my trips and meals I eat at work!!" These quotes indicate how some Facebook users think of data collection and processing as trivial and not something that should be taken seriously. Also, many showed a lack of understanding of the metadata and how insightful that data could be for third parties.

Some had the feeling that data leaks from everywhere, and expressed their intention of "give up." A Facebook user said, "Data collection will not stop. It is open to everyone." Another user commented, "Delete your social media accounts. Data will

not be deleted." As I mentioned in the body of literature, using free services has a counterpart. When you use a service at no cost, you may need to give away something, and in this case, it is our personal data. A Facebook user explained, "You guys do not pay to use Facebook, do you? You are the commodity then! Get over it." Consequently, a Facebook user suggested a model for data exploitation and said, "I want them to use my data, but I also want them to share profit with me." Another one added, "Facebook should give us permission to access the records and control them. This needs to be in a new platform that takes our privacy seriously." The 'pay-me-model' seems to be a suggestion for big data transactions in the future.

Regarding data surveillance, the public knows that the government wants Facebook data, but many citizens might not know that the government actually already uses and exploits data from all electronic companies. A user said, "Governments may want to use Facebook data for surveillance. Of course, it is fresh and frequently updated." Another person commented on the fact that the government spies on citizens more than Facebook and said, "Senators are doing this to this genius…FBI and CIA already have it all. Wake up!!"

I chose the following comment to close this brief discussion on data collection, and then open the next discussion on privacy. This Facebook user expressed their feelings about self-protection and argued,

> I think none has ever thought our personal information will be compromised. No one forced us. It is our entire mistake. We were the ones who opened social media accounts here and there. We need to stop blaming others for our mistakes or because we did not practice caution to protect our data. Only us can protect our data.

The lingering question is, can we truly protect our data by ourselves?

Senators and the government. Most comments about the senators centered around their inability to understand how Facebook works or how data processing functions. The public shared plenty of sarcasm and funny comments pertaining to the fact that the U.S. Senators could not figure out the problem. A comedic comment read as follows, “Watching this trial and how Mark Zuckerberg explains Facebook to these senators is like my grandpa learning how to use his iPad, lol.” Another citizen added, “Senators! Get some education. Maybe I need to step-in and teach you all the basics of using the Internet, then we can talk about Facebook.” The conversation went on mostly mocking at the Senators’ lack of knowledge on how the system operates. Someone commented on this and said, “Senators seem to be blind to the fact that technology has advanced so much in the last decade.” And finally, a Facebook user asked the question, “Senator what happens when you forget and do not remember the password to your Facebook?”

Regarding surveillance, the public revealed some of their sentiments around trust in government. Most of their feelings expressed mistrust and denounced the government watch. However, there was no comment that explained how the government exploits data or surveils U.S. citizens through SNSs. Some expressed how the government watches everything and mentioned that they trust Facebook more than the government. A commenter said, “Facebook is safe. Thanks to you Zuck. You guys all know your phones have cameras and microphones. We use those to connect and talk to our dears. The government listens and watches all of it.” Another one added, “I love Facebook and I will not delete my account. I trust you Mark. I do not trust these senators.” One user contested lack of legislation and prosecution of data breaches and linked that to government trust saying, “Companies will not inform you of any breaches… especially the banks… no penalties… I do not trust the government.” On

surveillance, someone mentioned spying using Facebook data and wrote, "...the government holds these hearings to justify their spying activities on us and on social media." These comments illustrate how the public distinguishes Facebook from the government, and only places surveillance activities on the government.

Privacy. The word privacy ranked as the 23rd most mentioned word with 203 appearances in the corpus. Although the focus of the hearing was a breach of privacy and data, the trends of discussion showed that the public did not unpack the mysteries of privacy. Figure 30 shows the trending of the words 'Facebook, data, and privacy' across the 8,926 comments.

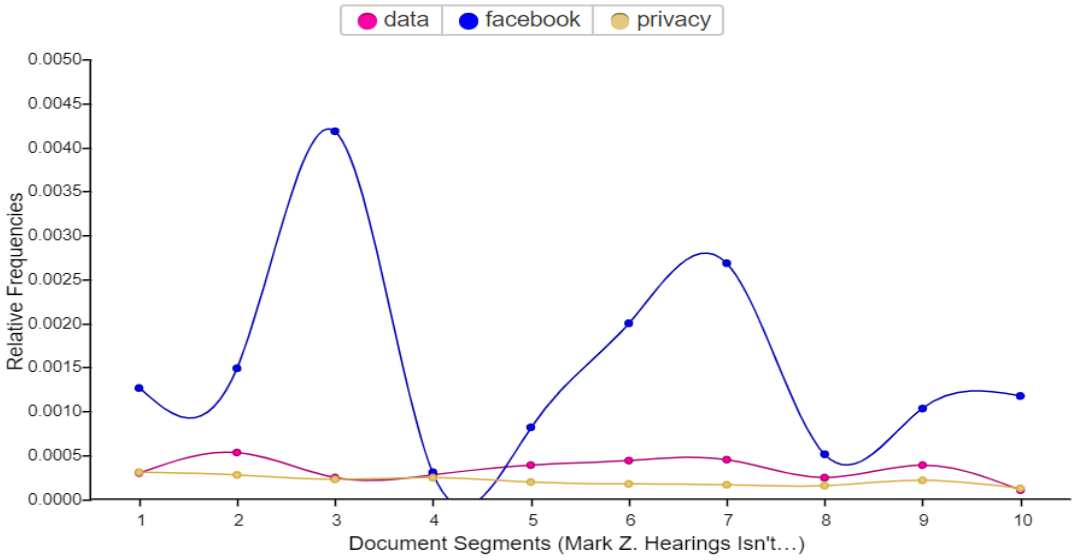


Figure 32. *Trends of discussions related to Facebook, privacy, and data*.

The graph shows the gap between discussions around Facebook and other discussions regarding data and privacy. The words privacy and data were mentioned with similar word frequencies of 203 and 329 respectively. However, the word Facebook was mentioned 1,605 times. All comments, with no exception, centered around trying to resolve privacy while focusing on the Facebook interface and the platform affordances. In other words, no Facebook user mentioned the words

metadata, data in aggregate, or companies like Acxiom, which pairs its data with Facebook. A citizen said, “Privacy? Whatever you post on Facebook is seen by your network of people and whoever they are related to. Idiots put stuff out there and assume it is private.”

The findings from this CLR, as noted in Chapter IV, emphasized the fact that SNSs users have concerns for peer and social sharing and surveillance versus the government watch. Another user alluded to the fact that Facebook privacy settings are ineffective. This user said, “So you think you can go through your Facebook setting, activate privacy, and magic happens?”

Another Facebook user commented on the company’s business model and declared, “Whoever created Facebook was not worried about privacy. You think you could use this platform for free? Where does money come from? Your data!!” Some believed that privacy is gone, as this user said, “If Facebook ever shuts down, there is Tinder, Instagram, Twitter… People wake up! There is no privacy on the Internet.” Data and privacy discussions have also drawn the public’s attention to data permanency. A citizen commented on this and posited, “Take a picture, post it, it is there forever even if you delete it.” The same citizen went on and placed the privacy responsibility on individuals saying, “. . . you were the one who took the picture and posted it, right? It is you not Facebook’s fault.”

Although some showed trust in Facebook’s privacy settings, others blamed the public for not reading the privacy policies, implying that privacy could be secured by reading the policy. They said, “Only few read privacy policies. You guys have no idea what you sign up for. If you agree, it is your full responsibility.” A member of this discussion mentioned the U.S. PATRIOT Act of 2001, and made a comparison between the government and Facebook. This individual argued, “Anyone can relate to

the patriot act? The government has all of our information. You want to know the difference between Facebook and the government? The government has been collecting your personal information since birth."

The public solution was twofold: to either stop using any SNSs, or then to use the sites wisely and be attentive to the privacy settings and the terms of service. To illustrate opinions on the privacy settings, a commenter said, "I love Facebook. Be proactive and do your due diligence. Read about the settings and use them wisely." Another Facebook user suggested that privacy can never be reached on the Internet or while surfing the SNSs, and argued, "Do you want privacy? Drop all technology." Another Facebook user emphasized that "Everyone on here keeps complaining about data and Facebook… you are still using Facebook. Delete your account if you are that concerned."

Chapter Summary

In this chapter, I discussed publicly available data I collected using back-end channels from Facebook. The analysis showed that the public lacks understanding of the metadata black-box (Berry, 2011; Baruh & Popescu, 2017; Everson, 2017; Lynch & Gerber, 2018; Manovich, 2013; De Montjoye, Radaelli, Singh, & Pentland, 2015). Additionally, many individuals showed their intentions to trust SNSs more than the government, as the latter collects information and surveils the public without an alert. Finally, harvesting online data has ethical and research practicality issues that I examined using the ontological imperative (Lynch & Gerber, 2018), as well as the data concealment levels of Burckman (2002).

CHAPTER VI

Step 8: Discussion and Implication

Chapter Overview

This chapter aims to highlight the major trends and orientations about privacy literacy 2.0. As I mentioned in the introduction, among the main goals of this study is to map the skill of privacy literacy. I call it privacy 2.0, and in this chapter, I present the skill and knowledge in three maps. The chapter also presents the concept of liquified surveillance, which responds to the work of Brandeis and Warren (1890) that 'the right to be let alone' is a relic of the past. During Brandeis and Warren's time, access to the person was confined to the physical surroundings and a few online archives that were unavailable except to select governmental agencies. Today, surveillance is everywhere, and no one knows from where a piece of information will leak. The discussion ends with critical questions needed to emphasize the circularity of the CLR, where findings lead to gaps, and therefore, to more questions.

Discussion of the CLR

Turow, Hennessy, and Draper (2018) reminded us that, "Thirteen years of research show consistently, though, that the label [privacy policy] is deceptive. A strong majority of Americans thinks it means that firms will not use their information without their permission" (p. 476). This quote highlights the prevalence of commercial data collection and places the citizen in a vulnerable so-called 'no-choice' situation. Like one of my students once told me, "While I am certain that these companies want to keep their consumers safe, it is not something that they can ensure" (Student, personal communication, July 2018). Anecdotally, this reminds me of another student who participated in the privacy unit I co-taught, mentioned in their

reflection assignment how shocked they were after realizing the spread of their information and how they could not control anything. This individual said,

> I was giving Instagram permission to use my content as they please. This made me think of my own account which includes pictures and videos of my friends, family members, and my pets. Instagram has the right to use my pictures and videos and share it with anyone they want. It is a scary thought that I gave them permission to do this by using their services. (Student, personal communication, July 2018)

Another student made a realization about data collection depth and said, “It was surprising how much data is (sic) collected about everything you do in, out, and offline with the app. I wouldn’t have imagined they used that much data about what I did” (Student, personal communication, July 2018).

This realization is hidden from many others and is hidden within long, and sophisticated privacy policies (Fuchs, 2014a; Monteleone, 2015; Obar & Oeldorf-Hirsch, 2016; Turow, Hennessy, & Draper, 2018). When asked for an opinion, Ian O’Byrne, an educational technology researcher and privacy scholar, told me, “We don't spend as much time thinking about privacy, data privacy, identity, and security as we should. I think that there is a narrative structure in place and I think companies make this problematic for people to think about” (I. O’Byrne, personal communication, February 12, 2020).

I asked the software theorist and education researcher Tom Liam Lynch about why people disclose much of their personal information despite the privacy risks. He replied that “...when you look at the interface design. It's the role, specifically, of buttons. When you click a button in the software space…it's masking all of these other legal, ethical, and other commitments that you're actually making.” He added that

“The actual implications of sharing your data are thoroughly masked by companies…they didn't want to slow you down. They don't want you to second guess it.” (T. L. Lynch, personal communication, February 18, 2020).

The citizen does not always have choice about what data to reveal or use in order to benefit from SNSs. Privacy is a multi-faceted concept (Baek et al., 2014; Baruh & Popescu, 2017; Ewbank, 2016; Petronio, 2013; Wachter, 2018). Additionally, little research has been conducted to investigate privacy literacy (Magolis & Briggs, 2016; Schmidt, 2013). This scarcity of research around privacy literacy is partly because it is a new literacy (Veghes, Orzan, Acatrinei, & Dugulan, 2012; Warzel, 2019; Wissinger, 2017); it is ill-defined (Johnson & Hamby, 2015; Solove, 2003; Solove & Schwartz, 2018); and it is sensitive to both culture and society (Nissenbaum, 2010).

The CLR has illuminated several gaps in the scholarship of privacy literacy. Theoretical gaps (see Figure 30) indicated a heavy emphasis on the communication privacy management theory (Petronio, 2002), as a dominant theoretical framework in the privacy literacy scholarship and less on other theoretical frameworks or perspectives which might indeed be better to study privacy literacy.

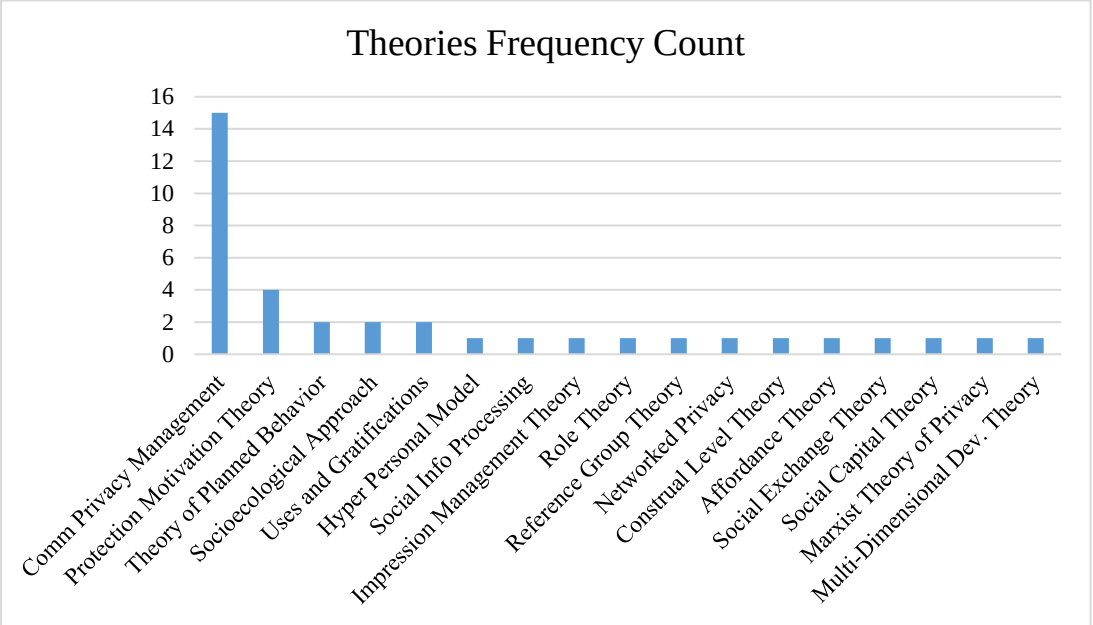


Figure 33. *QDA Miner Lite frequency analysis of theories used in privacy literacy scholarship*.

Moreover, self-reporting instruments, such as surveys, appeared to be the standard instrument regarding privacy literacy research (see Figure 31). More research needs to be conducted using other methods and designs, particularly methods that mix and remix data from back ends of systems and merge with front end data and traditional methodologies (e.g., focus groups and interviews). This means the richest research to understand socialization in online spaces includes mixing digitally native methods (API calls) with traditional methods, such as interviews (Gerber, 2016). These remixed methods that include both front-end and back-end data when paired with traditional research methods, can provide individuals a better understanding what is happening both within the platform (i.e., Facebook) and outside and through the platform (in real life) (Davidowitz, 2017; Gerber, Abrams, Curwood, & Magnifico, 2017; Gerber, Lynch, and Onwuegbuzie, forthcoming; Lynch & Gerber, 2018; Williamson, 2017).

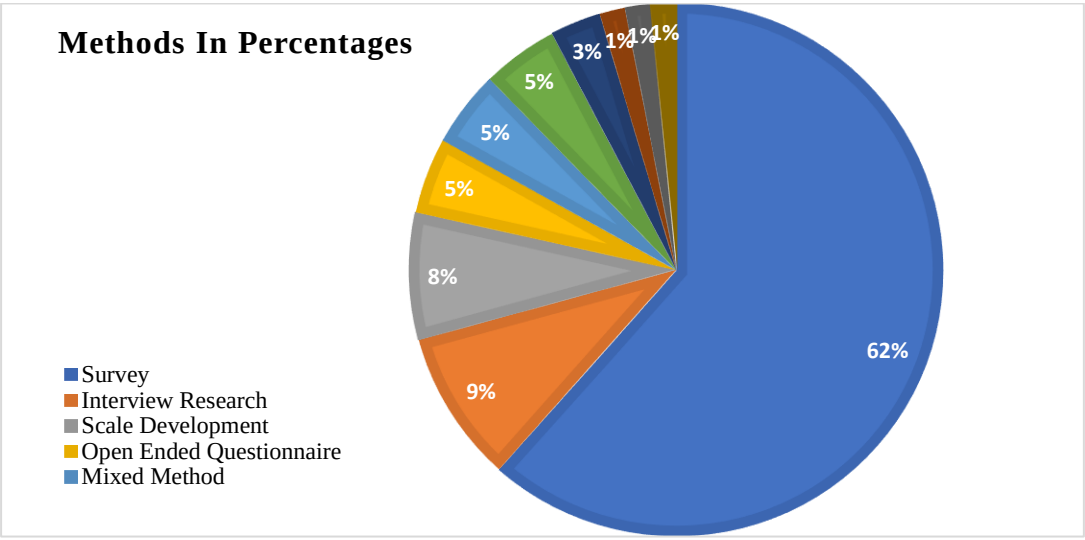


Figure 34. *Frequency analysis of the most used instruments/methods in privacy literacy scholarship*

Privacy versus transparency. Most of the research mentioned in this CLR revolved around investigating privacy literacy as a consequence of companies' software design and data collection practices. Table 14 summarizes research and topics:

Table 22. *Main research topics with example studies*

Topic	**Example of research**
Privacy management	Baruh, Secinti, & Cemalcilar, 2017; Child, Pearson, & Petronio, 2009; Child, & Starcher, 2016
Self-disclosure	Special & Li-Barber, 2012; Farinosi & Taipale, 2018
Privacy literacy competency	Trepte, Teutsch, Masur, Eicher, Fischer, Hennhöfer & Lind, 2015

Collective privacy management	Altman,1977; Marwick & boyd, 2014
Privacy practices such as obfuscation	Brunton & Nissenbaum, 2011

Some scholars (Aldritch, 2015; Kosinski, 2017; Webb, 2019) advanced the thought that scholarship and debate should shift from focusing on privacy as a consequence to focusing on transparency of data collection and processing. These scholars focused on what companies do with customer data and advocated for a transparent approach. I asked Hannah R Gerber, a digital literacies and software theory expert about her thoughts on this, and she said, "…it's not privacy that we are arguing for. What we are actually arguing for is complete transparency. So, that's the opposite, in a way of privacy, but we want to know what these tech companies collect and what they do with our data." I then asked her about privacy literacy and education. She posited that "… education starts before the algorithms are built. You bring in people before the algorithm is designed; you conduct focus groups; then you decide what data are people willing to share; and what do people want out of the platform…" (H. Gerber, personal communication, February 12, 2020).

These models advocate for the citizen inclusion in the design of data collection mechanisms and algorithms. The idea is that the citizen would consent to share their data prior to the design of the system and its algorithms. Some benefits of this model may reduce privacy concern, data breaches, and privacy paradox. The model is a reverse of the way scholarship and software design is currently practiced. The model would bring back the citizen to the center of media ecology, versus at the center of media consumerism.

Privacy surface level versus privacy at the deep level. When it comes to privacy literacy as illustrated in this CLR, most research and practice is centered around privacy at the surface level i.e., how to control data about ourselves (Bast & Brown, 2013; Liu et al., 2017; Proudfoot et al., 2018; Romo et al., 2017). Research then shifted focus on behavior studies (Dienlin & Trepte, 2015; Millham & Atkin, 2018; Park, 2013), citizen concern for loss of privacy (Ajayakumar & Ghazinour, 2017; Osatuyi, 2014), and the impact of privacy breaches on citizens' intentions to use SNSs (DeGroot & Vik, 2017; Taneja et al., 2014).

Contrary to these scholarship orientations is software operation at the deep level. In other words, what happens beyond the buttons that SNSs users click to secure their own privacy? Moreover, what happens from the back-end perspective, where data are amassed in aggregate and pre-packaged for marketing or surveillance? Some future research questions could be: (a) What happens beyond surface level privacy settings? And (b) How does that endanger our data, behavior, and self-disclosure practices?

Liquified surveillance. A key takeaway from this CLR is the pervasiveness and abundance of data available to government surveillance. Surveillance means the one that is present everywhere, just like the 'Big Brother' in *1984* (Orwell, 1949) or the panopticon as conceptualized by Bentham (Bentham, 1790, 1791). Surveillance is real and at when examining current practices of surveillance, they appear to be worse than the ones portrayed in *1984*. At least in *1984* surveillance was somewhat overt. I call the current state of surveillance a liquefied surveillance. The word liquified is an appropriate analogy because liquids take a multitude of shapes and forms depending on their surroundings. A key feature of this surveillance is the fact that majority of

people know that are being watched; yet they continue to reveal and show, subscribing to ‘the I have nothing to hide’ paradigm of thought.

Liquified surveillance has an objective of behavioral control and suppression more than protection and safety. This type of surveillance manipulates people’s state of expression, freedom, and how they connect with others through an omnipresent thought that everything an individual does or say is permanently stored. The stored data may not be all handled and analyzed with the same rigor, as it would be in the case of a dangerous threat; however, the liquified surveillance system is set to digitally oppress and suppress the public from expressing their political views, thoughts, and exercise of civic duties. The China social credit score is a perfect example of one of the mutations that could happen to liquified surveillance.

Social networking sites have opened a door to an unprecedented dataveillance (De Zwart et al., 2014; Fuchs, 2012a; Lyon, 2017; Marwick, 2012; ; Zuboff, 2015) that has different forms and shapes. We do not always see it, but it comes from the companies’ databases, our cell phones, peer surveillance, pictures taken about us, third party insights about our data, and much more. If data are everywhere, then so is surveillance.

Mapping the CLR and Privacy Literacy 2.0

One of the objectives of this CLR was to map the entire work and explain what it takes to be a privacy 2.0 literate individual. The mapping process is long; therefore, for practical reasons, I split the map into three parts: Self disclosure dynamics, Tech giants and data, and Privacy law. The maps contain elements of scholarship, consumer knowledge, as well as questions about the system.

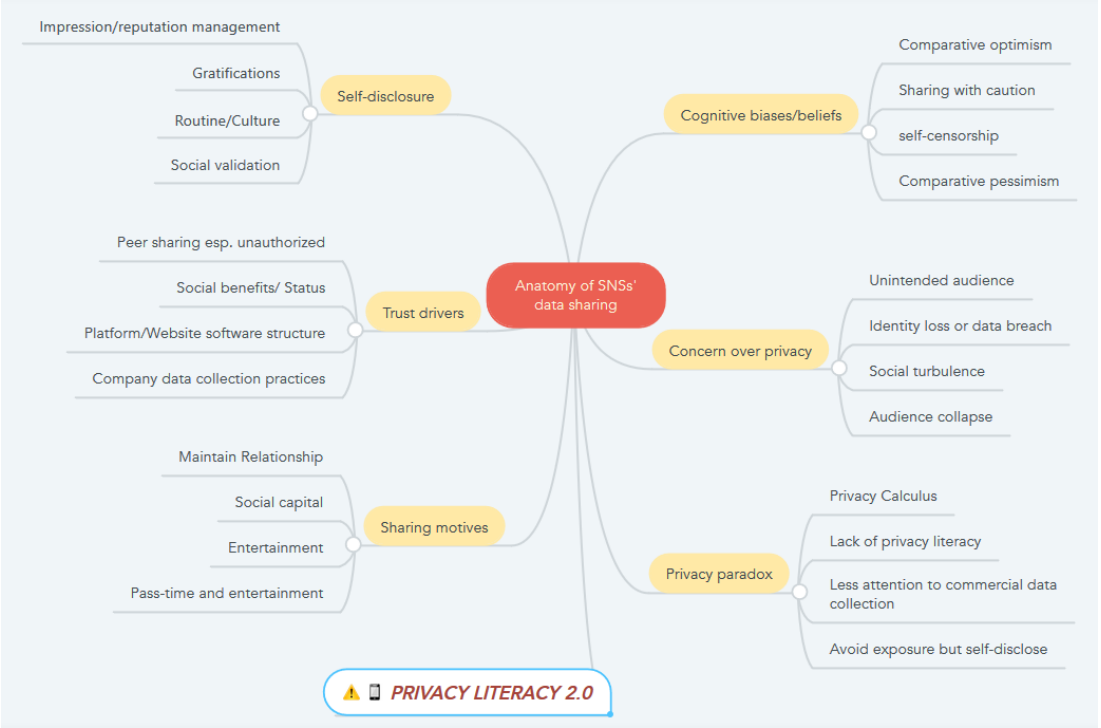


Figure 35. *Privacy literacy 2.0: Mind mapping the anatomy of SNSs' data sharing*

Self-disclosure on SNSs is driven by multiple key factors such as the cognitive biases, trust in the platform, the degree of concern, and entertainment. As evidenced by this CLR, almost all areas of the map require more research with regards to privacy literacy. Moreover, privacy literacy is also being aware of how self-disclosure and sharing occurs on SNSs.

Figure 36. *Privacy literacy 2.0: Tech giants business model and data collection practices*

The advancement in technology made it difficult for education and law to frequently update their practices. As the map shows, software has been an area of less focus in most privacy literacy studies. The deep layers of software (see Lynch, 2015) are a necessary knowledge for the general public. Additionally, the government control of data and reluctance on legislation spurs debate about data and public control through abundance of data amassment for surveillance purposes. And through this CLR, we learned that self-regulated companies' laws (e.g., privacy policy), and privacy engineering, without control or ethics, will only increase data collection and fail the individual citizen. As Renee Williams, attorney at law said, ". . . the consumers are a major player, but the consumers really don't have a say. So, you know… in those company decisions… they're just the target, so to speak" (R. L. Williams, personal communication, February 24, 2020).

Figure 37. *Privacy literacy 2.0: Law and the future of privacy*

When we speak about law and the future of privacy, we actually find more questions than answers. When we think of smart cities, nanotechnologies, and the social credit score of China, we start posing questions around transparency and death of privacy. Furthermore, this CLR showed examples and opinions about the government's lack of data regulation and legislation. Even when there will be data regulation for commercial companies, the remaining question will be about governmental agencies and surveillance. The citizen, as the central player in the privacy 2.0 map, may be required to become proactive rather than reactive. Non-Governmental Organization need to take their share of education and activism. Universities and K-12 schools need to start designing and implementing curricula for

privacy and data literacy. The government could also sponsor such activities and maybe push for a software-literacy for all.

Software, I believe, is the engine of all debates around data and privacy. Maybe it is time, more than ever before, for a federal review protocol that could assure software compliance with ethics of human-subject data collection. Software engineering should be regulated whenever there is a possibility of data collection or breach of human-data. The field of software design is non-regulated partly because it changes rapidly, and also, it is hard for public law and education institutions to remain updated.

Conclusion

This CLR has been inspired by the work of Onwuegbuzie and Frels' (2016) seven steps methodological framework. The model comprised seven steps: (a) Step 1: Exploring Beliefs and Topics (b) Step 2: Initiating the Search, (c) Step 3: Storing and Organizing Information (d) Step 4: Selecting/Deselecting Information, (e) Step 5: Expanding the Search to MODES (Media, Observations, Documents, Expert, Secondary Data), (f) Step 6: Analyzing and Synthesizing Information, (g) Step 7: Presenting the Comprehensive Literature Review. For the sake of dissertation formatting, I then added (h) step 8: Discussion and Implication of the CLR for Privacy Literacy 2.0.

From a dialectical pluralism 2.0 perspective (Johnson, 2011, 2012, 2017), I tried to listen to different research methods, perspectives, opinions, and live updates. I did that by analyzing scholarly work, conducting expert interviews, and analyzing publicly available SNSs data. The methods used for analysis derived from both traditional paradigms, qualitative and quantitative, as well as digitally native tools, as deemed necessary by the researcher.

Finally, I would like to close with these lingering questions about privacy literacy 2.0. (also see Figure 43), which remain unanswered by the current CLR:

1) In software engineering, could there be and Institutional Review Board (IRB) if the software involves data collection of human-subject?
2) Who owns the data generated by citizens?
3) Should citizens' insights be included in privacy engineering?

4) Is the problem about digital privacy enforcement or data transparency? Why?

5) How does software design release or restrict privacy and freedom of expression?

6) Will privacy laws hinder tech innovation?

7) Is free service for personal data the only business model?

Figure 38. *Privacy literacy 2.0: key questions*

REFERENCES

Aboulkacem, S. (2019). *Media and information literacy in Algeria: Perspectives from students, media practitioners, and government officials*. Deutsche Welle and Pyalara, Germany, Berlin: Pyalara publishing LLC.

Aboulkacem, S., & Haas, L. E. (2018). Perceptions, practices, and guiding principles of pre-service teachers in the quest for news and information across informal media. *The Online Journal of New Horizons in Education*, *8*(3), 129-139.

Aboulkacem, S., Haas L. E., & Winard, A. R. (2018). Perspectives from Algeria and the United States: media and news literacy perceptions and practices of pre-service teachers. *International Journal of Media and Information Literacy, 3*(2), 40-52.

Ackerman, P. L. (2008). Knowledge and cognitive aging. In F. I. M. Craik and T. A. Salthouse (Eds.). *The Handbook of aging and cognition*, (pp. 445–89). New York, NY: Psychology Press.

ACPA & NASPA. (2015). Professional competency areas for student affairs practitioners. Washington, D.C.: ACPA – College Student Educators International and NASPA–Student Affairs Administrators in Higher Education.

Acquisti, A. (2004, May 17). Privacy in electronic commerce and the economics of immediate gratification. In proceedings of the 5th ACM Electronic Commerce Conference, New York, NY: ACM Press.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE security & privacy*, *3*(1), 26-33.

Ajayakumar, J., & Ghazinour, K. (2017). I am at home: Spatial privacy concerns with social media check-ins. *Procedia Computer Science*, *113*, 551–558.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). Retrieved from https://journals.uic.edu/ojs/index.php/fm/article/view/2142/1949

Aldritch, R. (2015, May 7). Privacy is dead: The future is fabulous [video file]. Retrieved from https://www.youtube.com/watch?v=M11nmdKdKV8

Almgren, S. M., & Olsson, T. (2016). Commenting, Sharing and Tweeting News. *Nordicom Review*, *37*(2), 67–81. https://doi.org/10/f3tb3w

Alt, D. (2015). College students' academic motivation, media engagement and fear of missing out. *Computers in Human Behavior*, *49*, 111–119.

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.

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships.* New York, NY: Rinehart & Winston.

American Library Association. (1989, January 10). Presidential committee on information literacy. *Final report*. Chicago. Retrieved from http://www.ala.org/ala/acrl/acrlpubs/whitepapers/presidential.htm

Anderson, G. (2017, July 27). Walmart's facial recognition tech would overstep boundaries. *Forbes.* Retrieved from https://www.forbes.com/sites/retailwire/2017/07/27/walmarts-facial-recognition-tech-would-overstep-boundaries/#5a1b281445f8

Anderson, J., Rainie, L. (2012, July 20). Big Data: Experts say new forms of information analysis are helping us be more nimble and adaptive, but they worry over humans' capacity to understand and use new tools well. *Pew & American Life Project.* Retrieved from http://www.elon.edu/docs/eweb/predictions/expertsurveys/2012survey/PIP_Future_of_Internet_2012_Big_Data_7_20_12.pdf

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479-497.

Andrejevic, M. (2005). Nothing comes between me and my CPU: Smart clothes and 'ubiquitous' computing. *Theory, Culture & Society*, *22*(3), 101-119.

Armerding, T. (2018, December 20). The 18 biggest data breaches of the 21st century Security practitioners weigh in on the 18 worst data breaches in recent memory [website]. Retrieved from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Aufderheide, P., & Firestone, C. M. (1993). Media literacy: a report of the national leadership conference on media literacy. Washington DC, Aspen Institute.

Auxier, B., & Rainie, L. (2019, November 15). Key takeaways on Americans' views about privacy, surveillance and data-sharing. *Pew Research Center*. Retrieved from https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. *Pew Research Center.*

Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

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

Balkin, J. M. (2013). Old-school/new-school speech regulation. *Harvard Law Review*, *127*, 2296- 2342.

Ball, K. (2017). All consuming surveillance: surveillance as marketplace icon. *Consumption Markets & Culture*, *20*(2), 95–100.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), Retrieved from http://www.firstmonday.org/issues/issue11_9/barnes/index.html

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154.

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

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.

Bast, C. M., & Brown, C. A. (2013). Where has all our privacy gone? *Journal of Legal Studies in Business*, *18*, 17–43.

Bastos, M. T. (2015). Shares, pins, and tweets. *Journalism Studies*, *16*(3), 305–325.

Bavelas, J. B. (1983). Situations that lead to disqualification. *Human Communication Research*, 9, 130-145.

Bawden, D. (2001). Information and digital literacies: a review of concepts, *Journal of Documentation*, *57*(2), 218-259

Baxter, L. A. (1988). A dialectical perspective on communication strategies in relationships development. In S. W. Duck, D. F. Hay, S. E. Hobfoll, W. Ickes, & B. Montgomery (Eds.), *Handbook of personal relationships* (pp. 257-273). London: Wiley publishers.

Baxter, L. A. (2010). *Voicing relationships: A dialogic perspective*. Newbury Park, CA: Sage publishers.

Bedi, M. (2013). Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply. *Boston College Law Review*, *54*(1), 1–71.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, *35*(4), 1017-1042.

Bennett C., C. (1967). What price privacy? *American Psychologist*, *22*(5), 371–376.

Bentham, J. (1790). Bentham's draught for the organization of judicial establishments. *The Works of Jeremy Bentham*, *4*, 305, 316.

Bentham, J. (1791). *Panopticon or the inspection house*. London, UK: T. Payne.

Bentham, J., & Božovič, M. (1995). *The panopticon writings*. London, UK: Verso Trade.

Berkowitz, R. (2014, March 1). Privacy and politics. *The American Interest*. Retrieved from https://www.the-american-interest.com/2014/03/01/privacy-and-politics/

Berry, D. (2011). The computational turn: Thinking about the digital humanities. *Culture Machine 12*. Retrieved from: http://www.culturemachine.net/index.php/cm/article/view/440/470

Bertot, J. C., Gorham, U., Jaeger, P. T., Sarin, L. C., & Choi, H. (2014). Big data, open government and e-government: Issues, policies and recommendations. *Information Polity: The International Journal of Government & Democracy in the Information Age*, *19*(1/2), 5–16.

Biddle, S. J., Gorely, T., Pearson, N., & Bull, F. C. L. (2011). An assessment of self-reported physical activity instruments in young people for population surveillance: Project ALPHA. *International Journal of Behavioral Nutrition and Physical Activity*, *8*(1), 1–9.

Bigo, D. (2012). Digital surveillance and everyday democracy. In: Lyon D, Ball K, Haggerty KD (Eds.) *Routledge handbook of surveillance studies,* (pp. 151-161). New York, NY: Routledge.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018, May). Third party tracking in the mobile ecosystem. In *Proceedings of the 10th ACM Conference on Web Science*. ACM.

Bivins, R., & Marland, H. (2016). Weighting for health: Management, measurement and self-surveillance in the modern household. *Social History of Medicine, 29*(4), 757-780.

Blank, G., Bolsover, G., & Dubois, E. (2014). *A new privacy paradox: Young people and privacy on social network sites (Vol. 17)*. Oxford Internet Institute. Retrieved from

http://www.oxfordmartin.ox.ac.uk/downloads/A%20New%20Privacy%20Paradox%20April%202014.pdf

Bloom, R. M., & Clark, W. T. (2016). Small cells, big problems: the increasing precision of cell site location information and the need for Fourth Amendment protections. *Journal of Crime Law & Criminology*, *106*(2), 167-202.

Bossewitch, J., & Sinnreich, A. (2013). The end of forgetting: Strategic agency beyond the panopticon. *New Media & Society, 15*(2), 224–242.

boyd, D. (2008). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, Identity, And Digital Media.* The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press

boyd, d. (2012). Networked privacy. *Surveillance & Society*, 10(3-4), 348-350.

boyd, d. (2014). It's complicated: The social lives of networked teens. New Haven, CT: Yale University Press.

boyd, D., & Ellison, B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, *13*(1), 210-230.

Boyd, J. (2019, January 25). The history of Facebook: From BASIC to global giant. *Brandwatch.* Retrieved from https://www.brandwatch.com/blog/history-of-facebook/

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

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

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019). Thematic analysis. In P. Limaputtong (Ed.), *Handbook of research methods in health social sciences*, (pp. 843-860). Singapore: Springer Singapore.

Briggs, P., Churchill, E., Levine, M., Nicholson, J., Pritchard, G. W., & Olivier, P. (2016). Everyday Surveillance. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 3566–3573).

Brinson, N. H., & Eastin, M. S. (2016). Juxtaposing the persuasion knowledge model and privacy paradox: An experimental look at advertising personalization, public policy and public understanding. *Cyberpsychology*, *10*(1), 1–16.

BroadbandSearch. (2020). Time spent daily on social media (Latest data 2020) [Web-blog). Retrieved from https://www.broadbandsearch.net/blog/average-daily-time-on-social-media#post-navigation-3

Brook, C. (2019, Jun 10). Breaking Down LGPD, Brazil's New Data Protection Law. *Data Insider.* Retrieved from https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law

Brown, I. (2014). Social media surveillance. *The International Encyclopedia of Digital Communication and Society*. Advance online publication. doi:10.1002/9781118767771.wbiedcs122

Brown, M. (December, 1982). Personal computer "man of the year." *Time Magazine.* Retrieved from https://thisdayintechhistory.com/12/26/personal-computer-man-of-the-year/

Bruckman, A. (2002). Studying the amateur artist: A perspective on disguising data collected in human subjects research on the Internet. *Ethics and Information Technology*, *4*(3), 217-231.

Bruneel, S., De Wit, K., Verhoeven, J. C., & Elen, J. (2013). Facebook: When Education Meets Privacy. *Interdisciplinary Journal of E-Learning & Learning Objects*, *9*, 125–148.

Brunton, F., & Nissenbaum, H. (2011) Vernacular resistance to data collection and analysis: a political theory of obfuscation. *First Monday*, *16*(5). Retrieved from http://firstmonday.org/htbin/cgi wrap/bin/ojs/index.php/fm/article/view/3493/2955.

Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association*, *6*(1), 206-249.

Burgoon, J. K., Parrott, R., Le Poire, B., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships*, *6*, 131-158.

Campbell-Dollaghan, K. (2018, December 10). Sorry, your data can still be identified even if it's anonymized. *Fast Company.* Retrieved from https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized

Carbone, C. E. (2015). To be or not to be forgotten: Balancing the right to know with the right to privacy in the digital age. *Virginia Journal of Social Policy & the Law*, *22*(3), 525–560.

Cate, F. H. (2006). The failure of fair information practice principles. In J. K Winn (Ed.), *Consumer protection in the age of the information economy* (343-379). Surrey, UK: Ashgate Publishing.

Celeste, E. (2019). Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment?. *International Review of Law, Computers & Technology*, *33*(2), 122-138.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits and social influence. *Internet Research*, *25*(2), 279–299.

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior*, *54*, 483–490.

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*(5), 1859–1872.

Child, J., Pearson, J., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, 60, 1–16.

Chirita, A. D. (2018). The Rise of Big Data and the Loss of Privacy. In K. Bakhoum, C. B. Gallego, M. O. Mackenordt, & G. Surblytė-Namavičienė, (Eds.), *Personal data in competition, consumer protection and intellectual property law: Towards a holistic approach?* (pp, 153-189). Berlin; Heidelberg: Springer, MPI Studies on Intellectual Property and Competition.

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*(4), 480–500.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498-512.

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues, *Information Technology & People*, *7*(4), 6-37.

Cohen, J. E. (2012). *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven, CT: Yale University Press.

Cohen, J. E. (2012). What Privacy Is For. *Harvard Law Review*, *126*(7), 1904–19033.

Cohn, M. (2017, December) 'Beyond Orwell's worst nightmare', Huffington Post, Retrieved from: https://www.huffpost.com/entry/beyond-orwells-worst-nigh_b_4698242

Collins, K. (2017, November 21). Google collects Android users' locations even when location services are disabled. *Quartz*. Retrieved from https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

Connor, B. T., & Doan, L. (2019). Government and corporate surveillance: moral discourse on privacy in the civil sphere. *Information, Communication & Society*, 1–17.

Cope, B., & Kalantzis, M. (2015). The things you do to know: An introduction to the pedagogy of multiliteracies. In B. Cope, & M. Kalantzis (Eds.), *A pedagogy of multiliteracies: Learning by design* (pp. 1–36). London, UK: Palgrave.

Correia, J., & Compeau, D. (2017, January). Information privacy awareness (IPA): A review of the use, definition and measurement of IPA. In Proceedings of the 50th Hawaii International Conference on System Sciences. Hawaii, USA.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunication & High Tech Law.*, *10*, 273.

Crary, J. (2013) 24/7: Late Capitalism and the Ends of Sleep. New York, NY: Verso

Crowe, J. (2019). Cameras turned inwards: An enquiry into digital identities and the legitimisation of self-surveillance. *Critical Reflections: A Student Journal on Contemporary Sociological Issues*, 1-5.

Culnan, M. J., & Regan, P. M. (1995). Privacy issues and the creation of campaign mailing lists. *The Information Society*, *11*(2), 85-100.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*(2), 193–203.

De Mauro, A., Greco, M. and Grimaldi, M. (2015) 'What is big data? A consensual definition and a review of key research topics'. Presented at the 4th International Conference on Integrated Information, Madrid, 5-8 September.

De Montjoye, Y. A., Radaelli, L. V., Singh, K., & Pentland. A. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science, 347*(6221), 536–539.

De Wolf, R., Vanderhoven, E., Berendt, B., Pierson, J., & Schellens, T. (2017). Self-reflection on privacy research in social networking sites. *Behaviour & Information Technology*, *36*(5), 459–469.

De Zwart, M., Humphreys, S., & Van Dissel, B. (2014). Surveillance, big data and democracy: Lessons for Australia from the US and UK. *University of New South Wales Law Journal*, *37*(2), 713–747.

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 47-60). Berlin, Germany: Springer.

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108.

DeGroot, J. M., & Vik, T. A. (2017). "We were not prepared to tell people yet": Confidentiality breaches and boundary turbulence on Facebook. *Computers in Human Behavior*, *70*, 351–359.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 167-186.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, *45*(3), 285-297.

Dijck, J. van. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance and Society*, *12*(2), 197–208.

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

Eagle, N., Pentland, A. (Sandy), & Lazer, D. (2009). Inferring friendship network structure by using mobile phone data. *Proceedings of the National Academy of Sciences of the United States of America*, *106*(36), 15274–15278.

Eaton, P. W. (2017) Social media as everyday practice: Reflections on multiplicitous becoming activist. *Journal of Critical Thought & Praxis*, *6*(3), 55-70.

Eisenberg, M. B. (2008). Information Literacy: Essential Skills for the Information Age. *DESIDOC Journal of Library & Information Technology*, *28*(2), 39–47.

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society 37*, 32–64.

Eubanks, V. (2014, January 15) 'Want to predict the future of surveillance? Ask poor communities.' *The American Prospect*. Retrieved from http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities.

Evans, B. J. (2017). Power to the people: Data citizens in the age of precision medicine. *Vanderbilt Journal of Entertainment & Technology Law*, *19*(2), 243–265.

Everson, E. (2017). Privacy by design: Taking Ctrl of big data. *Cleveland State Law Review*, *65*(1), 27–43.

Ewbank, A. D. (2016, April 3). Student Privacy in the Age of Big Data. *Knowledge Quest*, 6–6.

Fallik, D. (2014). For big data, big questions remain. *Health Affairs-Chevy Chase, 33*(7), 1111–1114.

Farinosi, M., & Taipale, S. (2018). Who can see my stuff? Online self-disclosure and gender differences on Facebook. *Observatorio (OBS*), 12*(1), 53-71.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fleming, J. (2014). Media literacy, news literacy, or news appreciation? A case study of the news literacy program at Stony Brook University. *Journalism & Mass Communication Educator, 69*(2), 146–165.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160.

Fortier, A., & Burkell, J. (2018). Display and control in online social spaces: Towards a typology of users. *New Media & Society, 20*(3), 845–861.

Foucault, M. (1975). *Discipline and punish: The birth of the prison*. New York, NY: Pantheon.

Frabetti, F. (2015). *Software theory*. London, UK: Rowman & Littlefield.

Freire, P. (1970). *Pedagogy of the oppressed* (M. B. Ramos, Trans.). New York, NY: Sea-bury Press.

Fuchs, C. (2012b). The political economy of privacy on Facebook. *Television & New Media*, *13*(2), 139–159.

Fuchs, C. (2014). Social media and the public sphere. *Triple C: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *12*(1), 57-101.

Fuchs, C. (Ed.). (2012a). *Internet and surveillance: The challenges of Web 2.0 and social media*. New York, NY: Routledge.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (2011). Internet and surveillance: The challenges of Web 2.0 and social media. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, *1*(16), 352–352

Fujisaki, Y., & Kang, S. J. (2019). The influence of twitter and Facebook on supports toward anti-government demonstration in Japan: Focused on protests against nuclear power plants and Japanese military legislation in 2015. *Social Science Review*, *50*(1), 127–147.

Future Today Institute. (2019). Tech trends report [Web-report]. Retrieved from https://futuretodayinstitute.com/2019-tech-trends/

Fu-Yuan Hong, & Su-Lin Chiu. (2016). Factors influencing Facebook usage and Facebook addictive tendency in university students: The role of online psychological privacy and Facebook usage motivation. *Stress & Health: Journal of the International Society for the Investigation of Stress*, *32*(2), 117–127.

Gadekar, R., & Pant, S. (2015). Exploring Facebook users' privacy knowledge, enactment and attitude: A study on Indian youth. *International Journal of Communication Research; Iasi*, *5*(4), 273–283.

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), 279–288.

Gerber, H. R. & Lynch. T. L. (2017). Into the meta: Research methods for moving beyond social media surfacing techniques. *Tech Trends 61* (3), 263-272.

Gerber, H. R. (2008). New literacy studies: *Intersections and disjunctures between in-school and out-of-school literacies among adolescent males*. Unpublished doctoral dissertation. The university of Alabama.

Gerber, H. R. (2016, June). *Tracing informal learning: The role of social media analytics to understand meaning making in informal spaces*. Keynote address at the Joint European Conference on Technology Enhanced Learning, Roosta Resort, Estonia.

Gerber, H. R. (2018, September). *#love and*  : *Looking back to see the future.* Presidential Welcome Address at the 2018 Annual Conference for the International Council for Educational Media. Tallinn, Estonia.

Gerber, H. R., & Lynch, T. L. (2017). Into the meta: Research methods for moving beyond social media surfacing. *Tech Trends*, *61*(3), 263-272.

Gerber, H. R., & Lynch, T. L. (in press). Mixed methods integration to understand social media data. In J. Hitchcock & A. J. Onwuegbuzie (Eds.), *Routledge Handbook for Advancing Integrating in Mixed Methods Research.*

Gerber, H.R., Abrams, S.S., Curwood, J.S., & Magnifico, A.M. (2017). Conducting qualitative research of learning in online spaces. Thousand Oaks, CA: SAGE.

Gillis, T. B., & Simons, J. (2019). Explanation < Justification: GDPR and the perils of privacy. *Pennsylvania Journal of Law and Innovation*, *2*(71), 72-99.

Gilster, P. (1997). *Digital literacy.* New York, NY: John Wiley & Sons

Giroux, H.A., 2015. Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies*, *29*(2), pp.108-140.

Givens, C. L., (2015). *Information privacy fundamentals for librarians and information professionals.* New York, NY: Rowman and Littlefield.

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Anchor Press.

Golish, T. D. (2003). Stepfamily communication strengths: Understanding the ties that bind. *Human Communication Research*, *29*(1), 41-80.

Goodrum, A. (2014). Snopa and the Ppa: Do you know what it means for you? If Snopa (social Networking Online Protection Act) or Ppa (password Protection Act) Do Not pass, the snooping could cause you trouble. *Hamline Journal of Public Law & Policy*, *35*(1), 131–155.

Gopal, R. D., Hidaji, H., Patterson, R. A., Rolland, E., & Zhdanov, D. (2018). How much to share with third parties? User privacy concerns and website dilemmas. *MIS Quarterly*, *42*(1), 143-164.

Graber, M. A., D Alessandro, D. M., & Johnson-West, J. (2002). Reading level of privacy policies on internet health web sites. *Journal of Family Practice*, *51*(7), 642-642.

Greene, J. C. (2007). *Mixed methods in social inquiry*. San Francisco, CA: Jossey-Bass.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books.

Greenwald, G. (2014, October). Why privacy matters?. [Video file]. Retrieved from https://www.ted.com/talks/glenn_greenwald_why_privacy_matters?language=en#t-430404

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps into user data of Apple, Google and others. *The Guardian.* Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods, 18*(1), 59-82.

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

Halpern, E. S. (1984). *Auditing naturalistic inquiries: The development and application of a model*. Unpublished doctoral dissertation, Indiana University.

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

Henderson, S., & Gilding, M. (2004). 'I've never clicked this much with anyone in my life': trust and hyper personal communication in online friendships. *New media & society*, *6*(4), 487-506.

Herrman, A. R., & Tenzek, K. E. (2017). Communication privacy management: A thematic analysis of revealing and concealing eating disorders in an online community. *Qualitative Research Reports in Communication*, *18*(1), 54–63.

Hill, K. (2012, February 12). How target figured out a teen girl was pregnant before her father did. *Forbes.* Retrieved from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#23fcd0636668

Hobbs, R. (2010). Digital and media literacy: A plan of action. A white paper on the digital and media literacy recommendations of the Knight Commission on the information needs of communities in a democracy. Washington, DC: The Aspen Institute. Retrieved from www.knightcomm. org/digital -and-media-literacy/

Hobbs, R. (2016). *Exploring the roots of digital and media literacy through personal narrative*. Philadelphia, PA: Temple University Press.

Hodkinson, P. (2017). Bedrooms and beyond: Youth, identity and privacy on social network sites. *New Media & Society*, *19*(2), 272-288.

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society*, *30*(6), 377-386.

Horesley, J. (2019, November 16). China's Orwellian social credit score isn't real. *FP*. Retrieved from https://foreignpolicy.com/2018/11/16/chinas-orwellian-social-credit-score-isnt-real/

Horton, F. W. (2007). *Understanding information literacy: A primer.* Paris, France: Information Society Division, Communication and Information, UNESCO.

Hubaux, J. P., & Juels, A. (2016). Privacy Is Dead, Long Live Privacy. *Communications of the ACM*, *59*(6), 39–41

Igo, S. (2018). *The known citizen*. Cambridge, MA: Harvard University Press.

Information is Beautiful & Thomson Reuters. (2019, May). Number of compromised data records in selected data breaches as of November 2018 (in millions) [Website]. Retrieved from https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/.

Ingram, M. (2013, March 20). Even the CIA is struggling to deal with the volume of real-time social data [Web-blog]. Retrieved from https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/

Jackson, A. (2016, February 11). Husband and wife never expected their Fitbit would tell them this. *CNN Health.* Retrieved from https://www.cnn.com/2016/02/10/health/fitbit-reddit-pregnancy-irpt/index.html

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, *69*, 302–310.

Jia, H., & Xu. H. (2016). Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology*, *10*(1), 33–51.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note: privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information System Research, 24*(3):579–95.

Johnson, B., & Christensen, L. (2014). *Educational research: Quantitative, qualitative and mixed approaches* (4thed.). Thousand Oaks, CA: Sage Publications.

Johnson, R. B. (2011, May). Dialectical pluralism: A metaparadigm to help us hear and "combine" our valued differences. In S. J. Hesse Biber (Chair), *Addressing the credibility of evidence in mixed methods research: Questions, issues and research strategies.* Plenary conducted at the meeting of the seventh International Congress of Qualitative Inquiry, University of Illinois at Urbana- Campaign.

Johnson, R. B. (2017). Dialectical pluralism: A metaparadigm whose time has come. *Journal of Mixed Methods Research*, *11*(2), 156–173.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher*, *33*(7), 14-26.

Johnson, R. H., & Hamby, B. (2015). A meta-level approach to the problem of defining 'Critical Thinking'. *Argumentation*, *29*(4), 417-430.

Johnson, R.B. (2012). Dialectical pluralism and mixed research. *American Behavioral Scientist*.*56*(6), 751–754.

Jones, B., & Flannigan, S. L. (2006). Connecting the digital dots: Literacy of the 21st century. *Educause Quarterly*, *29*(2), 8-10.

Jordaan, Y., & Van Heerden, G. (2017). Online privacy-related predictors of Facebook usage intensity. *Computers in Human Behavior*, *70*, 90–96.

Jourard, S. M. (1964). *The transparent self.* New York, NY: Van Nostrand Co.

Joyce, D. (2015). Privacy in the digital era: Human rights online?'. *Melbourne Journal of International Law*, *16*, 270-284.

Juang, S. Y., & Juang, J. G. (2012, July). Real-time indoor surveillance based on smartphone and mobile robot. Paper presented at the IEEE 10th International Conference on Industrial Informatics. Beijing, China.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), 59-68.

Kats, R. (2018, June 1). Many Facebook users are sharing less content [website]. Retrieved from https://www.emarketer.com/content/many-facebook-users-are-sharing-less-content-because-of-privacy-concerns

Kember, S., & Zylinska, J. (2012). *Life after new media: Mediation as a vital process*. Cambridge, MA: MIT Press.

Kennedy, H., & Moss, G. (2015). Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society, 2*(2), 1-11.

Kerber, W. (2016). Digital markets, data, and privacy: Competition law, consumer law, and data protection. *Journal of Intellectual Property Law & Practice*, *11*(11), 856–866.

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology*, *10*(1), 52–71.

Kim, H. S. (2015). Attracting views and going viral: How message features and news-sharing channels affect health news diffusion. *Journal of Communication*, *65*(3), 512–534.

King, J. (2019, June 19). Trust social networks with your data? Nah. Use social networks anyway? Yep [website]. Retrieved from https://www.emarketer.com/content/users-have-little-faith-in-social-networks-privacy-protections

Kitchin, R., & Dodge, M. (2011). *Code/space: software and everyday life*. Cambridge, MA: MIT Press.

Klein, L. F., Eisenstein, J., & Sun, I. (2015). Exploratory thematic analysis for digitized archival collections. *Digital Scholarship in the Humanities*, *30*(1), 130-141.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Kondor, D., Hashemian, B., Montjoye, Y. de, & Ratti, C. (2018). Towards matching user mobility traces in large-scale datasets. *IEEE Transactions on Big Data*, 1–1.

Kosinski, M. (2017, March 4). End of privacy [Video File]. Retrieved from https://www.youtube.com/watch?v=NesTWiKfpD0

Kosinski, M. (2019, July 22). End of privacy [Video File]. Retrieved from https://www.youtube.com/watch?v=VUwBcTgzbtU

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805.

Kraut, R., Olson, J., Banaji, M., Bruckman, A., Cohen, J., & Couper, M. (2010). Building commitment and contribution in online groups through social interaction. Ethics Working Paper.

Krejecie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, *30*(3), 607-610.

Kshetri, N. (2014). Big data′s impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145.

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management*, *34*(6), 761–769.

Kyei-Blankson, L., Iyer, K. S., & Subramanian, L. (2016). Social networking sites: College students' patterns of use and concerns for privacy and trust by gender, ethnicity, and employment status. *International Journal of Information and Communication Technology Education (IJICTE)*, *12*(4), 62–75.

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *Journal of Consumer Affairs, 43*(3), 380–388.

Lanham, A. (1995). Digital literacy. *Scientific American, 273*(3) 160–161.

Lanier, J. (2013). How Should We Think about Privacy? *Scientific American*, *309*(5), 64–71.

Laufer, R. S., Proshansky, H.M., & Wolfe, M. (1976). Some analytic dimensions of privacy. In H.M. Proshansky, W.H. Ittelson, & L.G. Rivlin (Eds.), *Environmental psychology: People and their physical settings* (2nd Ed). New York, NY: Holt, Rinehart and Winston.

Le, H. M., Yue, Y., Carr, P., & Lucey, P. (2017, August). Coordinated multi-agent imitation learning. In Proceedings of the 34th International Conference on Machine Learning. JMLR. org.

Leaver, T. (2015). Born digital? Presence, privacy, and intimate surveillance. In Hartley, John & W. Qu (Eds.), Re-Orientation: *Translingual transcultural transmedia: Studies in narrative, language, identity, and knowledge* (pp. 149–160). Shanghai, China: Fudan University Press.

Leaver, T. (2017). Intimate surveillance: Normalizing parental monitoring and mediation of infants online. *Social Media + Society*, *3*(2), 1-10.

Lee, H., Park. H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Humans & Computer Studies, 71*(9):862–77.

Lehavot, K. (2009). "MySpace" or yours? The ethical dilemma of graduate students' personal lives on the Internet. *Ethics & Behavior*, *19*(2), 129–141.

Lehavot, K. (2009). “MySpace” or Yours? The ethical dilemma of graduate students’ personal lives on the Internet. *Ethics & Behavior, 19*(2), 129–141.

Liang, H., Shen, F., & Fu, K. (2017). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society*, *19*(9), 1476–1497.

Lincoln, Y. S., Lynham, S.A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions, and emerging confluences. In N. K. Denzin, and Y. S. Lincoln (Eds.), *Handbook of qualitative research* (4th ed.) (pp. 97-128). Thousand Oaks, CA: Sage publications.

Litt, E., & Hargittai, E. (2014). A bumpy ride on the information superhighway: Exploring turbulence online. *Computers in Human Behavior*, *36*, 520–529.

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social Media+ Society*, *2*(1), 1-12.

Liu, Q., Yao, M. Z., Yang, M., & Tu, C. (2017). Predicting users’ privacy boundary management strategies on Facebook. *Chinese Journal of Communication*, *10*(3), 295–311.

Luft, J. (1969). *Psychology of human interaction*. Palo Alto, CA: National Press.

Lynch, T. L., Gerber, H.R., & Onwuegbuzie, A. (forthcoming). *Making big data small: integrating approaches for social science researchers*. Sage Publishers.

Lynch, T.L. (2015). *The hidden role of software in education: From policy to practice*. London, UK: Routledge.

Lynch, T.L., & Gerber, H.R. (2018). The ontological imperative when researching the digital. *International Journal of Multiple Research Approaches, 10*(1), 112–123.

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance and Society, 13*(2), 139–152.

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

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.

Mackey, T. P., & Jacobson, T. E. (2011). Reframing information literacy as a metaliteracy. *College & research libraries, 72*(1), 62-78.

Madden, M. & Rainie, L. (2015, May 20). Americans' attitudes about privacy, security and surveillance [website]. Retrieved from https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

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

Manovich, L. (2013). *Software takes control*. New York, NY: Bloomsbury

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., Byers., A. (2011, May). Big data: The next frontier for innovation, competition, and productivity. *The McKinsey Global Institute.* Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx

Marr, B (2019, January). Chinese social credit score: Utopian big data bliss or black mirror on steroids? Retrieved from

https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#59466fb348b

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378-393.

Marwick, A. E. (2013). *Status update: Celebrity, publicity, and branding in the social media age*. New Haven, CT: Yale University Press.

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133.

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067.

Marwick, A. E., & boyd, d. (2018). Understanding privacy at the margins. *International Journal of Communication (19328036)*, *12*.

Maslow, A. H., & Mittelmann, B. (1941). *Principles of abnormal psychology*. New York, NY: Harper.

Maurice, P., Lavoie, M., Laflamme, L., Svanström, L., Romer, C., & Anderson, R. (2001). Safety and safety promotion: definitions for operational developments. *Injury Control and Safety Promotion*, *8*(4), 237-240.

McDonald, A., Cranor. L. (2009). The cost of reading privacy policies. *I/S: A J. Law and Polio/ Inform. Soc. 4*(3), 543-568.

Merchant, G., Weibel, N., Pina, L., Griswold, W. G., Fowler, J. H., Ayala, G. X., Gallo, L. C., Hollan, J., & Patrick, K. (2017). Face-to-face and online networks: college students' experiences in a weight-loss trial. *Journal of Health Communication*, *22*(1), 75–83.

Metzger, M. J., & Docter, S. (2003). Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting & Electronic Media*, *47*(3), 350–374.

Milan, S. (2015). Mobilizing in Times of Social Media. From a Politics of Identity to a Politics of Visibility. *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*, 53–72.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Thousand Oaks, CA: Sage.

Miller, A. R. (1969). Personal privacy in the computer age: The challenge of a new technology in an information-oriented society. *Michigan Law Review*, *67*(6), 1089-1246.

Millham, M. H., & Atkin, D. (2018). Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors. *New Media & Society*, *20*(1), 50–67.

Mims, C. (2018, May 6). Privacy is dead. Here's what comes next. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001

Mohamed, E., Gerber, H. R., & Aboulkacem, S. (Eds.). (2016). *Education and the Arab Spring: Resistance, reform, and democracy*. Rotterdam, The Netherlands: Sense Publishers.

Moll, R., Pieschl, S., & Bromme, R. (2014). Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in human behavior*, *41*, 212-219.

Monteleone, S. (2015). Addressing the “Failure” of informed consent in online data protection: learning the lessons from behaviour aware regulation. *Syracuse Journal of International Law & Commerce*, *43*(1), 69–119.

Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy*, *39*(9), 771–786.

Morning Consult. (2018, May). How comfortable are you with companies being able to purchase data related to you, such as an email address, for online advertising purposes? [Website]. Retrieved from https://www.statista.com/statistics/873789/internet-users-comfort-companies-purchasing-personal-data-online-ad-reasons/.

Morris, A., Onwuegbuzie, A. J., & Gerber, H. R. (2018). Using expert interviews within modes in online and offline spaces to extend comprehensive literature review processes. *The Qualitative Report 23*(8), 1777-1798.

Morris, M. (2016). My fitness pal? Calorie counting in an age of self-surveillance.

Morton, A., & Sasse, M. A. (2014, July). Desperately seeking assurances: Segmenting users by their information-seeking preferences. Paper presented at the Twelfth Annual International Conference on Privacy, Security and Trust. IEEE. Toronto, Canada.

Muoio, D. (2016, June 1). Nest could be working on a smart crib that can tell you why your baby is crying. *Tech Insider,* Retrieved from https://www.businessinsider.com.au/google-patents-smart-crib-2016-6

Murphy, M. H. (2016). Technological solutions to privacy questions: What is the role of law? *Information & Communications Technology Law*, *25*(1), 4–31.

Nakashima, R. (2013, August 13). AP Exclusive: Google tracks your movements, like it or not. *AP News.* Retrieved from https://apnews.com/828aefab64d4411bac257a07c1af0ecb

Napoli, P. M. (2015). Social media and the public interest: Governance of news platforms in the realm of individual and algorithmic gatekeepers. *Telecommunications Policy*, *39*(9), 751–760.

National Association for Media Literacy Education. (2007, November). Core principles of media literacy education in the United States [Website]. Retrieved from http://namle.net/publications/core-principles.

National Science and Technology Council. (2019, June). National privacy research strategy. *PCAST.* Retrieved from https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf

NCTE (2019, November 7). Position statement [Website]. Retrieved from https://ncte.org/statement/nctes-definition-literacy-digital-age/

Newell, S., Marabelli, M., (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification. *The Journal of Strategic Information Syst*ems. *24*(1), 3–14.

Newman, I., Ridenour, C. S., Newman, C., & DeMarco, G. M. P. (2003). A typology of research purposes and its relationship to mixed methods. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 167-188). Thousand Oaks, CA: Sage.

News & Events. (2018, March 27). How PredPol uses big data for predictive policing. *Data Science.* Retrieved from

https://www.datasciencegraduateprograms.com/2018/03/has-big-data-brought-us-closer-to-the-world-depicted-in-minority-report/

Nippert-Eng, C., E. (2010). *Islands of privacy*. Chicago, IL: The University of Chicago Press.

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Norman, G., Pepall, L., Richards, D., & Tan, L. (2016). Competition and consumer data: The good, the bad, and the ugly. *Research in Economics*, *70*(4), 752–765.

Nowak, G. J., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing*, *11*(4), 94-108.

Obar, J. A. (2015). Big Data and the phantom public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data & Society*, *2*(2), 1-16.

O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York, NY: Crown Publishers.

Onwuegbuzie, A. J., & Frels, R. (2016). *Seven steps to a comprehensive literature review: A multimodal and cultural approach*. Thousand Oaks, CA: Sage Publications.

Onwuegbuzie, A. J., & Frels, R. K. (2013). Introduction: Toward a new research philosophy for addressing social justice issues: Critical dialectical pluralism 1.0. *International Journal of Multiple Research Approaches, 7*(1), 9-26

Onwuegbuzie, A. J., & Leech, N. L. (2007). Validity and qualitative research: An oxymoron?. *Quality & quantity*, *41*(2), 233-249.

Onwuegbuzie, A. J., Johnson, R. B., & Collins, K. M. (2009). Call for mixed analysis: A philosophical framework for combining qualitative and quantitative approaches. *International Journal of Multiple Research Approaches*, *3*(2), 114-139.

Orwell, G. (1949). *Nineteen-Eighty Four*. New York, NY: Penguin.

Osatuyi, B. (2014). An instrument for measuring social media users' information privacy concerns. *Journal of Current Issues in Media & Telecommunications, 6*(4), 359–375.

Osatuyi, B., Passerini, K., Ravarini, A., & Grandhi, S. A. (2018). "Fool me once, shame on you… then, I learn." An examination of information disclosure in social networking sites. *Computers in Human Behavior, 83*, 73–86.

Palen, L., & Dourish, P. (2003, April). Unpacking" privacy" for a networked world. Proceedings of the SIGCHI conference on Human factors in computing systems. Lauderdale, Florida, USA.

Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media, 49*(3), 259–281.

Papathanassopoulos, S. (2015). Privacy 2.0. *Social Media + Society*, *1*(1), 1-2.

Park, M.-S., Shin, J.-K., & Ju, Y. (2015). A Taxonomy of social networking site users: Social surveillance and self-surveillance perspective. *Psychology & Marketing*, *32*(6), 601–610.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236.

Paul, M. J., Sarker, A., Brownstein, J. S., Nikfarjam, A., Scotch, M., Smith, K. L., & Gonzalez, G. (2016). Social media mining for public health monitoring and surveillance. Paper presented tat the Biocomputing Proceedings of the Pacific symposium. Kohala Coast, Hawaii, USA.

Payton, T., & Claypoole, T. (2014). *Privacy in the age of big data*. Lanham, MD, US: Rowman and Littlefield.

Peirce, C. (1893). Fallibilism. *Commens*. Retrieved from http://www.commens.org/dictionary/term/fallibilism

Pereira, S., Robinson, J. O., Peoples, H. A., Gutierrez, A. M., Majumder, M. A., Mcguire, A. L., & Rothstein, M. A. (2017). Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLoS ONE*, *12*(9), 1–11.

Perekalin, A. (2019, April 22). Ten tips to make your private digital life really private. *Kaspersky Daily*. Retrieved from https://usa.kaspersky.com/blog/privacy-ten-tips-2018/15719/?utm_source=facebook&utm_medium=social&utm_campaign=us_privacy-report_yn0105_promo&utm_content=video&utm_term=us_facebook_promo_yn0105_video_social_privacyreport&gclid=CjwKCAjw2cTmBRAVEiwA8YMgzfqFLdkGt5xj2CX-F3-0YF58YsVb6ZkUHa7IkV6ONS9qS_As-am7JhoCPQwQAvD_BwE

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*(1), 6–14.

Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality: Grasping the complexities through CPM theory. In T. Afifi & W. Afifi (Eds.), *Uncertainty and information regulation in interpersonal contexts: Theories and applications* (pp. 365 – 383). New York, NY: Routledge

Phua, J., Jin, S. V., & Kim, J. (Jay). (2017). Uses and gratifications of social networking sites for bridging and bonding social capital: A comparison of Facebook, Twitter, Instagram, and Snapchat. *Computers in Human Behavior*, *72*, 115–122.

Pisani, J. (2019, April 23). 'The creepy factor': Stores add cameras that can guess your age and sex to target ads. *Chicago Tribune*. Retrieved from https://www.chicagotribune.com/business/ct-biz-walgreens-kroger-store-cameras-20190423-story.html

Postman, N. (1970). The reformed English curriculum. In A. C. Eurich (Ed.), *High school 1980: The shape of the future in American secondary education* (pp.160–168). New York, NY: Pitman.

Potter, J. (2014). *Media literacy*. Thousand Oaks, CA: Sage.

Power, D. J. (2016). "Big Brother" can watch us. *Journal of Decision Systems*, *25*(1), 578–588.

Preneel, B., Rogaway, P., Ryan, M. D., & Ryan, P. (2014). Privacy and Security in an Age of Surveillance. *Dagstuhl Reports*, *4*(9), 106-123.

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature Medicine*, *25*(1), 37–43.

Privacy International. (2018, December). How apps on Android share data with Facebook (even if you don't have a Facebook account) [Web-report].

Retrieved from https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

Proudfoot, J. G., Wilson, D., Valacich, J. S., & Byrd, M. D. (2018). Saving face on Facebook: Privacy concerns, social benefits, and impression management. *Behaviour & Information Technology*, *37*(1), 16–37.

Quinn, K. (2014). An ecological approach to privacy: "Doing" online privacy at midlife. *Journal of Broadcasting & Electronic Media*, *58*(4), 562–580.

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.

Rachels, J. (1975). Why privacy is important. *Ethical issues in the use of computers*, *4*(4), 323- 333.

Rainie, L. (2018, March 18). Americans' complicated feelings about social media in an era of privacy concerns. *Pew Research Center.* Retrieved from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Rainie, L., & Duggan, M. (2016, January 14). Privacy and information sharing [website]. Retrieved from https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/

Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*, *17*(3), 185-197

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday,* 15, 1–4.

Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., . . . Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal, 30*(1), 39–88.

Reuters. (2016, April 22). James Clapper pressed for number of citizens US collects data on. *The Guardian.* Retrieved from https://www.theguardian.com/world/2016/apr/22/james-clapper-nsa-spying-us-data-collection-senate-hearing

Ridout, B., Campbell, A., & Ellis, L. (2012). "Off your Face(book)": Alcohol in online social identity construction and its relation to problem drinking in university students. *Drug & Alcohol Review*, 31, 20–26.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339–362.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Romo, L. K., Thompson, C. M., & Donovan, E. E. (2017). College drinkers' privacy management of alcohol content on social-networking sites. *Communication Studies, 68*(2), 173–189.

Ruhenstroth, M. (2018, December 23). How Facebook knows which apps you use – and why this matters. *Mobilsicher.* Retrieved from https://mobilsicher.de/ratgeber/how-facebook-knows-which-apps-you-use-and-why-this-matters

Safire, W. (2002, November). You are a suspect. *The New York Times*. retrieved from http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.htm

Samuels, D. (2019, January 23). Is big tech merging with big brother? Kinda looks like it. *Wired.* Retrieved from https://www.wired.com/story/is-big-tech-merging-with-big-brother-kinda-looks-like-it/

Sattikar, A. A., & Kulkarni, D. R. (2011). A review of security and privacy issues in social networking. *International Journal of Computer Science and Information Technologies, 2*(6), 2784-2787.

Schadt, E. (2015, November). The role of big data in medicine. *McKinsey & Company. https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/the-role-of-big-data-in-medicine#*

Schintler, L. A., & Kulkarni, R. (2014). Big data for policy analysis: The good, the bad, and the ugly. *Review of Policy Research*, *31*(4), 343–348.

Schmidt, H. C. (2012). Media, millennials, and the academy: Understanding the state of media literacy within higher education. *Journal on Excellence in College Teaching*, *23*(4), 53-75.

Schmidt, H. C. (2013). Media literacy education from kindergarten to college: A comparison of how media literacy is addressed across the educational system. *Journal of Media Literacy Education 5*(1): 295-309.

Scolari, C. A. (2012). Media ecology: Exploring the metaphor to expand the theory. *Communication Theory*, *22*(2), 204–225.

Semitsu, J. P. (2011). From Facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance. *Pace Law Review*, *31*(1), 291.

Shade, L. R., & Singh, R. (2016). “Honestly, We’re not spying on kids”: School surveillance of young people’s social media. *Social Media+ Society, 2*(4), 1-15.

Shapiro, C., Carl, S., & Varian, H. R. (1998). *Information rules: a strategic guide to the network economy*. Cambridge, MA. Harvard Business Press.

Shin, D. H., & Choi, M. J. (2015). Ecological views of big data: Perspectives and issues. *Telematics and Informatics, 32*(2), 311–320.

Silverblatt, A. (2008). *Media literacy: Keys to interpreting media messages* (3rd ed.). West Port, CT: Praeger Publishers

Silverman, J. (2015). *Terms of service: Social media and the price of constant connection*. New York, NY: Harper Collins.

Sinclair, S., Rockwell, G., & the Voyant Tools team. (2012). Voyant Tools. Retrieved from http://voyant-tools.org/

Singer, N., Conger, K. (2019, September 4). Google is fined $170 million for violating children’s privacy on YouTube. *The New York Times.* Retrieved from https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html

Sisson, P. (2018, January 17). Your city is watching you: How machine learning and “computer vision” will transform our cities. *Curbed*. Retrieved from https://www.curbed.com/2018/1/17/16897222/machine-learning-urban-planning-sidewalk-labs

Skinner, Q. & Marshall, R. (2013, July26) ‘Liberty, liberalism and surveillance: a historic overview. *Open Democracy.* Retrieved from https://www.opendemocracy.net/en/opendemocracyuk/liberty-liberalism-and-surveillance-historic-overview/

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European journal of operational research, 177*(3), 1333-1352.

Smith, A. (2014). What Internet users know about technology and the Web. *Pew Research Center*. Retrieved from http://www.pewinternet.org/files/2014/11/PI_Web-IQ_112514_PDF.pdf

Smith, C. (2013, October 10). 7 statistics about Facebook users that reveal why it's such a powerful marketing platform. *Tech Insider.* Retrieved from https://www.businessinsider.com.au/a-primer-on-facebook-demographics-2013-10

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167-196.

Smith, K. (2019, December 30). 122 Amazing social media statistics and facts [website]. Retrieved from https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/#section-2

Solove, D. J. (2003). The virtues of knowing less: Justifying privacy protections against disclosure. *Duke Law Journal, 53,* 967.

Solove, D. J. (2006). "A Taxonomy of Privacy," *University of Pennsylvania Law Review 154*(3), 477-560.

Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven, CT: Yale University Press

Solove, D. J., & Schwartz, P. (2018). *Information privacy law* (6th ed.). New York, NY: Wolters Kluwer Law & Business.

Special, W. P., & Li-Barber, K. T. (2012). Self-disclosure and student satisfaction with Facebook. *Computers in Human Behavior*, *28*(2), 624–630.

Sprout Social. (2017, November). Preferred social media platforms accessed by internet users in the United States to share life milestones [Website]. Retrieved from https://www.statista.com/statistics/809980/us-internet-users-preferred-social-media-platforms-share-life-milestones/.

Statista Survey. (2017b, August). Have you ever had the following positive, tangible benefits, from being active on social media? [Website]. Retrieved from https://www.statista.com/statistics/379350/positive-benefits-from-being-on-social-media/.

Statista. (2017a, June). Statista Survey Advertising & Privacy [Website]. Retrieved from https://www-statista-com.ezproxy.shsu.edu/statistics/714048/us-internet-user-personal-data-worry-online-retail/

Stein, J. (2016). Lies, the whole lies and nothing but the lies. *Time*, *188*(25–26), 158–158.

Stephens-Davidowitz, S., & Pabon, A. (2017). *Everybody lies: Big data, new data, and what the internet can tell us about who we really are*. New York, NY: HarperCollins.

Stoddard, J. (2014). The need for media education in democratic education. *Democracy & Education*, *22*(1), 1-9.

Sundstrom, B. (2016). Mothers "Google It Up:" Extending communication channel behavior in diffusion of innovations theory. *Health communication*, *31*(1), 91-101.

Syn, S. Y., & Kim, S. U. (2016). College students' health information activities on Facebook: Investigating the impacts of health topic sensitivity, information

sources, and demographics. *Journal of Health Communication*, *21*(7), 743–754.

Taddicken, M. (2014). The “privacy paradox” in the social Web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/jcc4.12052/abstract

Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual’s attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, *38*, 159–173.

The International ICT Literacy Panel. (2007). *Digital transformation: A Framework for ICT literacy*. Princeton, NJ: Education Testing Service

The New London Group. (1996). A pedagogy of multiliteracies: Designing social futures. *Harvard educational review*, *66*(1), 60-93.

Thompson, D. (2012). I Agreed to what-a call for enforcement of clarity in the presentation of privacy policies. *Hastings Communications and Entertainment Law Journal*, *35*(1), 203-226.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “online privacy literacy scale” (OPLIS). In *Reforming European Data Protection Law* (pp. 333–365). Springer, Dordrecht.

Trope, Y., & Liberman, N. (2000). Temporal construal and time-dependent changes in preference. *Journal of personality and social psychology*, *79*(6), 876.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological review, 117*(2), 440-463

Trottier, D. (2014). Crowdsourcing CCTV surveillance on the Internet. *Information, Communication & Society, 17*(5), 609–626.

Trottier, D. (2016). *Social media as surveillance: Rethinking visibility in a converging world*. New York, NY: Routledge.

Trottier, D. (2019). A research agenda for social media surveillance. *Fast Capitalism, 8*(1), 59-68.

Trottier, D., & Lyon, D. (2012). Key Features of social media surveillance. In Fuchs, C., K. Boersma, A. Albrechtslund, and M. Sandoval (Eds.), *Internet and Surveillance: The challenges of web 2.0 and social media* (pp 89-105). New York, NY: Routledge.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media & Society*, *20*(1), 141–161.

Tucker, P (2015). *The naked future*. New York, NY: Penguin Group

Tucker, P. (2013, May 7). Has big data made anonymity impossible?. *MIT Technology Review.* Retrieved from https://www.technologyreview.com/s/514351/has-big-data-made-anonymity-impossible/

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20–36.

Tuominen, K. (2007). Information Literacy 2.0, *Signum*, 5, 6–12.

Turow, J. (2012). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven. CT: Yale University Press.

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to exploitation: American shoppers online and offline*. Philadelphia, PA: University of Pennsylvania: Annenberg Public Policy Center.

Turow, J., Hennessy, M., & Draper, N. (2018). Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003–2015. *Journal of Broadcasting & Electronic Media*, *62*(3), 461–478.

Unuchek, R. (2018). Leaking ads--is user data really secure? [PowerPoint slides]. Retrieved from https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8161/ASEC-T08-Leaking-Ads-Is-User-Data-Truly-Secure.pdf .

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., & Gill, P. (2016). Tracking the trackers: towards understanding the mobile advertising and tracking ecosystem. *ArXiv:1609.07190 [Cs]*. http://arxiv.org/abs/1609.07190

Veghes, C., Orzan, M., Acatrinei, C., & Dugulan, D. (2012). Privacy literacy: what is and how it can be measured?. *Annales Universitatis Apulensis: Series Oeconomica*, *14*(2), 704-711.

Velten, J. C., Arif, R., & Moehring, D. (2017). Managing disclosure through social media: How Snapchat is shaking boundaries of privacy perceptions. *The Journal of Social Media in Society, 6*(1), 220–250.

Vishwanath, A., Xu, W., & Ngoh, Z. (n.d.). How people protect their privacy on Facebook: A cost-benefit view. *Journal of the Association for Information Science and Technology*, *69*(5), 700–709.

Vitak, J., & Ellison, N. B. (2013). 'There's a network out there you might as well tap': Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. *New Media & Society*, *15*(2), 243-259.

Vitak, J., Lampe, C., Gray, R., & Ellison, N. B. (2012). Why won't you be my Facebook friend?: Strategies for managing context collapse in the workplace. Proceedings of the 7th Annual iConference. Ontario, Canada.

Vraga, E. K., Bode, L., Smithson, A. B., & Troller-Renfree, S. (2016). Blurred lines: Defining social, news, and political posts on Facebook. *Journal of Information Technology & Politics*, *13*(3), 272–294.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, *34*(3), 436–449.

Wahyuningtyas, S. Y. (2017). Abuse of Dominance in Non-Negotiable Privacy Policy in the Digital Market. *European Business Organization Law Review*, *18*(4), 785–800.

Waldman, A. E. (2015). Privacy as trust: Sharing personal information in a networked world. *University of Miami Law Review*, *69*(3), 559–630.

Waldman, A. E. (2016). Privacy, notice, and design. *Stanford Technology Law Review*,*21*(4), 76-126.

Waldman, A. E. (2019). Privacy law' s false promise. *Washington University Law Review*, *97*(3), 1-76

Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology*, *114*(2), 246-257.

Warzel, C. (2019, April 16). Privacy is too big to understand. *The New York Times*. retrieved from https://www.nytimes.com/2019/04/16/opinion/privacy-technology.html

Warzel, C. (2019, August 6). The privacy project. *The New York Times*. Retrieved from https://static.nytimes.com/emailcontent/PRIV_sample.html?module=newsletterconfirmationemail&version=regi&contentId=PRIV&eventName=readlatestnewsletter&region=copy&emc=confirmregi_PRIV_20190418&nl=PRIV

Wash, R. (2013, February 11). The big bang: How the big data explosion is changing the world. *Microsoft News Center.* Retrieved from https://news.microsoft.com/2013/02/11/the-big-bang-how-the-big-data-explosion-is-changing-the-world/

Webb, A. (2019, March 27). Privacy is dead [video file]. Retrieved from https://www.youtube.com/watch?v=vpeXGBhHyQU

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & society*, *58*(1), 20-41.

Westgate, E. C., Neighbors, C., Heppner, H., Jahn, S., & Lindgren, K. P. (2014). "I will take a shot for every 'like' I get on this status": Posting alcohol-related Facebook content is linked to drinking outcomes. *Journal of Studies on Alcohol & Drugs*, 75, 390–398.

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

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. New York, NY: New Press.

Whittaker, z. (2017, July 12). Millions of Verizon customer records exposed in security lapse [Web-blog]. Retrieved from https://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/

Whittaker, Z. (2018, September 11). Online security 101: Tips for protecting your privacy from hackers and spies [Web-blog]. Retrieved from https://www.zdnet.com/article/simple-security-step-by-step-guide/

Williamson, B. (2015). Governing software: Networks, databases and algorithmic power in the digital governance of public education. *Learning, Media & Technology*, *40*(1), 83–105.

Williamson, B. (2017). *Big data in education: The digital future of learning, policy and practice*. Thousand Oaks, CA: Sage.

Wissinger, C.L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy, 11*(2), 378-389.

Witzleb, N., Paterson, M., & Richardson, J. (2019) (Eds.). *Big data, political campaigning and the law: Democracy and privacy in the age of micro-targeting*. New York, NY: Routledge.

Worldwide. (2017, May). Types of personal information and images shared digitally by global internet users [Website]. Retrieved from https://www.statista.com/statistics/266835/sharing-content-among-us-internet-users/.

Wright, D., Rodrigues, R., Raab, C., Jones, R., Székely, I., Ball, K., Bellanova, R., & Bergersen, S. (2015). Questioning surveillance. *Computer Law & Security Review*, *31*(2), 280–292.

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897.

Xu. H., Luo. X.R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. *Dec Support Syst*, *51*(1):42–52.

Zibuschka, J., Kurowski, S., Roßnagel, H., Schmuck, C. H., & Zimmermann, C. (2019). Anonymization is dead–long live privacy. Open Identity Summit, Bonn, Germany.

Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. *Ethics and information technology*, *12*(4), 313-325.

Zittrain, J. (2008). Privacy 2.0. *University of Chicago Legal Forum*, 65-119.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: Profile Books.

VITA

Slimane Aboulkacem, Ed.D.

Sam Houston State University

The school of Teaching and Learning

Department of Education

EDUCATION

March 2020 Doctorate of Education, The School of Teaching and Learning, Sam Houston State University, Huntsville, Texas, USA University of Sam Houston. Texas, United States. Dissertation Title: Privacy Literacy 2.0 Framework: A three-layered comprehensive media & literature review.

2009-2013 M.A. Applied Linguistics, Department of English, Faculty of Letters and Foreign Languages, Algiers University of Algiers-2-, Algiers., Algeria. Master's thesis: The Use of Writing Conferences to Teach Students about Tense Shift in Narrative Paragraphs. A Case Study of EFL Algerian Freshman Students

2012-2015 MBA in Management/Marketing. Dual Degree: Institut International des Sciences Commercial (Algiers) and Paris Graduate School of Management

Master's Thesis: Customer service delight: an inquiry into Techno- Stationary customers' experience with locally made products in Algeria

2009-2010 Degree of higher studies in Management. ECOFAM, Joint School of Management. University of Perpignan, France and Algeria

2005-2009 Bachelor of Arts in English Language Teaching Pedagogy, Department of English, Faculty of Letters and Foreign Languages, University of Algiers, Algeria

CERTIFICATION

2019 Social Media Analytics Certificate. Queensland University of Technology.

2016 Certificate of completion of Technology Enhanced Learning course. School of Digital Technologies, Tallinn University, Estonia

2014 SAP Certificate of Human Capital Management. College of Business Administration. Sam Houston State University. Huntsville, Texas

2012-2013 Advanced Studies in French Language at Institut Français, Algiers, Algeria (Expert Level)

2013 DALF C1 & DELF B2 (French Language Studies Diplomas). Institut Français, Algiers, Algeria

GRANTS, FELLOWSHIPS AND HONORS

2019 Participant in piloting DA.RE European Union Project on data science (visit http://dare-project.eu/)

Tasks

•Took the beta course and application of data analytics

•Participated in program evaluation

•Discussed with members and administrators the best ways to improve the product

2019 Alumni Engagement Innovation Fund Winners: Empowering rural women to make soap and cleaning products with a business plan for sustainability. (Grant: 15,000$) Role: Project co-leader.

Tasks

•Project research

•Proposal drafting

•Budget drafting

•Project implementation

•Project assessment and evaluation

2016-2017 Alumni Engagement Innovation Fund Winners: Exchange in English Caravane across Algeria. (Grant: 20,000$) Role: Member and professional developer

Tasks

•Designed recruitment survey

•Analyzed participants survey-returns

•Project Assessment

2016 JTEL- Joint Technology Enhanced Learning summer school. School of Digital Technologies, Tallinn University, Estonia

2015 Alumni Engagement Innovation Fund Winners: Innovating English Language teaching in Algeria. (Grant: 20,000$) Role: Data analyst

Tasks

•Co-drafted the project

•Designed recruitment survey

•Analyzed participants survey-returns

•Project Assessment

2013 Fulbright Language Teaching Assistantship at Sam Houston State University, Huntsville, Texas, USA

Tasks

•Designed lessons

•Ran a conversational club and cultural visits

•Delivered culture-related seminars

RESEARCH AND SCHOLARSHIP

PUBLICATIONS

Books:

Eid, M., Gerber, H. R., & Aboulkacem. S. (Eds.). (2016). Education and the Arab Spring: Shifting toward Democracy. Rotterdam, The Netherlands: Sense Publishers

Book Chapters:

Aboulkacem, S., Foster, C., Gerber, H., & Montenegro, M. (2018). "I am a Shape-changing, Mask-wearing, Sixteen year-old" Super-heroine: Women in comics and identity construction. In Eckard. S (Ed.). Connecting the dots in classroom research. Jossey Brass, LA: California

Aboulkacem, S. Gerber, H, R., & Eid, M. (2016). Introduction: Education, democracy, and the Arab Spring. In M. Eid, H.R. Gerber, & S. Aboulkacem (Eds.). Education and the Arab Spring: Shifting toward Democracy. Rotterdam, The Netherlands. Sense Publishers

Bouguerra, F., & Aboulkacem, S. (2016). Vulnerability of the Tunisian Education System: a pendulum swing between hope and reality. In M. Eid, H.R. Gerber & S. Aboulkacem (Eds.). Education and the Arab Spring: Shift toward Democracy. Rotterdam, The Netherlands. Sense Publishers

Research Articles/ Reports

Winard, A., Aboulkacem, S., & Haas, L. E. (Forthcoming). Preservice teachers' perspective of photovoice and visual literacy experiences. IVLA book. Routledge

Aboulkacem, S. (2019). Media and information literacy in Algeria: Perspectives from students, media practitioners, and government officials. DW and PLAYAR Sponsored research report.

Research Tasks

•Consulted on report design

•Snowball-hied the participants

•Consulted on instrument design (Quantitative and Qualitative)

•Collected and directed data collection process

•Analyzed data

•Wrote and published the report

Aboulkacem, S., Haas, L. E., & Winard, A. R. (2018). Perspectives from Algeria and the United States: Media and News Literacy Perceptions and Practices of Pre-service Teachers. Media Education Journal

Aboulkacem, S., & Haas, L. E. (2018). Perceptions, Practices, and Guiding Principles of Pre-service Teachers in the Quest for News and Information across Informal Media. International Journal of New Horizons in Education

Book Reviews

Aboulkacem, S. (2017). Conducting qualitative research of learning in online spaces by Gerber, H.R., Abrams, S.S., Curwood, J.S. & Magnifico, A.M. (2016). READ Journal

Columns

Aboulkacem, S. & Gerber, H, R. (2016). Culture and ethnicity in select videogames: Portrayals of minorities in Action. Voice of Youth Advocate (VOYA)

Conference Proposals (presented)

Winard, A. R., & Aboulkacem, S. (2019, October). Perceptions of pre-service teachers using photovoice inside and outside the classroom. Paper presented at the 51st annual conference of the International Visual Literacy Association, Brussels, Belgium

Winard, A. R., Haas, E., L. & Aboulkacem, S. (2019, February). Photovoice and visual literacy: Perspectives from pre-service teachers. Paper presented at the 6th Universality of Global Education conference, Sam Houston State University, Texas, USA

Aboulkacem, S. & Winard, A. R. (2018, November). How do pre-service teachers quest for news and information across informal media: Perspectives from the U.S., and Algeria. Panel presentation at Information & Media Literacy: Interdisciplinary Perspectives on Education and Digitalization in a Mediatized Information and Knowledge Society, Passau University, Passau, Germany

Montenegro, M. A., Aboulkacem, S. & Votteler, N. B. (2018, February). Readers' voices in a book club: Costarican high schoolers' perceptions of reading for pleasure. Paper presented at the 5th Universality of Global Education conference, Sam Houston State University, Texas, USA

Nasiri, S., Montenegro, A. M., & Aboulkacem, S. (2017). Caring across communities: Strategies to help teach refugees and ELLs. Paper presented at the Texas Association for Literacy Education (TALE), University of Texas A&M, Corpus Christi, Texas, USA

Aboulkacem, S., & Haas, L. E. (2017). Do I feel confident about understanding news? Measuring pre-service teachers' News media literacy abilities across social media. Round-table session presented at the Texas Association for Literacy Education (TALE), University of Texas A&M, Corpus Christi, Texas, USA

Aboulkacem, S. (2016). Education in Tunisia: Swinging between hope and reality. Paper presented at the 3rd International Universality of Educational Issues conference, Sam Houston State University, The Woodlands Centre, The Woodlands, Texas, USA

Aboulkacem, S. (2016). From video gaming to crafting papers: Writing through play. Poster session presented at the JTEL- Joint Technology Enhanced Learning summer school. School of Digital Technologies, Tallinn University, Estonia

Aboulkacem, S., & Montenegro, M. (2016). Videogames and writing: what students could take from home to class. Poster session presented at the Literacy Summit Conference, University of the Incarnate Word, San Antonio, Texas, USA

Gerber, H. R. (chair), Gaitan, L., Aboulkacem, S. (2015). Mobile gaming, girls' empowerment, and developing nations: A civic engagement project during Egypt's transitional democracy. Paper submitted for Featured Paper on the Association of Educational Computing and Technology, Indianapolis, Indiana, USA

Aleisa, M., Aboulkacem, S., Fuqua, J. & Gerber, H. R. (2015). Incidental language learning and popular media: A conceptual software design. Round-table session presented at the Association of Educational Computing and Technology Conference, Indianapolis, Indiana, USA

Peer-Reviewed International Professional Conferences

Aboulkacem, S. (2017, October). Media Assault: Perceptions, Practices, and Guiding Principles of Pre-service Teachers in the Quest for Information across Informal Media. UNESCO Media and Information Literacy Feature Conference, Kingston, Jamaica

Aboulkacem. S, & Haas, L. E. (2017, July). Exploring Online News Media Practices of College Students. Paper accepted for an Oral Session at the 20th European Literacy Conference. Madrid, Spain

Aboulkacem, S. (2017, March). Assistant and Member of the International Council for Education Media. Creating mobile learning resources for displaced populations in times of emergencies and crises. A Strategy Lab session at Mobile learning week Conference at UNESCO Headquarters, Paris, France

Montenegro, M. A., Aboulkacem, S. & Votteler, N. B. (2016, August). Readers' voices and free reading: Let's gather and talk. Paper presented for 3rd Baltic Sea / 17th Nordic Literacy Conference arranged and hosted by FinRA in Turku/Åbo, Finland

Gerber, H. R., & Aboulkacem, S. (2015, May). Citizen Media, Digital Literacy, and Mobile Games: Shifting Pedagogy for Exploration and Discovery. Proposal presented to the International Multidisciplinary Conference on English Language, Literature, and Information Technology. Muscat, Oman

TEACHING

Higher Education Experience

Fall 2019 Research assistant on a federally sponsored grant for clinical behavioral research. Role: Coding and analyzing behavioral data charts.

Fall 2018 Teacher Assistant of Digital Literacy and Pedagogy, READ 5313. The School of Learning and Teaching, College of Education at Sam Houston State University, Huntsville, Texas, USA

Summer 2018 Teacher Assistant of Digital Literacies, READ 6088. Department of Literacy, Language and Special Populations, College of Education at Sam Houston State University, Huntsville, Texas, USA

Spring 2018 Teacher Assistant of Literacy and Learning Grade 8-12, READ 5311. Department of Literacy, Language and Special Populations, College of Education at Sam Houston State University, Huntsville, Texas, USA

Fall 2017 Teacher Assistant of Digital Literacy and Pedagogy, READ 5313. Department of Literacy, Language and Special Populations, College of Education at Sam Houston State University, Huntsville, Texas, USA

Fall 2016 Teacher Assistant of Workshop in Bilingual Education and Second Language Learning, BESL 4088. Department of Literacy, Language and Special Populations, College of Education at Sam Houston State University, Huntsville, Texas, USA

2015 to 2019 Research Assistant, Department of Literacy, Language and Special Populations, College of Education at Sam Houston State University, Huntsville, Texas, USA

2013-2014 Teacher Assistant/Arabic Language and MENA Culture, Department of Foreign Languages, College of Humanities and Social Sciences, Sam Houston State University, Huntsville. Texas, USA

2011- 2012 Teacher Assistant, Department of English, Faculty of letters and Foreign Languages, University of Algiers, Algiers, Algeria at Algiers University. Algiers, Algeria

2010-2011 Teacher Assistant, Department of English, Faculty of letters and Foreign Languages, University of Algiers, Algiers, Algeria Teacher Assistant at Algiers University. Algiers, Algeria

Course Teaching Experience

At Sam Houston State University

Undergraduate

- •READ 5313 01 Digital Literacy and Pedagogy
- •READ 5311 01 Literacy and Learning Grade 8-12
- •MCOM 1130 04 Media Literacy

Graduate

- •READ 6089 02 Independent Studies in Reading
- •READ 6088 03 Digital Literacies
- •Seminar in using software to conduct comprehensive literature review
- •Seminar in Bilingual Education
- •Seminar in Sociolinguistics
- •Arabic and MENA culture

At University of Algiers 2

Undergraduate

- •English Language Acquisition
- •Linguistics
- •English for Specific Purposes
- •Grammar

SERVICE

NGO service 2018-present.....Board member and Finance Chairman of Diversity Education Non-Profit.

Tasks

- •Oversee budget drafting and expenses
- •Supervise spending and expenses
- •Co-ordinated meetings with board members and field managers
- •Negotiate future projects
- •Oversee grant drafting and research

•Reported to the CEO

•Supervise the NGO App design

•Supervise the NGO performance management system for remote countries

•Review grants

Guest Speaker 2018 QDA Miner and literature review selection and analysis process. Sam Houston State University—A doctoral class

Guest Speaker 2019 Digital privacy literacy in the age of mass surveillance, University of Southern Main—Preservice teachers.

STEM Summer 2018Co-lead teachers' STEM summer camp (N= 300 teachers).

Tasks

•Camp design

•Material design and curriculum development

•Co-led camp implementation

•Lead sessions and learning experiences

•Led material illustration

•Trouble shoot technology products and use

Tutor English 2018 Tutor of writing at the Academic Success Center. Sam Houston State University.

Faculty book circle Co-facilitator of university wide reading circle on Weapons of Math Destruction by Cathy O'Neil.

Lab research 2016-2017 Manager of a science videogame design team at the Center of Excellence in Digital Forensics, Sam Houston State University

Tasks

•Oversee the purchase demands of the software team

•Attendance

•Debrief the project's progress

•Resources needs analysis

•Led team cooperation and communication to reach targeted objectives

•Reported to the director of the lab on the project progress

•Resources acquisition

SKILLS

Software: Microsoft office, QDA Miner, Voyant Tools, TAGS API, Hoaxy API, SPSS, Tableau, Gephi, SAP (Human Capital Management), Qualtrics surveys.

Research: Qualitative, Quantitative, and Mixed Methods research designs; grant writing; statistical analysis; interviewing; focus groups; observation protocol design; instrumentation validation and administration.

Miscellaneous: Negotiation, leadership, stress management, time management, inter-personnel communication, conflict resolution, research.

EDITORIAL ASSISTANT:

2019 Assistant Manager of READ Journal, a scientific literacy research journal housed at the college of Education, Sam Houston State University.

Tasks

•Contact selected authors to start the review process

•Perform first screening of articles topic fit and sound method

•Blind the manuscripts and assign them for review

•Gather updates about the review process

•Follow up with authors' revisions

•Copy-edit the manuscripts and relay them to publisher

2017 Guest reviewer of Education Media International Journal, Austria.

2017 Editor of Texas Association of Literacy Education conference proposals

2014-2015 Editorial Assistant of Educational Media International Journal, Special Edition, Austria

2015-2017 Editorial Assistant and Committee Member of English in Texas Journal

PROFESSIONAL ASSOCIATIONS

ICEM International Council of Education and Media (Member since 2015)

IVLA International Visual Literacy Association (Member since 2019)

AECT Association of Education and Communication Technologies. (Member since 2015)

NAMLE National Association of Media Literacy Education. (Member since 2016)

Association of Algerian American Scientists. USA. (Member since 2014)

Algerian Scout: Assistant Youth Tutor. (Member since 1994)

Texas Youth Soccer League. (Coach 2016-17)

LANGUAGE PROFICIENCY

Berber (native), French (fluent), Arabic (fluent), English (fluent), Spanish (Basic skills)