A NEW FRAMEWORK OF PRIVACY CONCERNS ASSESSMENT IN THE CONTEXT OF FACIAL RECOGNITION TECHNOLOGY (FRT): MIXED-METHODS SEQUENTIAL EXPLORATORY ANALYSIS OF YOUTUBE USERS

by

Yazeed Alhumaidan

A Dissertation Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

in Information Studies

at

University of Wisconsin-Milwaukee

May 2021

ABSTRACT

A NEW FRAMEWORK OF PRIVACY CONCERNS ASSESSMENT IN THE CONTEXT OF FACIAL RECOGNITION TECHNOLOGY (FRT): MIXED-METHODS SEQUENTIAL EXPLORATORY ANALYSIS OF YOUTUBE USERS

by

Yazeed Alhumaidan

The University of Wisconsin-Milwaukee, 2021
Under the Supervision of Dr. Michael Zimmer

Facial Recognition Technology (FRT) has become one of the most rapidly growing technologies. A statistical report expected that the global market size of FRT will record an increase by over 100% within five years, from $3.8 billion in 2020 to $8.5 billion in 2025 ("Facial Recognition Market Size, Share and Global Market Forecast to 2025 ," n.d.). The proliferation of FRT is primarily related to the organizational desire to bridge integrity, credibility, and reliability vulnerabilities that are inherent in traditional identification mechanisms. The ambiguity of how information flows in this system has led to an increase in individuals' privacy concerns. Prior studies have statistically measured the volume of individuals' privacy concerns of FRT across various regions and contexts. However, the authors have failed to investigate the root of those concerns to provide a thorough framework illustrating the dimensions of FRT-related activities that breach privacy principles. This doctoral dissertation, therefore, bridged this gap by diving into user-generated text on the YouTube platform to develop a new framework of the most common FRT-related privacy concerns.

The sequential exploratory mixed-method design was selected to evaluate user-generated text on 206 FRT-related YouTube videos. In the qualitative phase, user-generated text on five FRT-related videos was analyzed to explore different dimensions of FRT-related users' privacy concerns. In the quantitative phase, the supervised text classification was

developed through SVM algorithms to apply the qualitative findings to a larger sample to achieve the external validity requirement. The sequential analysis of 206 video transcripts, 123301 top-level comments, and 75326 low-level comments revealed that what has motivated the users' privacy risk belief in FRT lies in nine dimensions divided into four main themes: information collection (surveillance, coercion), information processing (retention period, profiling, security, secondary use, exclusion) information dissemination (disclosure), and invasion (decisional interference). The findings should contribute to reconceptualizing privacy in the context of FRT as well as offering a comprehensive insight of current privacy laws flaws that are of interest to policymakers to enact new privacy laws or reform existing privacy laws to address organizations' abuses and protect the individuals' right to privacy in the era of FRT.

© Copyright by Yazeed Alhumaidan, 2021
All Rights Reserved

To

my inspired parents, brothers, and sister

my beloved wife and kids

my supportive friends

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

As long as I remain alive, I would be grateful to Almighty Allah for the health, power, time, and other countless resources motivated me to overcome life's challenges, especially challenges that faced me during the doctoral stage. One resource played a key role in the dissertation success is the open-handed people who have always been there for me without expecting something in return. Heartfelt thanks go to my parents, brothers, sister, wife, and kids for being the main inspiration source during the darkest moments by giving their never-ending love and support that made me enjoy my research. I am at a loss for words to express my thanks to Dr. Michael Zimmer for agreeing to be my major professor whose long experience and deep knowledge in privacy issues and academic research assisted me to cover the knowledge gap that I had and progress my dissertation in an effective approach. I am also forever indebted to Dr. Xiangming "Simon" Mu, Dr. Margaret Kipp, Dr. Wonchan Choi, and Dr. Shion Guha for serving on my dissertation and providing a great deal of professional feedback that improved the manuscript and my research skills. Last but not least, I thank Dr. Nadine Kozak, Dr. Dietmar Wolfram, Dr. Iris Xie, Dr. Jin Zhang, and Dr. Richard Smiraglia for building a solid base of knowledge of research methodologies and theories related to information science and technology during coursework.

Chapter 1: Introduction

Background

FRT has become one of the most rapidly growing technologies. According to Jain, Bolle, and Pankanti, (2006) and S. Liu & Silverman (2001), it is a form of Biometric Recognition Technologies (BRTs) that describe personal identity through extracting facial features, (e.g., the width of the nose and the curve of the chin). The system has been designed to perform one-to-many comparisons in an identification model where extracted facial features are compared with a database containing several face templates to detect who is that person (e.g., identifying travelers at border checkpoints). On the other hand, the system performs one-to-one comparisons in a verification model where extracted facial features are compared with a database containing a single face template to detect whether or not the identity belongs to a person who claimed that (e.g., verifying smartphone users). The central difference between the two models lies in informed consent, where an identification sensor could scan a person's face from a long distance without that person's knowledge or authorization, while a verification sensor scans a person's face from a short distance that often requires personal knowledge and authorization.

A statistical report expected that the global market size of FRT will record an increase by over 100% within five years, from $3.8 billion in 2020 to $8.5 billion in 2025 (“Facial Recognition Market Size, Share and Global Market Forecast to 2025 ,” n.d.). The proliferation of FRT is primarily related to the organizational desire to bridge integrity, credibility, and reliability vulnerabilities (e.g., identity frauds) that are inherent in traditional identification mechanisms (e.g., physical ID). A mass of government, for-profit, nonprofit, forensic, and other related organizations have implemented the system for different security aspects across offline and online environments, such as safeguarding mobile phone content (Haifeng Li & Zhu, 2016), and detecting identity frauds (Chen, Kuang Hsieh, & Tsai, 2010). However, the

community's acceptance of the implementation or usage of FRT relies on the extent to which organizations to comply with certain privacy principles as a result of the complex connection between security and privacy.

In 2018, the Future of Privacy Forum published a document consisting of seven privacy principles for FRT: consent, use-respect for context, transparency, data security, privacy by design, integrity and access, and accountability (*Privacy Principles for Facial-Recognition Technology in Commercial Applications*, 2018). To sum them up: Consent refers to individuals' express consent for enrolling in the system with some exceptions, such as the use of FRT for security purposes. Use-respect for context refers to the compatibility of the facial recognition template collection, use, and disclosure with individuals' privacy expectations for a particular context. Transparency refers to privacy statements giving a clear description of the purpose of facial recognition template collection, the boundary of facial recognition template use and disclosure, and archival rules for facial recognition templates.

Data security refers to the application of the optimum security technologies, regulations, and practices for facial recognition templates that are in a position to address security threats. Privacy by design refers to the embedding of technological controls into the system design, besides legal and administrative procedures, to boost or impose compliance with privacy principles. Integrity and access refer to the accuracy of the linkage of facial recognition templates to other personal information, such as name and an individual's ability to access personal profile for the purpose of facial recognition template review, correction, and deletion. Accountability refers to additional measures that need to be carried out to guarantee that organizations, third parties, and other partners do not employ FRT in ways that violate these principles.

It was observed that many systematic reviews of FRT (e.g., Bowyer, 2004) have indicated that the main challenge of FRT is organizational practices of information that against privacy principles and individuals' right to privacy. In his theoretical framework, *Social and Political Dimensions of Privacy*, Westin (2003) discussed the changes in the confidence ratio between individuals and organizations regarding privacy protection over different timeframes (1945–1960, 1961–1979, 1980–1989, 1990–2002). Although each period has a considerable alteration in individuals' privacy protection beliefs, the notable shift took place in the most recent era (1990–2002) because of the advancement in technologies post the September 11 terrorist attacks. An online poll, likewise, found that 70% of Americans feel personal information had been more secure five years ago (Auxier et al., 2019c). The reason for this consequence is quite not clear, but it very likely has something to do with Edward Snowden's serious leaks in 2014 about the National Security Agency project of creating a big database of images for FRT (Feeney, 2014).

Problem statement

Research problem

Prabhakar, Pankanti, and Jain (2003) suggested that the enactment of biometric privacy regulations plays a key role in overcoming biometric privacy principles-related violations, which should also cover privacy principles-related violations in the face recognition system (e.g., unauthorized information collocation, access, use, and disclosure). Over the last few decades, privacy safeguard has been a global priority and considered an individual's right that has been enshrined under constitutional laws in some nations (Solove, 2008). The total number of countries that have legislated privacy laws has been raised from 109 in 2015 to 120 in 2017, including countries located in Europe and the Middle East regions. There are also over other 25 countries located in various regions such as Africa and Latin America have officially proposed privacy legislation that needs to be passed by the legislature or executive (Greenleaf,

2017). This led the average annual growth rate of privacy laws, which stabilized at 2.9% since 1973, registering 134 states in 2019 (Greenleaf, 2019).

The growth of privacy laws, doubtless, reflects the importance of individuals' rights to privacy, especially in the age of information and communication technology, from authorities and lawmakers. Nevertheless, current privacy laws are, unfortunately, unprepared to overcome abusive practices within the technology industry (Zimmer, 2005), including facial recognition data-related misuse. This is due to the fact that the domain of FRT has suffered considerably from insufficient scholarly attention to rigorous assessment of the privacy measures to be employed as a basic guideline for lawmakers. Studies (e.g., Smith, 2019; Yang & Murgia, 2019) have statistically measured the volume of individuals' privacy concerns of FRT across various regions and contexts. But to the best of my knowledge, none of those or other relevant studies have attempted to investigate the root causes of privacy concerns to provide a thorough framework illustrating the dimensions of organizational practices of information that breach privacy principles and their impacts on control over personal information.

This doctoral dissertation filled this gap by diving into user-generated text on the YouTube platform applying mixed-methods content analysis to develop a new scheme of the most common FRT-related privacy concerns. In a general sense, social media networks have recently witnessed researchers' interest across different fields and become a suitable data source in view of the amount, boundary, and source of shared content. These platforms encompass billions of participants from all over the world with gender, age, cultural, religious, and cognitive differences that have offered a distinctive opportunity for researchers to explore the phenomenon among multiple groups instead of limiting themselves to a single community. But because of the uniqueness in the communication method (video-based communication) in YouTube, it has been the most second visited websites (“The top 500 sites on the web,” n.d.), and a target for 1.9 out of 3.8 billion social media users and 4.5 billion internet users (Kallas,

2020). Such a huge amount of YouTube user-generated text represented a valuable source for achieving the objective of this study.

Research questions and design

RQ1: What the most common FRT-related privacy concerns are raised by YouTube users?

RQ2: How do FRT-related privacy concerns reflect difficulties in the control over personal information?

YouTube users can express their attitudes toward FRT through posting videos, comments on FRT-related videos, or replies to other comments. User-generated text (video transcripts, comments, and replies) might hold negative, positive, neutral, or mixed perspectives that are influenced by many factors (e.g., personal experiences, the value of privacy, and the amount of knowledge of FRT). The retrieval of negative attitudes to get a better understanding of the phenomenon, the aim of this doctoral dissertation, was a bit complicated, with the absence of a scheme defining the dimensions of FRT-related privacy concerns. Therefore, there was a need to develop a novel methodological framework using the sequential exploratory mixed-method design to guide the user-generated text collection and analysis process to answer the research questions.

A taxonomy of privacy advanced by Solove (2006) was adopted in the user-generated text collection phase to make a decision of whether or not retrieved videos were fit for the research context (see Table 1 in the following chapter for more details about this taxonomy). Negative attitudes that existed in five out of 206 involved FRT-related videos were captured through the use of a privacy-related keywords list that was developed in the first phase of the methodological framework. The captured and relevant user-generated text was analyzed qualitatively to identify the most common FRT-related activities that caused the users' privacy concerns and impacted the users' control over personal information. Quantitative content analysis followed qualitative content analysis to generalize qualitative findings for the purpose

of external validity fulfillment by means of producing a multi-label classifier using a supervised machine learning model.

Significance of the study

It has previously been observed that conceptualizing privacy in an understandable and comprehensive pattern has become a significant challenge in view of the rapid changes in information technologies and social norms. Researchers over the past decades have provided a large body of systematic reviews and meta-analyses in an attempt to address this problem, but privacy theories that emerged from those frameworks were considered invalid, since they put privacy in too broad or too narrow theme (Solove, 2002). For example, some of the privacy theories limited the privacy boundary to activities that individuals privately practice such as intimacy. It is, therefore, needful to understand the common individuals' FRT-related privacy concerns to establish the theoretical basis of privacy in the context of information technologies, as Solove (2008) suggested that the privacy concept has to be constructed from a specific context (bottom-up approach).

It was showed early in this chapter that there has been a remarkable growth in enacting privacy legislation at the global level during the past 10 years (see Greenleaf, 2017, 2019). However, the majority, if not all, of existing privacy laws have not been legislated in a contextual paradigm. In simple words, those regulations have not taken into consideration all situations that are expected to violate the right to privacy in a particular context. Nissenbaum (2009) confirmed that privacy is a contextual factor not a generalizable factor due to the dissimilarity in information flow from a context to another, situations that might violate privacy in a context (e.g., smartphone) are not necessary to violate privacy in another context (e.g., social media). This study traces FRT-related privacy concerns aiming to raise policymakers' and marketers' awareness of this issue to enact or update privacy laws to be compatible with the age of FRT.

Recently, there has been renewed interest in investigating privacy concerns through the analysis of user-generated texts across social media platforms. Prior studies adopted different qualitative research methods to map privacy concerns surrounding various contexts. For instance, Shi, Xu, and Chen (2013) examined user-generated text on Facebook to identify users' privacy concerns about the Friendship Pages using a qualitative case study design. One of the greatest challenges of applying qualitative research design is the validation of research findings (Niaz, 2007) because of the sample size. For that reason, the dissertation represented a piece of significant evidence showing a way in which the findings of user-generated text on social media networks, particularly YouTube, could be generalizable by using one of supervised machine learning algorithms.

Outline of the dissertation

The doctoral dissertation is divided into four chapters: literature review (chapter 2), methodology (chapter 3), results (chapter 4), and discussion (chapter 5). Chapter 2 presents an overview of the most relevant literature about the conceptualization of privacy, FRT-related privacy concerns, measurement models of privacy concerns, and YouTube data collection and analysis mechanisms. Chapter 3 describes the methodology used for the privacy-related keywords list development and the YouTube data collection and analysis process along with a discussion of the findings of the privacy-related keywords list. Chapter 4 presents the qualitative and quantitative findings of FRT-related privacy concerns. Chapter 5 discusses the results chapter in light of previous theories, research implications, research limitations, and future research recommendations.

Chapter 2: Literature Review

The conceptualization of privacy

Privacy is sacrosanct in many civilized societies and has become one of the pressing issues in light of technical progress that has been witnessed by human beings for past decades. Clarke (1999, p.60) argued that "privacy is often thought of as a moral right or a legal right." The author, furthermore, identified four sorts of privacy: privacy of the person, privacy of personal behavior, privacy of personal communications, and privacy of personal data. Privacy of the person refers to the protection from interventions in personal decisions about one's body (e.g., mandatory immunization). Privacy of personal behavior refers to the protection from personal behavior control (e.g., forcing an individual to follow uncomfortable social habits). Privacy of personal communications refers to the protection from personal communications surveillance (e.g., monitoring social media threads). Privacy of personal data refers to the protection from the misuse of available Personally Identifiable Information (PII) (e.g., unauthorized collection and linkage of social media photos to personal profiles for identification).

It is significantly noticed that challenges related to privacy of personal data have received more attention than other sorts of privacy among privacy advocates and consumers, particularly in the age of information technologies. PII was interpreted as any information that has the capability to describe an individual's identity to distinguish between groups of people in a community, consisting of personal attributes (e.g., gender) biometrics (e.g., faceprints), and identifiers information (e.g., social security number) (Zimmer, 2018). The majority of PII has been generated and flowed in an electronic approach (Gladney, 2006) since the emergence of information technologies and the online environment in the early 1990s that resulted in an actual crisis in privacy protection. Byford (1998, p.1) stated that "At no time have privacy issues taken on greater significance than in recent years, as technological developments have

led to the emergence of an “information society” capable of gathering, storing, and disseminating increasing amounts of data about individual citizens."

Several lines of research have proposed different theoretical frameworks during the last decades in an attempt to provide an obvious conceptualization of privacy. Privacy as the right to be let alone theory, which appeared in the widely-cited article *The Right to Privacy* (Warren & Brandeis, 1890), shaped the philosophical ground of the privacy concept in a legal context. As a response to the failure of privacy law to overcome the advent of information technologies, Warren and Brandeis, American attorneys, introduced their theoretical framework by emphasizing that "the individual shall have full protection in person and in property" (p.193). They illustrated how privacy implications of any shifts in political, social, economic, and technological trends might be faced through enacting or reframing existing privacy regulation as an efficient strategy to maintain the right to privacy. For example, their paper voiced concern about the impact of instantaneous photographs on privacy back then and showed how reforming some simple flaws in current privacy laws could reimpose their ability to confront those threats.

The right to be let alone theory immediately received corroboration in the past and present literature at a broad scale, yet other scientific papers (e.g., Allen, 1988; Freund, 2017; Gavison, 1980; Schoeman, 1984) assured that there has not been a consensus among researchers to approach privacy as the right to be let alone neither in a traditional nor digital age. Allen (1988) claimed that if our insight into privacy is limited to such proposed theory, all our daily activities should thus lead to breaching the others' right to privacy, because the nature of the right to be let alone theory encourages seclusion (Solove, 2002), being isolated from the community. By way of illustration, taking a personal photo as a part of The Division of Motor Vehicles (DMV) requirements for driver's license issuance could be considered a form of privacy invasion.

A group of privacy scholars who have mainly been interested in bridging the shortcoming of the right to be let alone theory conceptualized privacy as limited access to self, including limited access to physical, information, and attention (Bok, 1989). The starting point of privacy as limited access to self was launched by Godkin (1880), reminding us that "nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself" (p.736). Gavison (1980), by the same token, tied privacy protection with "the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention" (p.423). Put differently, the authors and those who believe privacy as limited access suggested that the fulfillment of privacy protection requires inaccessibility to a person.

Solove (2002) recognized that privacy as limited access to self was not able to refine or advance the privacy notion developed by Warren and Brandeis (1890) owing to the fact that privacy in such framework was reconceptualized in an analogous and more complex paradigm. Privacy as limited access to self, without a doubt, address the broad visibility of privacy as personal isolation but still tended to restrict the circle of privacy protection into a personal desire for the concealment of private affairs, such as secret behaviors (e.g., Warren & Laslett, 1977), and secret information (Thompson, 2001). In addition to that, with no elucidation of what events are considered private, the right to privacy, in this case, can be simply violated during daily activities. For a social media user, for instance, who shared a photo on the network while at home, any social interaction with this user or posted photo might be interpreted as a privacy invasion.

In this context, Zimmer (2007) shed a light on the importance of not limiting the span of privacy to practices and actions that we have carried out secretly. Instead, our idea and expectation of privacy should be extended to center on private information protection regardless of whether this information has been generated in a public or private space.

Nissenbaum (1998), who labeled this case as the problem of privacy in public, suggested that theories that relied on control over an access framework have conceptualized privacy in unavailable conditions in the age of information technologies. Recent information technologies (e.g., surveillance) are powerful enough to identify, collect, store, and analyze individual-generated information in public that would invade the values of privacy (e.g., autonomy, freedom, and anonymity) that individuals always seek for in their private place. Walkers, for example, could lose their right to anonymity once they pass by a public street with facial identification sensors.

For that reason, many recent studies have theorized privacy as control over personal information to face the problem of privacy in public. In his discussion, Westin (1967) affirmed that privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (p.7). Fried (1968) also supported this notion and highlighted that "privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves" (p.482). Both writers found that privacy is a sort of reserve (personal desire to reveal information about themselves) and anonymity (unrecognized identity in public) other than solitude (being alone) or intimacy (being alone with a small number of individuals) as formulated in the right to be let alone and limited access to self.

The framework of control over personal information perhaps handled the issue of privacy in public, but the master disagreement point among scholars is that such an approach, in essence, considered that the right to privacy ends once self-disclosure of PII has occurred. McCroskey and Richmond (1977) offered an elucidation of the core idea of self-disclosure of PII that includes intentionally or unintentionally releasing any PII to others, across an online or offline environment. The deprivation of the right to privacy due to self-disclosure of PII has become a phenomenon in the industry since organizations, unfortunately, have adopted this

principle to treat privacy as a commodity, not as a right or social norm. Individuals are supposed to perform a cost-benefit analysis to evaluate the potential risks and benefit consequences of disclosing PII, which is also known as the privacy calculus theory (Laufer & Wolfe, 1977; Milne & Gordon, 1993). In this way, those who willingly or forcibly choose to take a risk and reveal PII in order to get served would be out of the scope of privacy protection.

Solove's (2008), who is well-known for his support to approach privacy as a multi-dimensional factor, concluded that the conceptualization of privacy in a single dimension has never been an appropriate manner to paint a thorough description of privacy. The traditional theories on privacy, the aforementioned privacy theories, have been developed through an excessive angle that drove to provide a narrow or broad image of the privacy scope (Solove, 2002). Some of these theories "fail to include the aspects of life that we typically view as private" (Solove, 2002, p.1094), such as the problem of identification and surveillance in public. Other privacy theories "fail to exclude matters that we do not deem private" (Solove, 2002, p.1094), such as the daily interaction between individuals that the right to be alone theory consider a privacy breach.

Past studies believed that the central factor that caused the current ambiguity of privacy concept and boundaries is the overlap between privacy and other relevant terminologies. BeVier (1995) demonstrated that "privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests" (p.458). In other words, privacy is an all-embracing term used to indicate other values such as confidentiality and anonymity. This statement has pushed Solove (2006) to advance a taxonomy of privacy, known in the literature as Solove's taxonomy, to map the fine lines that link those terms with each other based on capturing common activities against social norms. It is also worth noting that the purpose of Solove's taxonomy was to not just define privacy but to give assistance to policymakers who are interested in creating a balance between privacy and other relevant interests.

Table 1 presents an overview of Solove's taxonomy that consist of 16 elements divided into four main categories: information collection (surveillance, interrogation), information processing (aggregation, identification, insecurity, secondary use, exclusion), information dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion), and invasions (intrusion, decisional interference). Information collection refers to activities related to gathering information about individuals in public and private spaces with or without informed consent (e.g., tracking social media users' daily activities). Information processing refers to activities related to processing the collected information in ways that are not compatible with social, legal, technical norms (e.g., using gathered photos for purposes that are out of agreement context). Information dissemination refers to activities related to the increased accessibility of information (e.g., sharing PII with third parties). Invasions refer to activities related to the intervention into individuals' isolation (e.g., the appearance of pop-up advertisements on the phone screen to change personal choices).

Table 1. The description of Solove' taxonomy

Category	Subcategory	Description
Information collection	Surveillance	It refers to the process of gathering information about individuals in public and private spaces without their knowledge and consent.
	Interrogation	It refers to the process of forcing individuals to disclose information that preferred to be private.
Information processing	Aggregation	It refers to the process of creating personal profiles by combining information about individuals gathered from several sources.
	Identification	It refers to the process of linking personal profiles that contain aggregate information about individuals to personal identity.
	Insecurity	It refers to the process of not providing an appropriate mechanism to prevent unauthorized access to personal records.
	Secondary use	It refers to the process of using the gathered information for purposes that are out of agreement context.
	Exclusion	It refers to the process of excluding individuals from being involved in the decision-making process about information collection, use, storage, and disclosure.
Information dissemination	Breach of confidentiality	It refers to the process of breaching the promise of maintaining the confidentiality of information leading to destroy the trust between organizations and individuals.
	Disclosure	It refers to the process of disclosing information about individuals leading to change others' judgment of individuals.
	Exposure	It refers to the process of exposing private, sensitive, and embarrassing information about individuals that should not be shared with other parties.
	Increased accessibility	It refers to the process of expanding the access scope of databases that consist of information about individuals.
	Blackmail	It refers to the process of threatening individuals to reveal their private information if the blackmailers have not got their demands.
	Appropriation	It refers to the process of taking advantage of information about individuals to serve the objectives of organizations and other parties.
	Distortion	It refers to the process of disseminating false information about individuals.
Invasions	Intrusion	It refers to the process of intruding into individuals' private lives and interrupt their daily activities.

Decisional interference	It refers to the process of interfering in personal decision-making.

While Solove's taxonomy has been widely adopted among researchers to serve as the theoretical framework (e.g., Alsulaiman & Alrodhan, 2014; De Assis Rodrigues & Sant'Ana, 2016), the work that was undertaken by Massey and Antón (2008) showed that Solove's taxonomy is too broad to conceptualize privacy or assess the state of privacy. There is a high chance that Solove's taxonomy fails to include all organizational practices of information that violate privacy in a specific context by virtue of the variation in information flow from a context to another (e.g., FRT, internet of things, and blockchain). Solove (2007), in any case, seems to be aware of this limitation, which motivated him to confess that his taxonomy might not be quite comprehensive enough, but it is considered a project that would keep being revised and ameliorated with the emergence of new privacy issues. Consequently, this dissertation endeavors to use Solove's taxonomy as an initial theoretical framework and modify it to be in harmony with the context of FRT based on the analysis of FRT-related privacy concerns among YouTube users.

A trade-off between public security and privacy interest

Information explosion

The world has lately witnessed unprecedented inflation of data growth, specifically with the explosion in communication channels' development and Internet use. In a statistical report of online users, it was predicted that the Internet population would arrive at no less than seven and half billion active users by 2030, which represented approximately 90% of the world's population at that time (Calif, 2019)—8.5 billion people ("UN projects world population to reach 8.5 billion by 2030, driven by growth in developing countries," 2015). Those alone could contribute to producing 44 zettabytes of data (44 trillion gigabytes) by 2020,

promising that the annual growth of data traffic ratio is in its path to score up to 40% ("Executive Summary: Data Growth, Business Opportunities, and the IT Imperatives | The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," 2014).

The founder of Kodak, George Eastman (1888), coined a popular advertising slogan, "You press the button, we do the rest" (Munir, 2005), as a signal of the high value of individual-generated information. The gathering and storage of individual-generated information, which includes biometric information, has been a reality that cannot be denied. Davis (1997) suggested that personal body parts and biological traits shared across different settings have been already mapped and digitized, in government databases (e.g., driver's license photos) or commercial databases (e.g., social media photos). The Center on Privacy & Technology at Georgetown Law, at the same time, reported that there is a good enough chance, almost 50%, of the presence of American adults' photos in government agencies' and their allies' databases ("The Perpetual Line Up - Unregulated Police Face Recognition in America," 2016).

The wide availability of facial features has definitely influenced the investment volume of FRT in the market, which would continue growing to 17.2% within five years beginning in 2020 ("Facial Recognition Market Size, Share and Global Market Forecast to 2025 ," n.d.), for public security reinforcement. However, many studies and systematic reviews of sociotechnology (e.g., Nissenbaum, 1998; H. J. Smith, Milberg, & Burke, 1996; Turner & Dasgupta, 2006; Westin, 2003) have detected that there is a significant relationship between the application of information-based technologies and individuals' concerns for the circle of privacy protection. An online poll was internationally carried out among 10,000 participants recruited from nine countries (e.g., Brazil and the United States) to examine the previous hypothesis. The findings plainly indicated that the majority (over 70%) of participants have

expressed their uncomfortable feelings and privacy concerns about how organizations manage their information (Bacchi, 2019).

It has been well established in the literature that the source of individuals' privacy concerns usually lies in a difficulty in getting a sense of the limits of organizational practices of information (information collection, use, and sharing) because of complex privacy agreements. In the analysis of 4,048 participants' attitudes toward online companies' privacy policies, Wronski (2019) concluded that 87% believe that the clarity of privacy policies shapes a significant element in their decision-making process. Auxier et al. (2019b) additionally found that the larger part of those who are always willing to read privacy policies struggle to comprehend the entire content. That has inspired some investigators (e.g., Sadeh et al., 2013) in the field of artificial intelligence to apply multiple machine learning algorithms to privacy policies in order to summarize and interpret their main themes in a more simple pattern for the public.

The key point to bear in mind is that the absence of transparency in privacy agreements is not a matter motivating individuals to withdraw from that agreement. The same statement reported by Wronski (2019) shed a light on the desire of 53% out of participants who took the clarity into consideration intended to accept privacy policies without reading their content. Much of the previous research (e.g., Walsh, Parisi, & Passerini, 2017) named this phenomenon as the economies of privacy, explained earlier, that an individual's privacy is given up in exchange for some rewards (e.g., purchase discounts and free services). The adoption of this behavior is generally dependent on an individual's consciousness about degree of the value of privacy, which is undoubtedly influenced by different factors including gender (e.g., Hoy & Milne, 2010; Youn & Hall, 2008), age (e.g., Kezer, Sevi, Cemalcilar, & Baruh, 2016; Van den Broeck, Poels, & Walrave, 2015), and cultural values (Bellman, Johnson, Kobrin, & Lohse, 2004; Harris, Van Hoye, & Lievens, 2003).

Unfortunately, the thing that makes the phenomenon more complicated is that the belief in privacy as a commodity at the individual level is not an issue belonging to its believers alone but encompasses their peers in the community. Kelman's (1958) Social Influence Theory (SIT) illustrated the magnitude of the catastrophe that the majority's attitudes cause over the minority's attitudes in one community. The minority's thoughts, beliefs, behaviors, etc., are always subject to alteration in order to make one able to engage in the community. Plenty of frameworks relied on SIT have evidenced that self-disclosure of PII in the information age has been completed under social pressure instead of personal desire. Kroschke and Steiner (2017), as a recent model of these frameworks, identified that the high adoption of apps among individuals has created tremendous pressure on their peers in connection with self-disclosure of PII.

However, it is worth noting that the social influence phenomenon often has nothing to do with the individuals' acceptance of non-transparent privacy agreements, self-disclosure of PII, or other relevant activities. Privacy has been turned into a dependent source controlled by the rapid changes in political and economic trends. It has been observed that numerous organizations have lately adopted repressive policies that link individuals' entitlement to basic life needs with the extent to which they follow certain behaviors. For instance, Chinese citizens have become required to verify personal identity through employing face characteristics along with other instruments in order to receive telecommunication services (Goh, 2019). On the other hand, other organizations have preferred to use soft power through minimizing some privileges for those who do not accept privacy agreements that would create discrimination between individuals. WhatsApp, owned by Facebook, for example, keeps the full functionality of WhatsApp unavailable for those who do not agree to the updated privacy policies (“What happens on the effective date?,” n.d.).

Mass surveillance

To gain more insight into privacy implications of information explosion, we should go back to Mason's (1986) paper, *Four Ethical Issues of the Information Age*. The author forewarned the exploitation of information technologies and obtained data for surveillance systems reinforcement; surveillance is also named dataveillance to refer to data that has been gathered in a digital form (see e.g., Clarke, 1993). Face recognition surveillance technology, one of the central aspects that have assisted to expand the application of FRT ("Facial Recognition Market Size, Share and Global Market Forecast to 2025 ," n.d.), represents an example of surveillance systems reinforcement that does not correspond with individuals' expectations of privacy. Organizations have obliterated the individual's right to anonymity by integrating FRT into traditional surveillance systems to enable them to recognize one's identity through personal photos that have been already stored in databases. A new document, for example, affirms that a variety of U.S agencies have employed driver's license photos stored in DMV databases for facial scanning (Harwell, 2019).

Relevant studies often end up with the similar conclusion that the use of collected personal photos for identification and surveillance in secrecy without informed consent is the essential root for the rejection of face recognition surveillance technology. As a result of a collaborative project between the Chinese police and an FRT company (SenseNets), a huge amount of citizens' location data was gathered within just a day and exploited to track upward of two and a half million people, who settled in the north-west part of Xinjiang, through matching their locations with PII including personal photos (Yang & Murgia, 2019). While it remains unclear if such an action was performed with or without informed consent, 53% of online poll respondents failed to understand how FRT in a real-time application could seek their permission for identification (O'Donnell, 2019). This concern led the big mass of 6,152

participants to heavily demand and wish to get back to conventional identification systems to avoid information abuse (Yang & Liu, 2019).

Nevertheless, several lines of evidence signify that the deployment of face recognition surveillance technology has become a global trend to enforce public security. Based on a recent statement that released by industry researcher IHS Markit, the worldwide installation rate of face recognition surveillance technology would likely grow 30% in 2021, from 700 million to over a billion (Nash, 2020). China was forecasted to represent the master player in this market, in excess of 50% of the total adoption rate (Lin & Purnell, 2019). That does not imply that liberal states (e.g., America and Canada) have an intention to not follow this direction; rather they have been one of the biggest rivals in the past few years. Pew Research Center, by way of illustration, revealed that it is impossible for roughly 60% of Americans "to go through daily life without having data collected about them by companies or the government" (Auxier et al., 2019c).

Social control

Organizations have strived for a long time to convince individuals to view privacy as having limited access, explained earlier, by limiting privacy regulations to activities in private space (e.g., the unreasonable expectation of privacy in public space in the Fourth Amendment to the United States Constitution) and encouraging the community to give up privacy in exchange for public security. The systematic review of the problem of surveillance in public that was developed by Solove (2007) provides multiple examples of agents who have attempted to publicize different slogans (e.g., I've got nothing to hide) to normalize extensive surveillance in public. Those slogans suggest that individuals are expected to be involved in public space with prior knowledge of the existence of surveillance systems for community security unless there are some illegal activities that individuals have engaged in and aim to hide. Schneier (2006) believed that I've got nothing to hide and similar arguments shape "the most common

retort against privacy advocates" to make privacy claim about surveillance in public unjustified.

It has been seen that the global orientation to support surveillance systems, particularly public surveillance, is related to the enhancement in social control level not public security level (Norris, 1997; Véliz, 2020). This view has been supported by Manders-Huits and Zimmer (2009) and Nissenbaum (2009) who indicated that the information explosion has paid extremely close attention to stakeholders as a consequence of its effectiveness on the decision-making process. People from all walks of life have become prone to surveillance operations (Nissenbaum, 1999; Zimmer, 2005), to get profiled (Clarke, 1993), also known as searchable databases (Lyon, 2005) or profiling mechanisms. The purpose of a profiling application is to link facial features to every single individual-generated information, from surfing the Internet to walking on the street, in an attempt to find new patterns about a target group, like criminal profiling that has been implemented to analyze aggregate information about someone's behaviors to predict the chance of committing a crime.

Privacy advocates, on this basis, have expressed their concerns about using public security as an excuse to increase the profiling enforcement that ought to steer personal behaviors. Kostka and Antoine (2019) investigated the extent of changes in Chinese citizens' behaviors that resulted from the enforcement of social credit systems, one of the profiling paradigms measuring the trustworthiness of individuals and entities via the continuous surveillance and analysis of their daily activities. A high percentage of surveyed and interviewed participants articulated that at least one time in their lives they have had to alter some behaviors. This behavioral change may be explained by the fact that individuals have become more aware that collected information is not always processed in ways that are compatible with personal interests (e.g., exposing information about sensitive activities to public networks in an effort to destroy personal reputation). For that reason, they are eager to

act contrary to their reality to minimize the chance of granting organizations any power over them.

Regardless that the adoption of profiling has been expected to improve the social accountability process for illegal activities (e.g., thefts, high-speed driving, and murders), the loss of the individuals' right to anonymity is problematic for the human right to equality and nondiscrimination that would open a back door for invasions of personal isolation. In recent years, there has been an increasing amount of literature on the ethics of face recognition algorithms to evaluate the discrimination rate between individuals. The majority of this literature has recognized that the mining of collected data is often directed by biased algorithms, called racial profiling (see Alschuler, 2002). Bacchini and Lorusso (2019) claimed that this system has contributed to enhancing racial prejudices because some groups are more subject to police stopping, searching, and seizure than others. In simple words, face recognition algorithms tend to classify individuals based on ethnicity instead of personal behaviors; for example, face recognition algorithms could categorize black women with positive behaviors to a suspicious group and white men with negative behaviors to a nonsuspicious group.

For-profit organizations are not excepted when it comes to invasion of privacy through the establishment of detailed profiles (e.g., interrupting personal isolation by pop-up advertisements to manipulate personal attention and choices). The 2018 survey carried out by NewVantage Partners among senior executives who were recruited from over 50 large businesses concluded that the investment of artificial intelligence and big data analytics (BDA) has turned into the target of 97% of firms (Davenport & Bean, 2018). This is due to the fact that BDA offers a pioneer opportunity for the market to boost its annual revenue, reaching up to $103 billion by 2027 (Kobielus, 2018). The investment of such a project perhaps requires data investors to expand the loop of information access, such as the Facebook–Cambridge Analytica data scandal when over 45 million profiles were accessed and analyzed without

informed knowledge (Cadwalladr & Graham-Harrison, 2018). Thus individuals in the U.S. have relatively a higher trust in government organizations to implement FRT for surveillance than nongovernment organizations (Smith, 2019).

Security vulnerability

The hearing of the senate judiciary committee Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism took place on Capitol Hill, Washington, November 14, 2001, to debate the security failure in confronting the 9/11 attacks. In the opening remarks, senator Dianne Feinstein, Democrat of California, started her discussion by asking, "How could a large group of coordinated terrorists operate for more than a year in the United States without being detected and then get on four different airliners in a single morning without being stopped?" Her brief answer alluded to the absence of FRT to recognize the hijackers' actual identities, which allowed hijackers to freely fake their identifications ("Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism. Congressional Hearing, 2001-11-14, 2001-11-14, 2001-11-14," 2001).

John Adam, the 2nd president of the United States, used to say that "Facts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passions, they cannot alter the state of facts and evidence" ("Adams' Argument for the Defense: 3–4 December 1770," n.d.). FRT is still too far away from achieving such a mission with the problem of inaccurate identification. In the Privacy Impact Assessment (PIA) report of the FBI's biometric identity system, it was acknowledged that FRT "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an unacceptable percentage of misidentifications." (Prest, 2019, p. 15). This means that FRT could identify an individual as another person on account of the high rate of the positive false match during the scanning

process. As a case in point, 81% of those who have been classified by FRT as suspects and arrested by law enforcement agencies in the United Kingdom were innocent (D. Davis, 2019).

In general, the positive false match is not a new problem but has been detected since 1903 when the Bertillon identification system was unable to distinguish between twin brothers Will West and William West, who were both incarcerated at the Leavenworth Penitentiary (Chalakoski, 2017). Scientists in the field of computer vision algorithms have determined the main two sources that result in misidentification: zero-effort attacks and adversarial attacks. Jain, Ross, Pankanti, and Member (2006) defined zero-effort attacks as attacks that occur if FRT faces difficulty in distinguishing between two similar face templates, like similarity in physiological characteristics (e.g., twin brothers). The zero-effort attacks sometimes emerge from an ethical issue (e.g., training the system based on ethnicity, gender, and class) (see e.g., Buolamwini & Gebru, 2018). In contrast to the zero-effort attacks, adversarial attacks are caused by hackers who use their skills to imitate a victim's face to fool the system with cheap materials, known as spoofing attack (e.g., generating 3D mask of the genuine face).

It is important to underline that the negligence of addressing the positive false match is possible to place privacy at infringement risks. Information security plays a key role in privacy protection through the implementation of necessary technologies and strategies to eliminate unauthorized access to personal records. But the failure of obtaining an adequate security level with the availability of the zero-effort attacks and the adversarial attacks would definitely raise identity theft processes. According to fraud and ID theft map that was published by Federal Trade Commission (2021), there were 1,387,614 identity theft cases reported in 2020, increasing approximately 53% (650,523) over the number of cases reported in 2019, 68% (444,344) in 2018, 73% (370,916) in 2017, and 71% (398,356) in 2016. The rapid growth of identity theft percentage from one year to another has had a negative impact on control over

personal information (e.g., creating 3D masks of famous people to gain access to their sensitive records for the purpose of blackmail or disclosure).

Examining personal attitude toward FRT

Personal attitude

Even though the information technology life cycle is fed by continuous improvement and inventions, the success or failure of those outputs primarily relies on personal attitudes. In the early 20th century, Eagly and Chaiken (1993) came up with an abstract definition of personal attitude by stating that it is about a person's expression and assessment of the material, person, place, and other events that arise from the emotional and mental entity. Investigators have unanimous agreement that the concept of personal attitude initially came into view in Jung's (1923) printed work, *Psychological types or the psychology of individuation*, seeking to provide an abbreviated term for one's tendency toward a thing. Individuals who hold positive attitudes toward a certain technology are more likely to have positive decisions than others who hold opposite attitudes.

Our attitude is developed based on three components: affection, behavior, and cognition (ABC model) (Fazio, 1986). Cognition is a component related to personal beliefs, thoughts, and knowledge about an object, that is affected by sundry factors, including personal traits (e.g., values), social traits (e.g., culture), and sociohistorical traits (e.g., economy) (Albarracin & Shavitt, 2018). Affection is a component related to personal emotions about an object that is motivated by cognition. A person could hold positive, negative, or mixed feelings. Behavior is a component related to actions that an individual would take based on affection. An example of those components is the Internet users whose attitudes have been impacted by knowledge or experience of cyberbullying. They feel the anxiety about being involved in social media networks (affection) because of the high chance of getting cyberbullying (cognition), so they prefer to not join social media networks (behavioral intention) to avoid cyberbullying.

The ABC model, of course, gives assistance to researchers who are interested in human-computer interaction (HCI) and other technology-related subjects like health, finance, and education to inspect and perceive personal beliefs, emotions, and decisions about technology stacks in dissimilar templates. Based on reviewing several studies that adopted the ABC model, it was noticeable that the variation from one study to another regarding the hierarchy of those elements is considered a natural phenomenon since the order is controlled by the purpose and conceptual framework of the project. For example, some examiners in the realm of virtual learning systems employ cognition, behavior, and affect layout to analyze students' affection after being involved in in electronic learning, while others apply cognition, affect, and behavior configuration to get a better understanding of students' beliefs and feelings about virtual learning systems to predict whether or not those students intend to choose online education over traditional learning systems.

Privacy-related decision-making

In the literature of decision-making processes, scientists in the information system area have been interested in mapping common grounds of users' decisions in regard to the use of technology products by applying different personal attitude models, like the Technology Acceptance Model (TAM) developed by Davis, Bagozzi, and Warshaw (1989) based on the theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980). A group of those examiners were data privacy proponents (e.g., Kim, Ferrin, & Rao, 2008; Lee & Rao, 2007; Ortiz, Chih, & Tsai, 2018) who found a piece of evidence that privacy belief constitutes an influential factor on a person's behavioral intention to use systems that require self-disclosure of PII in advance. Privacy belief can be either privacy protection belief or privacy risk belief (Li, Sarathy, & Xu, 2011), which is impacted by the extent of privacy protection provided by systems developers and operators.

With the enormous power of storing, accessing, and sharing a vast amount of PII in the digital age, the relationship between individuals and organizations has become controlled by the trust principle. In reality, individuals predominantly sense privacy concerns and tend to stay far away from some advanced technologies, especially multifunctional systems (e.g., smartphone), if there is a chance of handling their information in approaches that are out of legal and social norms. On the other hand, processing PII within the expectation of privacy creates privacy protection belief more than privacy risk belief that guides one to adopt technology materials. For example, Apple's decent privacy practices raised consumers' trust more than other companies, Facebook and Google among them (Tripathi, 2018). But it should be recalled that privacy risk belief may be increased as much as information sensitivity regardless of the organization's reputation.

Prior investigations, in line with Solove's (2006) discussion of privacy as a multidimensional factor, have hinted that the gauge of privacy risk belief of organizational practices of information seems an intricate mission with the absence of a multidimensional model. Smith et al. (1996) supported this notion by systematically positing the earliest privacy model to measure the common individuals' Concern for Information Privacy (CFIP) that was associated with organizational practices of information based on four dimensions and a 15-item instrument: collection (e.g., too much information collection), unauthorized secondary use (e.g., selling PII), improper access (e.g., accessing PII by unpermitted employee), and errors (e.g., inaccurate information entry). This model was essentially designed to capture the size of individuals' privacy concerns among those dimensions as the result of the inability to have control over PII. However, the authors realized that "this dimensionality is neither absolute nor static, since perceptions of advocates, consumers, and scholars could shift over time" (p. 190).

Although the validity of the CFIP instrument was repeatedly examined and applied to several samples, times, and settings, in their empirical study, *An Empirical Examination of the*

Concern for Information Privacy Instrument, Stewart and Segars (2002) indicated that such a scale would perhaps fail to conclude privacy concerns in an accurate portrait. The writers, then, proposed that the CFIP model could be valid if an investigator employed it as second order not as first order to demonstrate the interdependencies between subitems in each dimension as well as the main four dimensions. This suggestion has inspired a number of privacy researchers to adopt the CFIP model (e.g., Korzaan, Brooks, & Greer, 2009; Slyke, Shim, Johnson, & Jiang, 2006) or modify its dimensions (e.g., Malhotra, Kim, & Agarwal, 2004) in order to evaluate privacy trust, concerns, and behavior intention statistical method.

Privacy paradox

The unfortunate thing is that the CFIP model, or similar frameworks that assess privacy as self-disclosure of PII, always paint a misleading picture of the state of privacy. Their conclusion claims that the privacy paradox is still a common and obvious phenomenon among individuals. Drawing on the work of Dinev (2014) and Norberg, Horne, and Horne (2007), the privacy paradox term refers to the dissimilarity between an individual's privacy belief and an individual's behavioral intention. People sometimes express their privacy risk belief about PII-based technologies, but in the meantime, they fail to take action to address those concerns. For example, a survey showed that only in the region of 50% of participants who have the privacy risk belief about sharing PII across online sites have planned to use another phone number to safeguard their privacy zone. ("The Privacy Paradox lives on according to new survey ," 2018).

There has been a consensus among the modern philosophers of privacy (e.g., Solove, 2020) that the ground for the privacy paradox theory has been built by erroneous logic and does not have the capability, under any circumstances, to draw a valid conclusion about whether or not a person values privacy, since there is no a connection between the value of privacy and the self-disclosure of PII. The nature of life in the information age often requires individuals to share PII with some groups of people and organizations for a wide array of purposes (e.g.,

revealing personal photo to get employee ID issued). Those people, in this case, still value privacy even if they do not hold privacy risk beliefs about the self-disclosure of PII. They are more concerned about the information flow, as Nissenbaum (2004, 2009) formulated the contextual information flows theory to highlight the importance of understanding the expectation of privacy within a specific context.

In her book *Privacy in context: technology, policy, and the integrity of social life* Nissenbaum (2009) suggested that privacy violation is scaled based on social or legal privacy norms of information exchange. Contextual Integrity (CI) theory aims to identify five parameters to evaluate the state of privacy. The first three parameters are related to actors (a data subject, sender, and recipient). The fourth parameter is related to attributes (what type of information). The final parameter is related to transmission principles (the boundary of information flow permitted by a data subject). Any deviation that occurs in those parameters means a breach in privacy norms. For instance, an employee (data subject, sender) shares a personal photo (attributes) with an employer (recipient) to issue ID (transmission principles), but it is not expected to employ this data for FRT (privacy norm violation).

CI theory has been applied in different contexts, like vehicle communication (Zimmer, 2005), search engine (Zimmer, 2008), social network sites (Shi, Xu, & Chen, 2013), big data research ethics (Zimmer, 2018), Internet of Things (Apthorpe, Shvartzshnaider, Mathur, Reisman, & Feamster, 2018), and privacy policy analysis (Shvartzshnaider, Apthorpe, Feamster, & Nissenbaum, 2019). The privacy evaluation process in those studies goes beyond the behavioral intention of self-disclosure of PII by offering an explanation of particular contexts where information flow has not been compatible with the individuals' expectation of privacy. While the application of the complete CI framework (the five parameters) to unstructured data (e.g., user-generated text on YouTube in this study) is perhaps a complex function, CI theory helps researchers to evaluate the state of privacy based on identifying

organizational practices of information that violate transmission principles in a systematic method by tracking the deviation of information flow.

Content-based analysis applied on YouTube research

User-generated content on Web 2.0

Daugherty, Eastin, and Bright (2008) described user-generated content as "media content created or produced by the general public rather than by paid professionals and primarily distributed on the Internet" (p.16). The convenient environment provided by the Internet has heavily contributed to moving user-generated content, including but not limited to, news, advertising, and research, from traditional media hierarchies to user-generated sites. In the decade of Web 1.0 (read-only web), user-generated content has been only individually produced and streamed that other nodes in the same network are unallowed to be engaged in (e.g., faculty and staff directory pages). Such a norm was short-lived and has been replaced since the emergence of Web 2.0 channels (read-write web) in late 2004 that occurred a monumental leap in the communication world. The source of user-generated content in Web 2.0 Internet-based applications has not become exclusive to webpages owners. Rather, everyone has a chance to collaboratively participate in discussion threads through sharing personal attitudes across user-generated sites (e.g., forums sites).

User-generated content is not a modern concept, but the sharp growth of data traffic generated by online users, as discussed in the second section of this chapter, has prompted scientists to investigate the difference between online and offline individual-generated content. It was highlighted in the majority of the literature (e.g., Hollenbaugh & Everett, 2013; Joinson, 2001) that the degree of obtaining anonymity through multiuser communication online has affected individuals' desire to withdraw from real-life conversation. Online users who are unknown to their offline community feel much more comfortable about and agreeable to expressing their attitudes and sharing some information about them without facing any social

accountability or legal sanctions. For example, bloggers who are infected with Human Immunodeficiency Virus (HIV) might admit this and narrate their stories under a pseudonym, but in the meantime, they are embarrassed to do that in face-to-face communication because of the discrimination in some countries, cultures, and religions.

Social media networks

In the context of user-generated content, social networks forums (e.g., Facebook, Twitter, and YouTube) represent the most popular form of user-generated sites that allow their users to establish diverse content, from a simple text to advanced multimedia, to interact with other peers. The global digital 2021 report released in January 2021 revealed that the total number of social media users is 4.20 billion, which is equivalent to approximately 91% of the Internet population (4.66 billion) and 50% of the world population. The growth percentage of new social media users within just a year (2020 – 2021) is over 10% (Kemp, 2021). YouTube (1.9 billion users) and Facebook (2.23 billion users) are considered the main users' destination compared to other interactive platforms (Kallas, 2020), like Twitter, WhatsApp, and Snapchat.

YouTube, however, offers a unique landscape that has been designed to concentrate on video-based communication as an alternative choice to the text-based communication found in other social networks. Video-based communication is a vital solution for many individuals (e.g., paralyzed, blind, and busy people) who have faced difficulty in text-based communication engagement. This uniqueness drove YouTube to be ranked as the second top-visited website following Google ("The top 500 sites on the web," n.d.). As a user-friendly interface that developed in 2005, the majority of individuals and organizations have joined YouTube and participated in the process of the digital content industry via a wide array of techniques including creating, watching, and responding to videos. Those activities have got researchers' attention and made YouTube a suitable information warehouse to explore interesting topics at different levels.

Numerous investigators in recent decades have relied on gathering user-generated content to understand social phenomena in a pure image. Some groups prefer to get user-generated content from a publicly available dataset, such as the Kaggle dataset, that has been collected and uploaded by other researchers. This dataset might contain redundant and useless data variables for some projects like identifiable data (e.g., username) and metadata (e.g., video title). Other studies that have specific selection criteria usually apply different technical instruments to complete the data collection process. The choice of those instruments is determined by investigators' preferences, time, technical skills, and other factors. Data collection through Application Programming Interface (API), for example, requires programming skills while software (e.g., WordStat8) or browser extension (e.g., NCapture) were developed to target users who do not have a technical background.

Content analysis

Content analysis has become a very common approach amid YouTube studies for a long period; it provides an unprecedented opportunity for researchers to comprehend community interests and issues in more accurate shape (see e.g., Siersdorfer, Chelaru, Nejdl, & San Pedro, 2010; Uryupina, Plank, Severyn, Rotondi, & Moschitti, 2014). The basic idea of applying content analysis to user-generated text on YouTube is to, map words, phrases, themes, or concepts (Weber, 1990), and to discover new patterns that are invisible in numeric analysis methods (e.g., social network analysis). A review of the relevant works shows that the analysis of user-generated text (video transcripts, comments, replies) may perform through a statistical method (quantitative research), a non-statistical method (qualitative research) or both methods (mixed-method research).

Liddy (2005) identified three phases that the statistical analysis process must get through once the source of unstructured texts is selected: text preparation, processing, and analysis. The first stage is that researchers need to search for well-suited material to clean and

prepare the dataset for later analysis. The data cleansing includes converting sentences to words (e.g., I am so happy → I, am, so, happy), removing useless parts (e.g., punctuation, numbers), stopping unnecessary words (e.g., the, me, for, and to), getting the original root of verbs (e.g., lives, living, and lived → live), correcting misspellings (e.g., ues → use), and restricting the language (e.g., English). Analyzers decide to either utilize user-friendly software that is sophisticated (e.g., WordState8 and Discover Text) or develop their own machine learning algorithms to carry out this step.

Text processing refers to the determination of content analysis techniques to analyze prepared data and find new patterns. It is obvious that Natural Language Processing (NLP), as a high-performance machine learning method that takes the text structure into consideration, has been widely employed to extract significant knowledge from unstructured data. NLP is a system that consists of a group of theories and technologies aiming to arrive at the level of human brain ability in terms of analyzing and understanding natural language text (Liddy, 2001). There are two common models that NLP has been used with: supervised machine learning and unsupervised machine learning. Supervised machine learning is used for a corpus that has prior knowledge of outputs (e.g., using classification approach for part of speech tagging to retrieve noun, verb, adjective, and adverb counts of a document). Unsupervised machine learning is used for a corpus that has no prior knowledge of outputs (e.g., using topic modeling algorithms to extract common themes from customer reviews).

Lastly, once the aforementioned procedures are accomplished, researchers would start evaluating outputs to report extracted knowledge. But it should be emphasized that painting a conclusion of the studied problem by relying on only the quantitative analysis of users-generated text on YouTube is extremely dangerous. Almost every YouTube comment box has a number of off-topic and spam comments and replies that are able to contribute to drawing a contrary image of reality. For example, Tian (2010), showed that the ratio of irrelevant user-

generated text on organ donation-related videos is not simple, like asking about the music name used for a video background. The detection of such data to be excluded from the study is still in debate among industrial and academic society. As long as this problem has not been addressed yet, the adoption of the quantitative analysis approach alone does not seem the best option to process unstructured and complex data.

With regard to qualitative research methods, there is no specific guideline for researchers to follow before conducting user-generated text analysis. Scholars, especially those who focus on information privacy, have applied various qualitative techniques to their studies in an effort to get in-depth knowledge of personal attitudes toward technologies and practices. A few of them have established their analytical frameworks based on contextual integrity scale to examine transmission principles (e.g., Shi, Xu, & Chen, 2013), while the majority have used content analysis to identify the problem dimensions in a bigger picture (e.g., Ghosh, Badillo-Urquiola, Guha, Laviola, & Wisniewski, 2018). But the disadvantage of this research design is that the generalization of findings is not recommended (Niaz, 2007) because the sample size is often small. Accordingly, a mixed methods research design has become indispensable for unstructured data to analyze the research problem quantitatively and qualitatively.

Chapter summary

The analysis of FRT-related privacy concerns is one of the most active areas in the information age due to the increase of inappropriate practices committed by organizations (e.g., improper information collection and access). Previous studies have attempted to propose an accurate, ideal and an extensive framework to conceptualize privacy and analyze privacy-related challenges in different contexts. Some of those frameworks have been established based on privacy theories (e.g., privacy as limited access to self) that view privacy as a single dimension instead of, a dynamic (Altman, 1977), multifaceted (Heravi, Mubarak, & Raymond Choo, 2018), and complex perception (Wang, Lee, & Wang, 1998). Other frameworks have

been built relying on privacy theories (e.g., privacy as control over personal information) that limit the right to privacy to self-disclosure of PII. This research gap has pushed this study to develop a new framework seeking to reconceptualize privacy and evaluate the state of privacy in the context of FRT.

Chapter 3: Methodology

Overview of research design

As the prime objective of this doctoral dissertation was to assess information privacy in the context of FRT, this chapter sheds light on a novel framework that was implemented for the user-generated text on YouTube to answer the following research questions:

RQ1: What the most common FRT-related privacy concerns are raised by YouTube users?

RQ2: How do FRT-related privacy concerns reflect difficulties in the control over personal information?

The sequential exploratory mixed-method design was selected, as the most appropriate approach for a research issue that has no previous theories, to qualitatively explore various dimensions of FRT-related YouTube users' privacy concerns and quantitatively test them on a larger sample. In their joint work, Ivankova and Creswell (2009) described this design as the combination of qualitative and quantitative research methods used in two sequential stages within one study. The researchers in this design are allowed to first identify principal themes of a targeted phenomenon in a qualitative manner and then to examine the qualitative results by applying one of the statistical measurement instruments (e.g., questionnaire) for the purpose of external validation.

Based on that, Solove's taxonomy (2006) was chosen to initially direct the data collection and analysis operation of the user-generated content on YouTube. This taxonomy, as discussed earlier, consists of 16 elements (surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion, and decisional interference). These 16 elements are coded under four themes (information collection, information processing, information dissemination, and invasions) to look at privacy concerns from different angles. In order to make the taxonomy align with the context of this project, the

concept of each element was slightly adjusted and given an example based on the literature of FRT before starting the data collection and analysis operation.

YouTube data collection

Research queries development

Since its emergence in 2004, the YouTube website has hosted a wide array of live streaming and recorded videos. YouTube announced that its users contribute to producing video content equaling over 500 hours per minute, 30,000 hours per hour, and 720,000 hours per day (Hale, 2019). The content, similar to the majority of Web 2.0 Internet-based applications, is organized and indexed based on a user-generated keywords system to smooth the videos retrieval process, through hooking some keywords used in the video title and description (Kalra, Kathuria, & Kumar, 2019). The unfortunate thing is that a controlled vocabulary is not yet rooted into the YouTube search engine system to guide searchers to the selection of the right keywords. This means that YouTube video seekers are required to put in extra effort to come up with a list of the most commonly used words and phrases in a particular domain to retrieve relevant videos.

The preferable approach to address the above-mentioned dilemma in this doctoral dissertation was to extract contextual keywords from scientific and nonscientific sources to systematically structure the matrix. To begin this process, I first consulted the Google Keyword, Google Trends, and vidIQ tools. The principal purpose of the instruments is to suggest and compare the globally trending keywords for any topic that relied on search queries frequently performed by YouTube and Google users at an earlier time. A total of 11 search queries were identified; "biometric", "biometric" AND "privacy", "biometric technology" AND "privacy", "face recognition", "facial recognition", "face recognition technology", "facial recognition technology", "face recognition system", "facial recognition system", "face recognition" AND "privacy", and "facial recognition" AND "privacy"

Each of the search queries was posteriorly examined in an attempt to determine its validity rate in terms of FRT-related video retrieval. The single most striking observation to emerge from the preliminary screening was that the first nine search queries brought a massive number of FRT-irrelevant videos. Approximately two out of 18 videos were pertinent to FRT in general, and no more than one out of 10 videos was pertinent to the research context. For instance, the usage of "biometric technology" AND "privacy" retrieved videos about fake fingerprints, biometric security, privacy laws, biometric system development, and so on. Accordingly, "face recognition" AND "privacy" along with "facial recognition" AND "privacy" were initially assigned for this function.

On the other hand, to entirely ensure all or at least the larger part of FRT-related videos were brought to light, I formulated auxiliary search queries in a more specific pattern by pulling keywords from Solove's taxonomy. The 20 words and phrases labeled by Solove to describe and classify the categories and subcategories of his taxonomy were combined with the earliest search queries group. For example, I separately and sequentially employed "face recognition" AND "information collection", "face recognition" AND "surveillance", "face recognition" AND "Interrogation", " facial recognition" AND "information collection", " facial recognition" AND "surveillance", and "facial recognition" AND "Interrogation" for the first category. As a result, the eventual search queries set consisted of 42 items.

Sampling

The exact number of FRT-related videos as well as the attributes of their content has not been documented so far and will unlikely be for many reasons, including the inability to cover all dimensions of such a forked subject. For that reason, the selection of videos was restricted to three eligibility criteria both to involve a representative sample of the population and to guarantee the fulfillment of the principle of data quality. The criteria were: (1) videos where their master debate concentrated on information privacy concerns toward FRT to align

with the research aims and question, (2) the timeframe of video publication date was 2014 and later, as it has been proven that the individuals' privacy concerns rate has negatively changed since 2014 (Auxier et al., 2019a), and (3) the whole video content must be produced in English to be completely understood.

I randomly selected and screened the first 20 unique FRT-related videos of each search query filtered by views to offer an equal chance of being engaged. However, it is important to take into account that the response for the search queries was utterly different in its quantity due to the variation in the nature of keywords adoption within the YouTube community. Some search queries were able to capture fewer videos than others since the video title and description contained keywords used by the minority of video publishers. For instance, the use of "facial recognition" AND "privacy", "face recognition" AND "privacy", "facial recognition" AND "surveillance", and "face recognition" AND "surveillance" retrieved in excess of half of the reviewed videos, while "facial recognition" AND "Distortion" and "face recognition" AND "Distortion" came back with a poor output, namely 11 videos, none of which was relevant or touched any element of the selection criteria.

Given the high complexity of the YouTube algorithms structure, there was tremendous noise in the video retrieval process. Several videos were presented more than once across various search queries because of YouTube's Recommendation System. This system is a form of machine learning developed to observe YouTube users' behavior in order to establish a suggested list of relevant videos for those who have the same interests (Cooper, 2020). As an illustration, when 100 users seek FRT-related videos using dissimilar search queries and then watch the same video, the algorithm connects the employed search queries to the watched video to keep it frequently retrieved for future users who adopt one of the search queries. In view of this, any FRT-related videos previously watched and appearing again with other search queries were skipped and uncounted within the first 20 unique FRT-related videos.

It should be admitted, however, that the existence of duplicate video content was the biggest challenge I faced during the sampling. Online video-sharing platforms on the whole, including the YouTube website, are in a significant crisis of repeatedly uploading matching video content by different users. Some search queries resulted in bringing up the same FRT-related video content published by multiple channels that might or might not belong to one entity for a wide array of aims. For example, I observed that news organizations on YouTube heavily support the duplicate-content strategy as a means of reaching the largest segment of their targeted population. This norm is not novel and has been investigated for quite some time in the literature of information retrieval; the framework is known as Near-Duplicate Video Retrieval (NDVR) (see e.g., Kordopatis-Zilos, Papadopoulos, Patras, & Kompatsiaris, 2017; Liu et al., 2013; Song, Yang, Huang, Shen, & Hong, 2011).

Uploading the same video multiple times—perhaps to create an uncomfortable feeling for YouTube researchers and to cause difficulty for them in the performance of their tasks—could feed scientific projects much more data than planned. The duplicate FRT-related videos in this doctoral dissertation were not completely excluded; rather this issue was managed through a data synthesis pattern because the main objective of FRT-related videos sampling was to scrape data associated with their pages. I considered the FRT-related video firstly uploaded based on its publication date as the original video version, tied the rest of duplicate videos to it for later data extraction, and counted only the original video copy within the first 20 unique FRT-related videos. At the data extraction phase, which is described in the next section, unique user-generated content in the original video and its duplicate copies was aggregated.

Nearly a month, August 1 to September 7, 2020, was spent on the videos sampling. There were 1,318 watched and evaluated videos that emerged from 42 search queries, but less than 16% were the candidates to join this study. Table 4 provides the summary statistics for

assessed, excluded, and included FRT-related videos across various aspects of the users' privacy concerns. It is obvious that by far the majority of included videos covered a couple of privacy concerns in their content, whereas very few videos were limited to a single aspect of the users' privacy concerns, such as information dissemination-centered video content. The grounds behind the exclusion of videos were roughly 6% non-English, 14% misleading title, 17% out of the publication date range, 19% identical content published by different users, 20% out of the context, and 24% frequently retrieved across search queries.

Table 2. Statistical summary of assessed, excluded, and included FRT-related videos

Video content	**Assessed videos**	**Excluded videos**	**Included videos**
Information collection	337	298	39
Information processing	112	86	26
Information dissemination	106	92	14
Invasions	84	73	11
More than a category	679	563	116
Total	1,318	1,112	206

Data extracting

The users' interaction shapes the prime data source contributing to the architecture of YouTube pages, from publishing a video to commenting on a comment. Current scholars who are interested in investigating the analogous line of this research have a tendency to divide the video data source into a video publisher and commentator. They labeled a video publisher a user whose mission is to produce or upload video content while they labeled a video commentator a user who responses to video content or other comments. But, regrettably, those broad terminologies will likely cause confusion for readers, since they are open for several interpretations. For example, when a researcher discusses study results with regard to the video

commentator, the audience needs much effort to predict whether it means the user who replied to the video or other comments.

To handle such barrier before beginning the data gathering, the video data source in this research was alternatively sorted into three layers: a speaker, a commentator, and a replier. A speaker refers to a video content maker regardless of whether or not the video speaker was the exact person who uploaded the video; a commentator is a top-level comment maker who responded to the actual post; and a replier indicates a low-level comment maker who responded to a top-level comment or another low-level comment. Each of the predefined data subjects was given an unparalleled code beside their appellations, a speaker (1), a commentator (2), and a replier (3), in order to simplify and arrange the data collection and analysis process as well as to minimize the occurrence of any ambiguity in the study outcomes.

Overall, extracting the necessary and valuable data from included videos passed through a long journey of development, evaluation, and aggregation. Every video content, in the first phase, was transcribed in real time exploiting the voice typing feature in Google Docs that listens to video audio that come out of video speakers and automatically converts it into a textual form. Even though transcripts were available in all included videos via their publishers, the greater part of which were transcribed through YouTube Auto-Generated Captions (YAGC) service. As stated on the YouTube help page, the machine learning algorithms used in YAGC might fail to recognize the right words spoken in video content for various reasons, including unintelligible accents and background noise. Lee and Cha (2020), likewise, emphasized this trouble and argued how such an inaccurate service could construct misrepresented content. Accordingly, adopting voice typing in real-time was a more reliable approach to track text conversion and revise mistakes in real-time.

A publicly available corpus of top- and low-level comments associated with videos was further automatically scraped to draw out the collective FRT-related privacy concerns among the three layers of users. It can be seen from the data in Table 5 that the final dataset of comments was composed of 198,627 rows, made up of 123,301 top-level comments and 75,326 low-level comments. Over 52% of commentators and repliers paid close attention to FRT-related videos that concentrated on privacy concerns surrounding information collection practices and surveillance in particular. But it should be pointed out that the comments dataset was not set up relying on only top- and low-level comments posted on the 206 videos. Approximately 7% of the involved top and low-level comments were collected from 19% of excluded videos, which had the same content and were published by many users, to maintain a balance between data quantity and quality.

Table 3. The statistical summary of comments dataset

Video content	**Acquired comments**	**Integrated comments**
Information collection	104,736	3,188
Information processing	22,814	1,527
Information dissemination	17,038	1,009
Invasions	5,993	841
More than a category	48,046	7,651
Total	19,8627	14,216

At the eventual phase of data collection, various types of metadata in posted videos were obtained for the purpose of general statistic description. Numeric data represents a central textual data's ally in the user-generated content that a machine produces in an automated manner to describe users' behavior toward a certain event. Though numeric data had minor importance and was not related to the research questions to any degree, it was taken out to

provide a broad insight into the change volume in the YouTube users' interaction with each other during different periods of time. Due to this, metadata about video content (video length, posted date) and the users' engagement (view, like, dislike, comment, and reply counts, as well as commented and replied date) were automatically download in a similar fashion to the comments through YouTube Data API (v3) developed in a Python environment.

YouTube data analysis

Privacy-related keywords development

As there is the possibility of scams and irrelevant materials to occupy a part in user-generated content in Web 2.0 (e.g., asking about the music background of a video or competing with whoever comments first), it is time consuming to begin the content analysis without establishing or adopting a tool to exclude those materials. One of effective mechanisms to address such a dilemma is the development of a relevant keywords list to retrieve only related materials. Diverse scholars have produced privacy dictionaries (e.g., Gill, Vasalou, Papoutsi, & Joinson, 2011; Vasalou, Gill, Mazanderani, Papoutsi, & Joinson, 2011); however, those projects have fell in the identical flaw that not taking language variation (sociolinguistic) into account by limiting their focus to a single aspect (e.g., privacy policies or interview transcripts).

It is well established from a series of studies (e.g., Bernstein, 1960) in the realm of sociolinguistics that it is natural to find that different groups in one society embrace different vocabularies to interpret an object. Privacy lawyers, for example, sometimes use surveillance in their speeches and writings to refer to data tracking, while privacy scholars use surveillance, control, monitoring, or collection to mean the same thing. If this variation is not borne in mind during the privacy dictionary development, the retrieval amount of relevant materials might be restricted, which undoubtedly will influence the conclusion. For that reason, I developed a privacy-related keywords list based on multiple aspects (legal, academic, personal) before diving into the YouTube data analysis to capture the most commonly used keywords that are

connected to Solove's taxonomy among policymakers, academic scholars, and social media users.

Data collection

Privacy policies

Privacy policies represented the legal component of the corpus acquired for privacy-related keywords development. I screened a network of top-visited websites with the intention of extracting their privacy documents, taking full advantage of the Websites Popularity feature in Alexa.com and Moz.com. Those tools basically provide their own list of top 500 websites globally visited, ranked based upon a complex statistical analysis of several factors, including search traffic and daily visitors, to be publicly available for academic research and other uses. The whole record advanced by Alexa.com was mapped, followed by the one in Moz.com at an early stage to filter duplicated materials that present in both records. An immense percentage (88%) of reviewed websites (1000 websites) were owned and managed by commercial sectors; roughly 50% of those websites were duplicate that appeared in both Alexa.com and Moz.com as one of the top 500 visited sites (e.g., Google.com showed up in Alexa.com and Moz.com as the second most visited site on the web).

A total of 546 websites were unique and being surveyed. Some of those websites' privacy statements were readily accessed via a hyperlink placed on the top or bottom of the web homepage, while locating others was a challenging mission and took considerable time. Regardless of that obstacle, there were only 317 websites that contained valid privacy policies imported by Selenium Python API, which captures and saves website page content in sundry formats such as HTML. Approximately 38% of excluded sites had no privacy policy, had a written privacy policy in languages other than English, or had a privacy policy mixed with Terms of Service. On the contrary, the largest number (62%) of sites embraced identical

privacy statements inasmuch as they are operated by one organization (e.g., Skype, Outlook, and Microsoft Teams software are used Microsoft corporation's privacy policy).

The collected privacy documents were varied considerably in their length, content, coverage, etc. This might be a natural phenomenon, as the privacy template design is usually manipulated by information flow in a given context. A fitting instance of such variation is Web 2.0 Internet-based applications (e.g., social media outlets), where their providers overwhelmingly build much longer privacy agreements than Web 1.0 channels suppliers do (e.g., online news organizations) because of the functions quantity that users could perform, including creating personal profiles. In view of this, pulling privacy statements across the multiple domains (e.g., Arts, Business, Computers, Games, Health, Home, Kids and Teens, News, Recreation, Reference, Regional, Science, Shopping, Society, and Sports) labeled by Alexa.com had a critical role to play in developing a thorough list of privacy-related legal keywords.

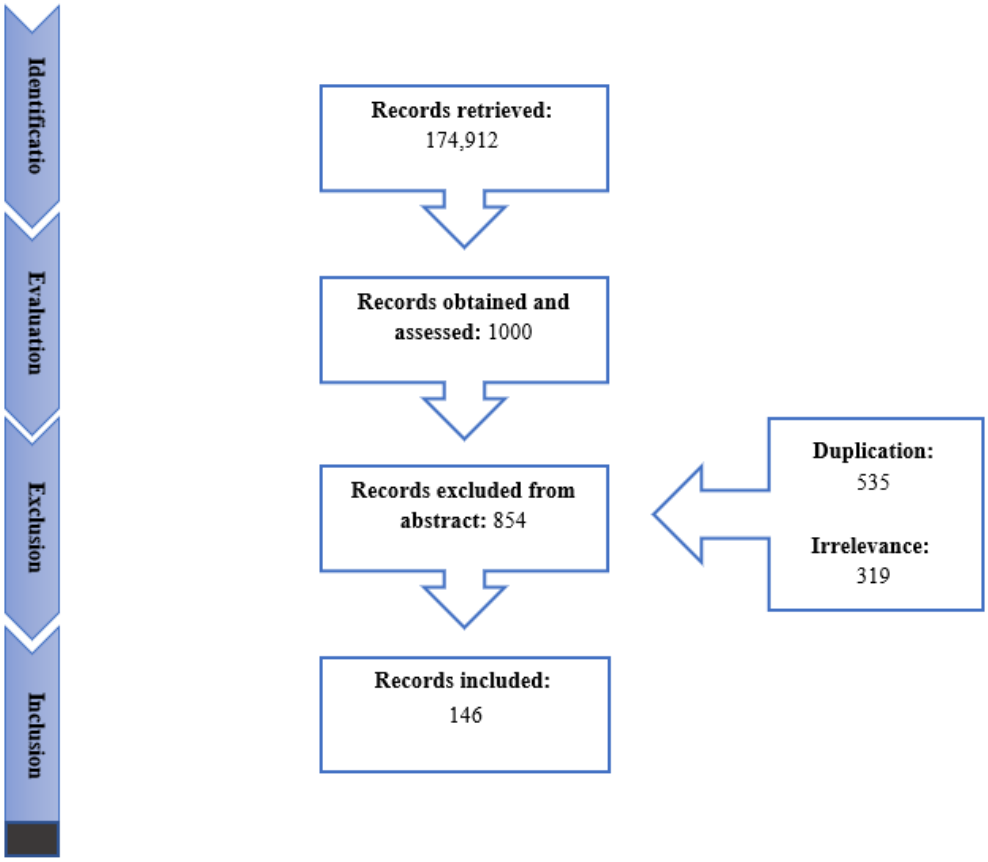
Scholarly articles

Privacy-related publications were a weighty data source that added a scholarly substance to the task and motivated its growth to move forward. I began this process by typing "Information Privacy" into the built-in search engine in the Saudi Digital Library (SDL), which has subscription-based access to a useful number of well-known research databases, including IEEE Xplore, and Web of Science. The search query results, through the advanced search feature, were limited to English articles where their titles contain information privacy or relevant keywords (e.g., data privacy, privacy concerns, and privacy risks) so as to not access irrelevant materials that just mentioned those keywords within their full text for other purposes. Similarly, this restriction was applied to search for only academic peer-reviewed journals in an effort to make certain that the extracted keywords had the capability of reflecting experienced scholars' language instead of that of enthusiastic or beginning authors.

From 2006 (the release year of Solove's taxonomy) to 2020 (the year of this process), 174,912 records that were sorted by relevance came to light. Privacy-oriented studies published in academic journals and conference proceedings formed nearly 89% of the aggregate, while the other 11% came from newspapers, magazines, etc. I manually downloaded the first 1000 rows (100 pages) as a sample and navigated among their abstracts to filter uncontacted frameworks. Each abstract was read multiple times by two evaluators, including the researcher, to recognize its alliance degree with Solove's taxonomy. The evaluators separately reported the article metadata and elements of Solove's taxonomy, if any, that the article abstract covered. Articles that both evaluators believed their abstracts discuss at least one element of Solove's taxonomy as the main research orientation were included. Other articles where any element of Solove's taxonomy was far away from their central point or the main research problem were unclear were eliminated to avoid useless keywords.

The diagram below (Figure 1) highlights the whole procedure of the inclusion and exclusion of those materials as well as the removal grounds. Surprisingly, the major proportion of the screened researches was unfortunately irrelevant. In the region of 85% (854) out 1000 scholarly products across realms (e.g., social media, IoT, and smartphone) were excluded, while less than 15% (146) out of which were involved. The exclusion of 854 records was due to duplication (62.65%), an article that was already reviewed, and irrelevance (37.36%), an article that has not touched any dimensions of Solove's taxonomy or the dimensions mentioned in the article did not represent the main focus (e.g., mentioning surveillance as one of the disadvantages of joining social networking sites but the main purpose of the article was to broadly discuss advantages and disadvantages of those sites instead of a particular aspect).

Figure 1. The procedure for the inclusion and exclusion of scholarly articles



Web-based survey

Inviting individuals to collaborate on the establishment of privacy-related keywords was the ultimate data collection procedure in this phase. Given the fact that the motivation for generating such a list was to serve as a map to retrieve privacy-centered textual data extracted from FRT-related YouTube video pages, recruiting participants from similar environments was indispensable in order to boost the reliability of the privacy-related keywords list. Thereupon a short, web-based survey (see Appendix A) was constructed via SurveyMonkey to

communicate with participants in a simple manner. The online-based survey link provided was distributed by seven people, who were hired by the author, across social media platforms (YouTube, Facebook, Twitter, WhatsApp, Instagram, Reddit, Snapchat, and Telegram) with an initial goal of obtaining 500 social media users' responses. This survey was accessible to the users for a three-week period, October 16 – November 6, 2020. During this duration, 10 reminders were sent through reposting the online-based survey, more or less, every other day in an attempt to obtain as many responses as possible.

The electronic-based survey invitation (see Appendix B) was restricted to users who accepted voluntary participation, speak English, and understand how FRT operates. In general, the survey consisted of closed-ended and open-ended questions divided into two segments. Users, first and foremost, were asked to report some of their demographic information including age, location, and gender to ensure that all spectrums of the social media community had an equal chance of being represented. The second part was designed to extract the most commonly used keywords in connection with Solove's taxonomy. A contextual definition and example for each element was provided based on the literature of FRT to help users comprehend Solove's taxonomy in the context of FRT. The role of users was then to write down synonyms and relevant keywords for each element. Surveillance (the first element of Solove's taxonomy), for instance, received keywords such as gathering, collection, spy, and consent.

Five hundred eighty-four responses to the survey were received, the majority (87%) of them during the first two weeks, especially on the weekends. An extremely low number of data subjects (22.8%) fulfilled the entire survey, while others (77.2%) missed the second and crucial part, which the study depended on. From Table 2, which presents the main characteristics of the 133 involved users, it is apparent that females between 30 and 49 years old, whose mother tongue is English, and live in North America countries shaped the largest group of the study

sample compared to other classes. This variation was absolutely not surprising, since the literature has proven that gender (e.g., Hoy & Milne, 2010; Youn & Hall, 2008), age (e.g., Kezer, Sevi, Cemalcilar, & Baruh, 2016; Van den Broeck, Poels, & Walrave, 2015), and cultural values (Bellman et al., 2004; Harris et al., 2003) are all factors that influence personal attitudes toward information privacy concerns.

Table 4. The main characteristics of participants

Characteristic		**Frequency**	**Percentage**
Age			
	18-29	19	14.3%
	30-39	57	42.9%
	40-49	44	33.1%
	50-59	12	9%
	60-69	1	0.7%
	70 >=	N/A	0%
	Unspecified	N/A	0%
Gender			
	Male	47	35.3%
	Female	86	64.7%
	Other	N/A	0%
	Unspecified	N/A	0%
Native language			
	English	79	59.4%
	Non-English	51	38.3%
	Unspecified	3	2.3%
Location			
	North America	82	61.7%
	Middle East	34	25.6%
	Europe	9	6.8%
	Australia	4	3%
	Africa	2	1.5%
	Asia	2	1.5%
	South America	N/A	0%
	Unspecified	N/A	0%
	Total	133	100%

Data analysis and results

Quantitative content analysis was used after extracting targeted content from the corpus (e.g., expunging headers and footers from scholarly articles and privacy documents) following

two steps: a rudimentary selection of keywords and a final selection of keywords. An appropriate number of comprehensive online thesauruses, suggested by an English professor in the U.S., including lexico.com, thesaurus.com, and merriam-webster.com, were searched with the objective of establishing an elementary series of keywords to assist in boosting the efficiency of actual data analysis performance. Their search engines independently received the 16 elements of Solove's taxonomy, as search terms, to map their synonyms and relevant keywords in the databases. The decision of whether or not a retrieved material was connected to this taxonomy relied on provided definitions and examples. If any of this material was conceptualized along the same line of an intended element and widely acceptable among those lexicons, it was marked as an item nominated for the next phase.

Before reaching the next point, conducting text preprocessing was indispensable to normalize the corpus through Natural Language Toolkit (NLTK), the most-used NLP library in Python environment, to transfer text from human to machine language as well as to exclude meaningless content. The text preprocessing patterns I implemented were *tokenization* to split a text into words (e.g., tokenizing the sentence: I have privacy concerns to I, have, privacy, concerns); *non-English words removal* to not involve words other than English (e.g., Arabic and Spanish); *stopwords* to exclude unaffected words (e.g., I, have, is, he, she); *special characters removal* to cut off symbols (e.g., punctuation, bracket, hashtags, numbers); *transform cases* to convert uppercase to lowercase (e.g., the substitution of I to i); and *lemmatization* to revert inflection words to their roots (e.g., lemmatizing finds, found, finding to find).

In the interest of effectively and efficiently evaluating the prepared list of keywords, the TF-IDF model was utilized to encode text into a numeric vector as a weighting scheme. TF-IDF is an unsupervised machine learning model standing for Term Frequency–Inverse Document Frequency; it statistically scales the degree of a word's importance across given

documents. It is unlike other text vectorization approaches, such as the bag-of-words model, where word frequency in the documents is only the factor taken into consideration. TF-IDF computes its weighting matrix by multiplying TF with IDF, where TF = (number of times the term *t* occurs in a document *d*) / (total number of terms in a document *d*) and IDF = log (total number of documents *D*) / (number of documents *D* contain term *t*). As a common example, assuming the word *cat* presents three times in a document that contains 100 words and the same word presents in 1,000 out of 1,0000,000 documents, then the TF-IDF is (3/100=0.03) * log (10000000/1000= 4) = 0.12.

Because words are treated individually in TF-IDF model that could easily lose meaningful phrases, the analysis of the keywords was filtered by the N-Gram model. N-gram is an unsupervised machine learning model for developing a co-occurrence matrix of a given text to move from extracting single words (unigram) to a sequence of N-Gram, called bigram for two words, trigram for three words, four-gram for four words, five-gram for five words, and so forth. The probability of a word occurrence for predefined N-Gram is basically relied on by dividing the total number of the previous word *wp* presents before the word *wn* by the total number of the previous word *wp* presents in the documents. In other terms, if N-Gram were set to bigram, the measurement of the probability of the word *secondary* occurring with the word *use*, for example, is (number of times *secondary use* occurs) / (number of times *secondary* occurs in the documents). As a consequence, I adjusted the feature space to trigram, as the longest phrase identified in the initial list of keywords was two.

With both models, the output of the three scanned sources was limited to the first 2,000 rows. Keywords extracted at an early stage were then evaluated based on their existence among the most important 2,000 rows to clean worthless items from the list. About half of keywords in the initial list were ranked between 0 to 0.5, and the other half did not appear with the first 2,000 keywords. This has something to do with the fact that some single or even compound

words might be adopted by only one party, such as the word *transfer* frequently used by privacy documents but not by scholars or users to refer to the information movement from a point to another. In consideration of the foregoing, other relevant keywords that appeared within this range (the first 2,000 keywords) but were not listed in the initial phase were inserted as well if they passed the definition assessment, as elucidated earlier; these represented 8% of the final list.

Table 3 presents the first 20 privacy-related keywords indexed in the final list along with their TF-IDF score (see Appendix C for the complete list). It was observed that the overwhelming majority of phrases emerged from the survey and scholarly articles (e.g., big brother, fake information, and information flow), whereas privacy documents put their main focus on single words (e.g., disclose, collect, and access). This might be linked to the nature of the legal language used in the privacy policy templates. However, what is more interesting about the results was that there was a huge gap in subjects covering. Privacy documents tended, regardless of whether this was intended or not, to not allude to any codes in the last theme of Solove's taxonomy (intrusion and decisional interference), unlike the other three themes, although the four themes were frequently covered by other parties.

Table 5. The first 20 common privacy-related keywords

Keywords	**TF-IDF**	**Keywords**	**TF-IDF**
Advertisement	0.02	Permission	0.03
Aggregation	0.06	Privacy Agreement	0.09
Anonymity	0.03	Profiling	0.04
Collect	0.00	Sell	0.06
Confidentiality	0.08	Share	0.05
Consent	0.05	Spy	0.01
Control	0.01	Surveillance	0.00
Disclosure	0.02	Third party	0.07
Gathering	0.01	Track	0.00
Leak	0.07	Watch	0.00

YouTube data analysis: qualitative analysis

Qualitative content analysis was done for the first part due to its efficacy to paint a deep and obvious frame of the roots of the users' privacy concerns toward FRT. I primarily picked the first five videos from the category that raised more than one privacy concern depending on the comments count to reduce the chance of being biased for one aspect over another and to get a better understanding of all dimensions linked to the studied phenomenon. This number was subject to augmentation in case the principle of saturation was unsuccessfully reached. As reported by Charmaz (2006), saturation is the continuation of the data collection or analysis process does not supply new information about the research problem. Nonetheless, the chosen videos were more than enough to accomplish this task.

For a systematic organization and evaluation, the transcripts, comments, and replies of these videos were merged into three separate text files to represents a different layer of the users and then uploaded to MAXQDA, computer-assisted qualitative data analysis software.

MAXQDA software offers a unique feature called Go Lists, customizing the retrieval results to be limited to particular keywords, which helped to only map cases where the users touched any privacy-related keywords illustrated in phase I. But the main obstacle was that this feature has not yet advanced with natural language processing to take affixes and other syntax into consideration. In other words, sentences that include surveil, surveilled, or surveilling are not expected to retrieve if the inserted query was surveillance. This difficulty, therefore, was addressed by feeding queried keywords their suffixes and prefixes, if applicable, in a manual mode to raise the retrieval rate.

The sum of data rows that emerged from the three text files was 29,074, nearly 70% of which hit at least one of the privacy-related keywords. I randomly analyzed the first 613 out of the retrieved cases; 34 cases from transcripts file, 318 cases from top-level comments file, and 261 cases from low-level comments file where the users expressed their privacy concerns surrounding the functions of FRT, not other technologies (e.g., smartphones). Every adopted case was categorized into the most relevant element of Solove's taxonomy at the outset. Some of these elements did not, unfortunately, get the majority of users' attention, as they were mentioned less than twice (e.g., intrusion and appropriation), while others came into view in dozens of lines (e.g., surveillance and insecurity). All classified cases were thereafter reread multiple times in order to find patterns enabling me to reconceptualize the taxonomy in the frame of FRT.

The analysis confirmed that there were nine different privacy concerns divided into four main themes: information collection (surveillance, coercion), information processing (retention period, profiling, security, secondary use, exclusion) information dissemination (disclosure), and invasion (decisional interference); these are explained in the results chapter. To ensure that the interpretation of data was valid and objective, intercoder reliability was applied to the outcomes. Twenty representative examples of each code were shared with a privacy scholar

and lawyer who has 18 years of expertise in the field of information privacy laws, after paraphrasing the content for the users' privacy protection. The agreement rate was almost 94% (see Appendix D for the detailed matrix), which is considered an acceptable rate.

YouTube data analysis: quantitative analysis

With the possibility of intended or unintended bias occurring in the qualitative analysis, it was important to perform further procedures guaranteeing the attainment of external validity of the study findings. As reported by Winter (2000, p.9) that "external validity is the extent to which the results can be generalised and thus applied to other populations." I, thus, developed supervised classification through RapidMiner Studio, a visual data science workflow for the development and validation of machine learning models, in order to automatically predict and categorize unseen (unanalyzed) texts into the nine predefined privacy concerns. The following subsections should draw a thorough image of the development and application process of the classifier divided into three essential steps: text preprocessing, text processing, and text analysis.

Text preprocessing

The first step that undoubtedly could not be overlooked before training and evaluating the classifier was to prepare the analyzed texts in the qualitative phase in a certain way to be understood by the machine and boost classifier accuracy. I followed the exact text preprocessing patterns completed for phase I (privacy-related keyword development) such as tokenization, non-English words removal, and transform cases. I did so for this corpus as well except the lemmatization algorithm, which was substituted for the stemming algorithm (snowball stemmer) to cut the suffixes of vocabularies instead of reverting inflection words to their roots. The logical basis for this substitution was the desire to prevent the machine from assessing a different part of speech for a word as a different word when starting to build a word

vectors matrix, especially for privacy-related keywords (e.g., reading surveillance, surveil, and surveilled as surveil not as surveillance and surveil).

Although the lemmatization algorithm outdid the stemming algorithm in handling complex language issues that might negatively affect classifier accuracy, such as irregular verbs, these and other issues observed during the qualitative analysis were controlled by the dictionary replacement operator. This operator received an Excel sheet that consisted of multiple instructions to guide the machine in reverting irregular verbs to their roots (e.g., reverting sold to sell), excluding the possessive form (e.g., removing the possessive form from organization's face recognition to be organization face recognition), replacing frequent abbreviations (e.g., replacing information with info), and standardizing some nomenclatures (e.g., replacing facial recognition technology with facial recognition, face system, face technology, and facial system).

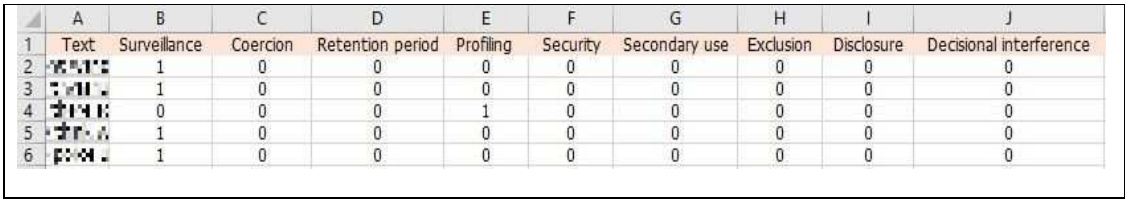
TF-IDF model filtered by the N-Gram model was adopted with the objective of generating an understandable weighting scheme for given and cleaned samples. There was a sequence of general concepts frequently raised among the texts (e.g., face recognition technology) where their meanings were manipulated by the context. Those items might cause misclassification if not being generated with obvious patterns that allow the system to identify the fine distance between two different points. For example, instead of linking face recognition technology to all the nine privacy-related concerns, it is better to specify Face_ surveillance_Public to surveillance and Face_ Profling_ Analysis to profiling. Hence, every row of the weighting scheme was expected to produce three or fewer trigrams, as the maximum length of analyzed concepts was not to exceed three words.

Text processing

Given that the users' engagement with the problem was quite dissimilar—some did not have any FRT-related privacy concerns while others had one or two at the same time with different degrees of importance—the classifier was developed in multi-label mode. In the field of machine learning, the application of multi-label classification has lately become a common practice for mapping *x* (given text) to *y* (target variables) to predict all relevant labels. It is in contrast to the multi-class classification that the prediction outcome is one and only one whether or not *x* is related to *y*, multi-label classification has the potential to sort a given text into none, single, or multiple labels. This means the developed classifier eliminated irrelevant materials (e.g., privacy concerns surrounding the smartphone's GPS chip) and positively predicted different dimensions of FRT-related privacy concerns mentioned in a row as long as the obtained value is considered significant by the used algorithm.

As shown in Figure 2, the nine labels were transformed into a separated binary classification, known as binary relevance, to originate a negative value (0) for irrelevant texts; otherwise, a positive value (1) was given. The dataset (613 rows) was split into 80% training and 20% testing to evaluate its performance. The elementary accuracy rate (58%), as anticipated, signalized that the classifier needs to be fed with more representative examples to minimize the chance of falling into the mislabeling problem, chiefly for classes that have an overlap with others (e.g., surveillance, profiling, and security). In order to reform that, the strategy put into practice in the qualitative analysis to extract related cases was reapplied on the same five videos to get extra inputs with taking into account the distribution of classes to make the difference between the minority (the lowest) class and the majority (the highest) class not overtake 50% to avert biased predictions.

Figure 2. A snapshot of the training dataset



	A	B	C	D	E	F	G	H	I	J
1	Text	Surveillance	Coercion	Retention period	Profiling	Security	Secondary use	Exclusion	Disclosure	Decisional interference
2	[redacted]	1	0	0	0	0	0	0	0	0
3	[redacted]	1	0	0	0	0	0	0	0	0
4	[redacted]	0	0	0	1	0	0	0	0	0
5	[redacted]	1	0	0	0	0	0	0	0	0
6	[redacted]	1	0	0	0	0	0	0	0	0

The exploited algorithm to train and test the final dataset that comprised 2,317 inputs (372 surveillance, 296 coercion, 182 retention period, 235 profiling, 326 security, 215 secondary use, 190 exclusion, 233 disclosure, and 268 decisional interference) was Support Vector Machine (SVM) linear kernel, it is an appropriate model for a small training dataset and offered the best accuracy rate for this classifier. SVM linear kernel is a powerful supervised machine learning algorithm for high-dimensional data (e.g., text classification) seeking to find the optimal hyperplane as the decision boundary by maximizing the marginal distance between the two classes to minimize the chance of misclassification. More clearly, the starting point of the negative (-1) and the positive (+1) region is determined by the nearest data point (support vectors) to the decision boundary that changes based on the placement of the new support vectors to reduce the risk of overfitting.

The main disadvantage of transforming the multi-label problem to binary classification in machine learning algorithms is imbalanced data; the negative class is much larger than the positive class and vice versa, which creates a bias to the majority class. In SVM, the regularization parameter, often called C parameter, guides the model of the misclassification rate accepted in a given dataset; assigning a large value to C leads to a smaller-margin hyperplane while a small value to a larger-margin hyperplane. Setting a single value, whether a large or a small value, for this dataset does not make any sense inasmuch as the difference between the negative class (16,151) and the positive class (2317) is very close to 88%. Accordingly, I optimized the weight for each class (1:2) to increase marginal distance in the

negative class and decrease it in the positive class, which aided in reducing the risk of errors on data.

The confusion matrix (Figure 3) provides an inclusive view of the classifier performance that confirmed the classifier's capability to generalize the qualitative findings (see Appendix E for the micro matrices). Both precision rate (98.1%) and recall rate (93.63%) were the two factors taken into consideration to evaluate classifier accuracy (98.08%). The precision rate is the total number of true positive prediction (the true positive predictions (400) + the false positive predictions (8)) / (the true positive predictions (400)), while the recall rate is the total number of true positive retrieval, (the true positive predictions (400) + the false negative predictions (63)) / (the true positive predictions (400)). In sum, the maximum rate the classifier could produce false positives predictions was less than 2% (1.9%) and false negative predictions was less than 7% (6.37%).

Figure 3. The confusion matrix

accuracy: 98.08% +/- 1.62% (micro average: 98.08%)

	true 1	true 0
pred. 1	400	8
pred. 0	63	3219

Text analysis

The classifier was loaded once the entire collected data (analyzed and unanalyzed data) was uploaded to the RapidMiner Studio and normalized (e.g., stemming) to launch the classification procedure. Each text row, as mentioned in the previous section, had a probability to receive negative values for all the nine labels if it is ranked as irrelevant content, a single positive value if it is connected to one of the nine labels, or more than one positive values if it is related to multiple labels. All three cases were inspected to determine: the rate of negative perspectives and nonnegative perspectives toward FRT, the common factors that caused

negative perspectives, the rate of adopting single and multiple negative perspectives, and factors that frequently came with each other among the users.

As the layout algorithms available to the RapidMiner Studio are almost limited to multiclass classification, the prediction matrix generated by the RapidMiner Studio was exported to the Python environment to complete the aforementioned functions. The preliminary analysis, however, indicated that the classifier would likely draw an inaccurate conclusion with the existence of duplicate content. Several speakers were observed to adopt a short clip from other videos as supportive evidence for their arguments or as a reference to clarify complicated concepts. This behavior was also found among the top-and-low-level comments for different reasons (e.g., the network latency or the user's desire to spread some attitudes at a wide scale). For that reason, the duplicate content was removed in an automated method to not count a particular privacy concern multiple times.

Research ethics

The deference to ethical principles of academic research is a key part of investigators' priorities, especially for online human subjects-centered studies. According to Zimmer (2018, p.2), a privacy and ethics scholar in Internet-based research, "A core principle of research ethics is non-maleficence—the duty to avoid, prevent, or minimize harms to subjects." In addition, the author in his framework came up with a set of detailed guidelines to direct those who are interested in undertaking such research to preserve subjects' values and private spaces from a wide array of ethical lapses in research. The instructions include getting informed consent followed by stating ethical concerns linked to a data collection and analysis protocol along with establishing an effective approach to overcome or at least minimize harms caused to individuals.

Three principles of research ethics (informed consent, anonymity, and confidentiality) are the prevalent challenges encountered in this and equivalent projects. Those obstacles, therefore, were taken into account and managed carefully in both studies to create a balance between research benefits and humans' privacy. In the web-based survey for privacy-related keywords development, all participants received the informed consent form that illustrated the study aims alongside risks and benefits related to their engagement in the survey so they could make an appropriate decision. Subjects who voluntarily agreed to participate were asked to disclose only de-identifiable information (e.g., current place of residence, gender, and age) and had the right to withdraw at any time with no negative consequences. Even so, to increase data confidentiality, this unidentifiable data was stored in an encrypted folder so that its access was limited to the main researcher to increase data confidentiality.

An ongoing debate revolving around social media research is whether or not publicly available data is authorized to be obtained without informed consent. A group of scientists (e.g., Huete-Alcocer, 2017) shed light on the variation in the expectation of information flow in real-life communication versus virtual-based communication. They reckoned that the general public has realized, expected, and accepted that information about them that has been exposed to the online environment is, unlike offline-based interaction, reachable by anyone and at any time and becomes subject to gathering. While this opinion has been embraced by many scholars from different research domains, others (e.g., Zimmer, 2010), expressed their rejection of such improper justification, as social media data collection without users' informed consent in the majority of circumstances is considered an unethical practice. Their philosophical viewpoint was structured on the basis of the fact that information flow is controlled by an information generator regardless of whether this information is presented in a public or private space.

Based on the prior argument and with a view to maintaining YouTube users' privacy during the second research phase, I applied a similar procedure performed for the first work except for the informed consent part because of the difficulty of communicating with over 150,000 users. The final dataset produced for this stage was devoid of any identifiable information (e.g., usernames, channel name, and channel URL) and contained only unidentifiable numeric and textual data (e.g., comment counts, video transcript, and comment content) that was available to unregistered audiences. Each textual data row in the dataset, as explained earlier in this chapter, was assigned to one of the replaced titles (a speaker, a commentator, and a replier) to attain YouTube users anonymity as well as to regulate data analysis and interpretation. All those data rows were also saved in the same folder encrypted and unencrypted by no one other than the author.

It is important to underline that research protocols in both phase I and phase II were reviewed and approved by Institutional Review Board (IRB) at University of Wisconsin-Milwaukee (UWM); approval code for the first phase: 21.083, approval code for the following phase: 21.093. "The mission of the IRB is to ensure the adequacy of the research plan, to minimize risks and to maximize the potential for benefit for human subjects who participate in research" (“Institutional Review Board,” n.d.). This acceptance was given based upon a written pledge to report the outcomes in aggregate and to destroy the datasets once this doctoral dissertation is successfully defended. Not only that, the content of the YouTube video transcripts and comments would be paraphrased instead of sharing the verbatim content. This is because such data is dissimilar from data collected through traditional methods (e.g., interview, survey, and questionnaire), where YouTube users' identity could be simply recognized via copying exact phrases and pasting them on information retrieval-based applications.

Chapter summary

Forty-two search terms (e.g., "facial recognition" AND "information collection", "facial recognition" AND "surveillance") elicited from scientific and non-scientific sources were used to capture relevant videos. The selection of videos was random and restricted to various criteria (e.g., FRT-related videos produced in English) to make certain that the involved sample represented the general population and to be able to answer the research questions. Out of 1,318 retrieved and watched videos, there were only 206 FRT-related videos that met the criteria. The user-generated content of the 206 FRT-related videos was extracted through Google Docs for video transcripts and Python for top-level comments, low-level comments, and video metadata (e.g., like counts).

For analysis, the collected corpus was split into two parts using the sequential exploratory mixed-method design. In the first phase, qualitative content analysis was applied to examine relevant cases across five FRT-related videos by means of a privacy-related keywords list that developed at the beginning of the analysis process that relied on 596 documents (317 privacy policies, 146 scholarly articles, and 133 web-based surveys). The reliability of qualitative findings was achieved through independent coders that the agreement rate was almost 94%. The following phase was the application of quantitative content analysis to the 206 FRT-related videos by establishing a multi-label classifier (SVM algorithm) to validate qualitative findings. The accuracy rate (98.08%) of this classifier illustrated the extent to which quantitative findings are reliable enough. Both MAXQDA software and the RapidMiner Studio were instruments adopted for the analysis task.

Chapter 4: Results

General descriptive analysis

As introduced in the methodology chapter, there were 206 FRT-related YouTube videos involved in the study. The publication date of 21.9% (45 out of 206) of which were in 2020, 52.9% (109 out of 206) were in 2019, 12.6% (26 out of 206) were in 2018, 6.8% (14 out of 206) were in 2017, 3.4% (7 out of 206) were in 2016, 1.9% (4 out of 206) were in 2015, and 0.5% (1 out of 206) was in 2014. The approach taken to address FRT-related privacy concerns was various from one year to another. Close to 65.4% (34 out of 52) of videos that were published from 2014 to 2018 put their full attention to a single theme such as information collection, while 63.7% (98 out of 154) of videos that were published from 2019 to 2020 were more interested in addressing multiple FRT-related privacy concerns in their debate.

The table below (Table 6) illustrates the main characteristics of the collected sample in terms of video length along with the view, such as, dislike, comment, and reply counts that were organized based on the publication date (2014–2020). The total of the videos' length was 00:03:18 (the average: 00:03:18) in 2014, 00:10:69 (the average: 00:02:67) in 2015, 00:25.94 (the average: 00:03:71) in 2016, 01:23:75 (the average: 00:05:98) in 2017, 02:08:79 (the average: 00:04:95) in 2018, 10:31:32 (the average: 00:05:79) in 2019, and 04:04:69 (the average: 00:05:39) in 2020. Overall, the range of videos' length in all periods did not exceed 15 minutes, since Google by default limits it up to 15 minutes for a regular user, while a verified user might create a longer time frame than that; however, relevant literature found that YouTube videos are often around or less than the default length (e.g., Cheng, Dale, & Liu, 2008).

Table 6. The main characteristics of the 206 involved videos

Measurement	Publication Date	Total	Minimum	Maximum	Average
Length					
	2014	00:03:18	00:03:18	00:03:18	00:03:18
	2015	00:10:69	00:02:07	00:03:03	00:02:67
	2016	00:25.94	00:02:56	00:05:20	00:03:71
	2017	01:23:75	00:03:28	00:12:30	00:05:98
	2018	02:08:79	00:01:53	00:11:08	00:04:95
	2019	10:31:32	00:01:30	00:12:55	00:05:79
	2020	04:04:69	00:01:36	00:11:49	00:05:39
	Total	**18:51:16**			
Views					
	2014	108011	108011	108011	108011
	2015	126127	4698	119011	34281.75
	2016	180428	1409	51420	21501.33
	2017	3658073	1594	1279383	261290.9
	2018	1083819	848	441142	41685.35
	2019	23241705	1022	6192845	213226.7
	2020	34754026	1523	8592836	772311.7
	Total	**63152189**			
Likes					
	2014	4359	4359	4359	4359
	2015	5396	32	5146	1349
	2016	2068	32	698	299.3333
	2017	31569	33	10574	2254.929
	2018	39754	12	16762	1529
	2019	690964	23	182101	6339.119
	2020	835581	28	175583	18568.47
	Total	**1609691**			
Dislikes					
	2014	49	49	49	49
	2015	74	3	64	18.5
	2016	159	2	41	20.66
	2017	2915	7	1071	208.2143
	2018	9905	0	6740	380.9615
	2019	31237	0	6800	286.578
	2020	32630	4	6197	725.1111
	Total	**76969**			
Top-level comments					
	2014	694	694	694	694
	2015	957	3	932	239.25
	2016	1813	3	1043	259

	2017	4606	9	1888	329
	2018	2768	5	928	106.4615
	2019	53811	4	8478	493.6789
	2020	58652	26	10195	1303.378
	Total	**123301**			
Low-level comments					
	2014	312	312	312	312
	2015	292	0	286	73
	2016	146	0	50	20.5
	2017	3905	3	1601	278.9286
	2018	2485	0	1057	95.57692
	2019	32833	0	5237	301.2202
	2020	35353	32	5282	785.6222
	Total	**75326**			

A closer inspection of the table shows that the number of likes, dislikes, and top-level comments received by videos that were published in 2020 were much more than other videos that were published in the period between 2014 and 2019. In general, video viewers had less of a tendency to interact with watched videos. Fewer than 5% of video viewers decided to leave a like, a dislike, or a top-level comment on videos published in 2014 (likes: 4359, dislikes: 49, top-level comments: 694), 5.5% in 2015 (likes: 5396, dislikes: 74, top-level comments: 957), 2.5% in 2016 (likes: 2068, dislikes: 159, top-level comments: 1813), 1.5% in 2017 (likes: 31569, dislikes: 2915, top-level comments: 4606), 5% in 2018 (likes: 39754, dislikes: 9905, top-level comments: 2768), 3.5% in 2019 (likes: 690964, dislikes: 31237, top-level comments: 53811), and 3% in 2020 (likes: 835581, dislikes: 32630, top-level comments: 58652).

Furthermore, it is clear that the percentage (38%) of textual interaction between the commentators and the repliers was quite poor in comparison with its counterpart (62%) between the commentators and the speakers. The commentators were discovered to be more eager to leave their imprint on all involved videos (the minimum top-level comments: 694 in 2014, 3 in 2015, 3 in 2016, 9 in 2017, 5 in 2018, 4 in 2019, 26 in 2020). In contrast, it was not

one of the repliers' priorities to share their thoughts with the commentators in some videos published in 2015, 2016, 2018, and 2019 (the minimum low-level comments: 312 in 2014, 0 in 2015, 0 in 2016, 3 in 2017, 0 in 2018, 0 in 2019, 32 in 2020), although a single video in 2018 received more low-level comments (1057) than top-level comments (928). This might be a natural behavior pushed by the variation in the rate of users' concerns from one category to another.

There were in the region of 2 million words extracted from the users-generated texts, in excess of 70% of which were produced by the top-level comments and low-level comments. Word clouds (Figures 4-6) exhibit the most frequent words that represented the core elements adopted in the users' communication, including privacy, surveillance, track, watch, facial, technology, information, recognition, security, camera, and database. Regardless of the fact that such word clouds may be interpreted from several angles, the most surprising aspect is that roughly 30% of the privacy-related keywords (e.g., surveillance, track, monitor, watch, and security) developed in phase I occupied a great position in the list of the first 100 high-frequency words, which explains the large number of text rows that were retrieved during the qualitative analysis in phase II.

Figure 4. Word cloud for the speaker-generated text

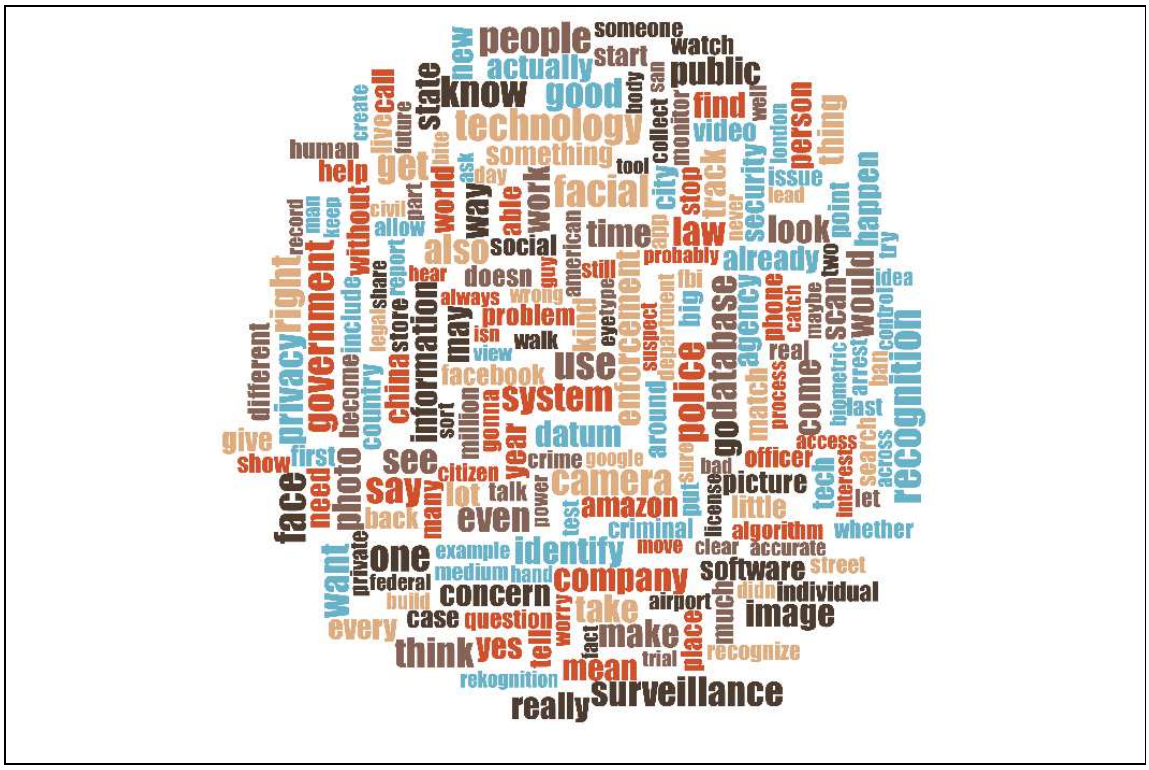


Figure 5. Word cloud for the commentator-generated text

Figure 6. Word cloud for the replier-generated text

Qualitative findings

In all, 1946 textual records (five transcripts, 1052 top-level comments, and 889 low-level comments out of five videos) were reviewed in the qualitative phase to establish a new framework of FRT-related privacy concerns. Close to 32% (613) of these held negative attitudes toward FRT, whereas others either had positive attitudes (21%) or irrelevant content (47%). From the graph below (Figure 7) we can see that the master FRT-related privacy concerns of 27.90% (171 out of 613) of the mapped texts was information collection (surveillance 16.15%, coercion 11.75%), 47.80% (293 out of 613) was information processing (retention period 6.53%, profiling 14.03%, security 10.77%, secondary use 9.62%, exclusion 6.85%), 14.36% (88 out of 613) was information dissemination (disclosure 14.36%), and 9.95% (61 out of 613) was invasions (decisional interference 9.95%). Both Table 7 and the

following subsections should paint a comprehensive image of these concerns to answer the research questions as well as to accomplish the research aim.

Figure 7. The distribution of the most common FRT-related privacy concerns in the qualitative analysis phase

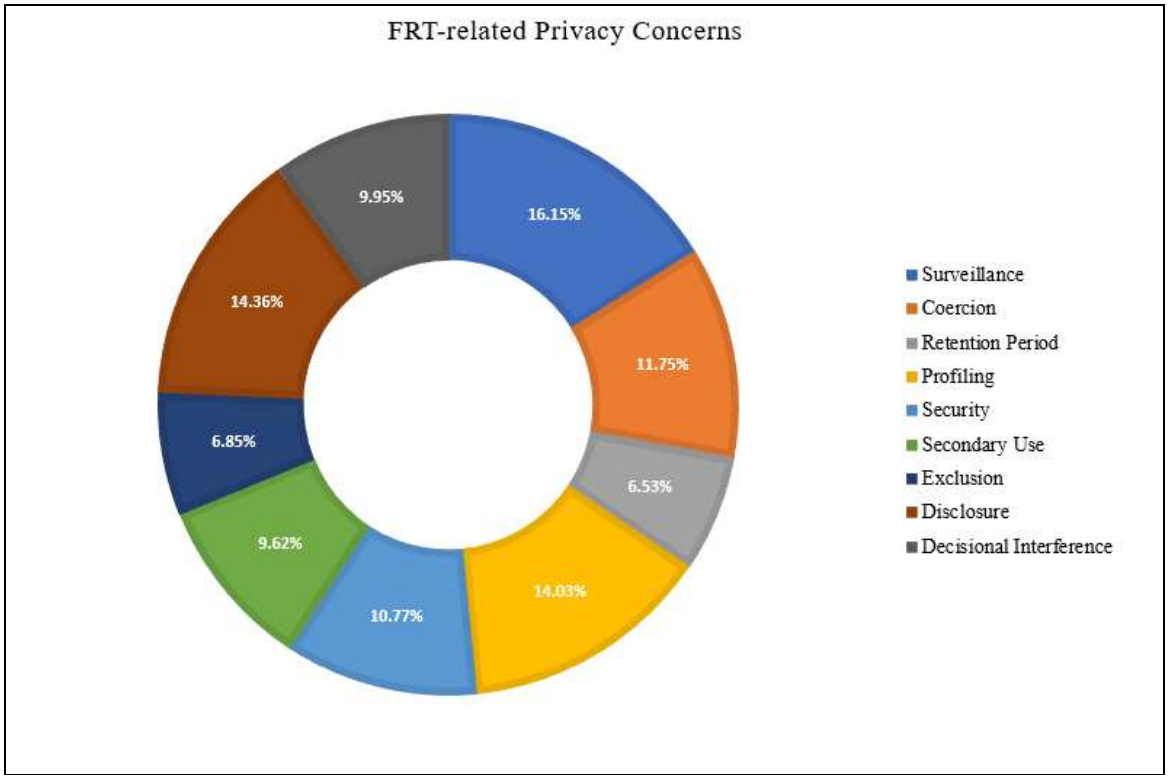


Table 7. Description of the most common FRT-related privacy concerns

Theme	Code	Description
Information collection	Surveillance	It refers to the process of recognizing personal identity via facial characteristics to keep gathering information about the users' daily activities and behaviors performed in public and private spaces without their knowledge and consent.
	Coercion	It refers to the process of recognizing personal identity via facial characteristics to keep gathering information about the users' daily activities and behaviors performed in public and private spaces with their knowledge and mandatory consent.
Information processing	Retention Period	It refers to the process of storing information that has been captured by face recognition surveillance technology in databases forever rather than destroying it within a reasonable period of time.
	Profiling	It refers to the process of acquiring stored information across multiple sources, combining it with its counterpart that has been already existed in the database, and connecting it to the users' facial characteristics to find new patterns.
	Security	It refers to the organizations' failure to take necessary measures to bridge security vulnerabilities that could contribute in obliterating the three core principles of information security: confidentiality, integrity, and availability (CIA).
	Secondary Use	It refers to the employment of legally obtained photo alongside its associated information for purposes that are out of the privacy agreement context.
	Exclusion	It refers to the prevention of personal records access upon the users' request to review obtained information in the interest of correcting misleading materials and removing the redundant, sensitive, unwanted, or entire records.
Information dissemination	Disclosure	It refers to the divulging of true, embarrassing, and/or distorted information to third parties.
Invasions	Decisional Interference	It refers to the exploitation of gathered information to model personal life in an approach that is incompatible with personal choices, interests, and values.

Information collection

Surveillance

Surveillance is a concern related to the process of recognizing personal identity via facial characteristics to keep gathering information about the users' daily activities and

behaviors performed in public and private spaces without their knowledge and consent. It was quite evident that the majority of the users were highly supportive of the implementation of FRT for surveillance and considered it a pioneer invention assisting to fight the problem of rising crimes in societies due to its capability to locate criminals within a short time compared to the traditional surveillance system. In the meantime, they were very concerned to be exploited in inappropriate methods ending up with an eternal conflict between its benefits for communities' security and the individuals' right to privacy. This worry was stemmed from their observation of the recent deployment of this instrument at every corner of the Earth, which gave an indication of stakeholders' intention to track everyone's movements rather than limiting it to the groups who were placed on watchlists.

In spite of the fact that a wide variety of negative perspectives toward face recognition surveillance technology were demonstrated during the data analysis, the behaviors with regard to surveillance notification, along with informed consent, were particularly prominent. It was fully understood that the problem of surveillance transparency began with the technological revolution and was addressed through the anonymity approach (e.g., using a pseudonym on the Internet (2)) to be de-identified during the organizational surveillance operations and have some freedom spaces. However, information about the users has become more accessible in the age of FRT, since facial features are unchangeable, and that boosted the users' concern in terms of being subject to constant surveillance in secrecy without prior permission, especially for those who live in the regions where both (informed consent and notification) privacy principles are protected by the constitution to guarantee the integrity of surveillance.

There was a prevalent conviction among those users that the application of face recognition surveillance technology has created a crisis in the right to control access to their information. As the access to a faceprint is dissimilar to other biometric identifiers—such as DNA, voiceprint, and fingerprint, which require informed consent and notification—faceprint

was alleged to have provided a great opportunity for organizations to impose a plan of massive and secret surveillance whose occurrence was impossible in the last decades because of the individuals' rejection of being under surveillance. Accordingly, the users found that the failure to fulfill the two privacy principles to the same degree should open a back door for information misuse (e.g., blackmailing to share information about shamed behaviors that were captured by hidden face recognition surveillance technology in an empty space (2)) and falsification (e.g., exploiting others' photos posted across social media to implicate them in criminal activities (3)).

Interestingly, over half of those responses explicitly mentioned that the rate of surveillance concern was much increased in public places because organizations still have a willful deficiency in realizing that privacy in public does not differ from privacy in private. Those users, including Muslim women whose faces are a private matter and not supposed to be seen by strangers in public, have been suffering for a long time from this situation. They have attempted over and over again to ask decision-makers in order to legally safeguard their privacy in public from data exploiters who believe the presence in public is like a gesture of personal approval for information collection. Nevertheless, this situation has not yet been resolved, which has caused social isolation for some. It has caused others to change their behavior and act contrary to their nature in anticipation of being identified and tracked during their daily activities.

By the same token, it was indicated that the social isolation and behavioral changes were all temporary solutions and could not play a significant role in addressing this situation. Face recognition surveillance technology in public was expected to capture sensitive activities in private even for those who literally followed strict privacy protection guidelines (e.g., being away from social media platforms (1) and not sharing information with others (3)). This has something to do with the fact that this sensor in public was not trained to determine if obtained

information was captured within the public or private scope (e.g., FRT that placed on a store's wall could record all the surrounding activities, including private activities in the home through its open windows (2)). For this reason, the idea of restricting the usage of FRT to governmental organizations under intense observation from the highest authority seemed more acceptable to them to reduce the chance of conducting activities against the privacy principles.

Some examples:

I bet it is a time to say goodbye to your privacy with deploying facial surveillance that generated more difficulty in maintaining the right to privacy and anonymity. This big brother has been designed in a method beyond our expectations. It becomes able to identify, observe, and record every single detail of activities you have performed in every second, from walking on a street to posting materials on the Internet without your knowledge and permission (1).

Several business owners have implemented FRT for public surveillance without consulting individuals, and they repeatedly announce to not open your mouth or seek privacy protection unless you are at home and not engaged in the Internet. The common ideology between them is people who participated in public have willingly chosen to give up their privacy and expose their identity to the whole world so that information about them is completely free for observation. Well, I am a conservative Muslim woman whose face is uncovered to certain groups like husband and brothers. So, this system does not just breach the privacy principles but the religious principles. (2).

Agreed! Our privacy is on its way to becoming terminated and becomes a reminiscence with FRT. We are as good citizens being monitored every day and everywhere without warning and authorization. This is not limited to the public but also includes the private. It can record you when you are in a good mood and dance in your vehicle, which is defined by law as private property. I see this technology as surveillance in public but seeking private information (3).

Coercion

Coercion is a concern related to the process of recognizing personal identity via facial characteristics to keep gathering information about the users' daily activities and behaviors performed in public and private spaces with their knowledge and mandatory consent. Even though the ultimate goal of coercion is aligned with the same purpose as a surveillance application—they both seek to hunt as much available information as possible—the users'

privacy concern surrounding coercion practices primarily concentrated on the acquisition of mandatory consent to engage in FRT more than the information collection itself. In the users' view, such harmful action has been lately adopted by a considerable number of organizations as a reaction to the high rejection that faced FRT implementation as a result of individuals' awareness of its risk to their privacy.

The main lesson the users have learned from the long history of technological inventions—this is often overlooked by privacy enemies—was that every emerged technology has its own price that must be paid by the consumers in one way or another. Paying this price does not necessarily affect the amount of money present in a personal financial repository, but it has the capacity to minimize the boundaries of information privacy protection. Their belief, therefore, was that the price for FRT is probably the restriction of personal choice in the voluntary information disclosure in favor of community security from criminal activities. This which eventually result in losing more control over access to their information and private information in particular.

In the past few years, the users have witnessed that several stakeholders, including employers, have directly forced them to get engaged in FRT for identification and surveillance; otherwise, loads of penalties and fines await them (e.g., the termination of an employment contract (2)). While direct orders are tightly tied to the entities who have power over their people, and those entities could be punishable by privacy laws, it was suggested that the right to privacy has become far worse inasmuch as organizations took another approach of coercion enabling them to avoid lawsuits as well as to dominate the majority of PII. Those institutions have started putting indirect pressure on individuals by blocking them from accessing some products and services or even basic human needs for living to involuntarily agree to provide their information (e.g., entering a grocery store requires face-scanning of the consumers for safety reasons (1)).

In light of the above, it was not that difficult to discern from the responses to this issue that society has significantly contributed to aggravating coercion-related activities, and this has been considered a dangerous factor in being able to protect information privacy. Various groups in society have been exposed to brainwashing through a loop of propaganda managed by organizations to convince them that FRT is for their society's safety, and those who are against it are simply their enemy. This pressure, hence, has negatively impacted other groups who are very often put in a position of having no choice other than relinquishing the right to privacy in exchange for being free from unfavorable accusations or suspicion. However, this phenomenon spreads on a wide scale among the population whose members look at privacy as a privilege more than a right given in limited circumstances to protect their environment from falling into security, health, and economic crisis.

Some examples:

Let us first agree that being forced to do something is without a question a big invasion of privacy. We have paid the price for FRT by mandating us to reveal our information and accept it. People who try to not comply with this order are prone to countless legal punishments. To be honest, it is not surprising to me at all because we have never had the right to decide about our privacy since 1984. But this activity should violate our privacy more than ever (1).

There is an urgent need for establishing regulations to curb activities against our privacy. It is unbelievable and unjust to consider that information disclosure is the only available key for us to get along on the new life. And I cannot imagine that products, services, and other basic life needs are all inaccessible for those who refuse to use their privacy as a commodity. Folks need to understand that the trade-off between privacy and other benefits is a myth and the balance between privacy and other benefits should be the reality (2).

Is this attack just because we have extreme privacy concerns about FRT and want to keep our privacy protected? That is why I prefer to disclose my information and use FRT at the cost of not being considered a suspect person by skeptics. As you know, skeptics are the enemy of privacy in all societies and view you as a dissenter. Their job is to keep attacking you with hurtful words, and your fault is only refusing to follow the herd and disclose your information. I do not blame them. Their minds are washed by propaganda distributed by data investors, and they always keep saying "If you have nothing to hide you have nothing to fear" (3).

Information processing

Retention period

Retention period is a concern related to the process of storing information that has been captured by face recognition surveillance technology in databases forever rather than destroying it within a reasonable period of time. There were several users paid full attention to this concern, since many organizations that put face recognition surveillance technology into practice were believed to have a great tendency to be more mysterious with their communities in connection with rules for information archiving. This ambiguity has empowered organizations to originate big datasets about individuals' activities for their own benefit (e.g., performing behavior analysis to increase annual profits (2)) without being exposed to lawsuits. This despite the fact that they have an obligation under privacy regulations in some countries (e.g., GDPR in the European area (3)) to remove information once the purpose of information collection has been accomplished.

Although roughly 18% of those users agreed that face recognition surveillance technology is anticipated to be employed for emergency cases (e.g. crime investigation (2)) without informed consent and public notification to maximize community safety, the transparency of the information storage process was one of their priorities in order to maintain relevant privacy principles (e.g., data minimization (1)). They, as information owners, were heavily interested in knowing the types of archived information, the reason for archiving the information, the duration of information archiving, the encryption used for archived information security, the confines of archived information access, and the strategies used for archived information destruction. Yet it was emphasized that information about these six factors has been Kept secret from them because of the lack of transparency in or the absence of local, regional, and global privacy laws about archival rules that gave organizations the ultimate freedom to interpret them in line with their interests.

Indeed, the long storage of past events that could prevent them from taking an equal part in their communities was the main root of this concern. Some times in their lives (e.g., teenage years (2)) were full of irresponsible adventures, the of which majority were against either social or legal norms. The consequences of those activities were not dire (e.g., temporary social ostracism (3)) as it is rare that information about such actions survives in human memory for a long time, especially when those who were pariahs rebuilt a good reputation for themselves. In this way, searching for information about past events to be exploited in the present time (e.g., criminalizing individuals for past activities that were legal in the past and illegal in the present (2) or threatening individuals to disclose shamed activities in the past (2)) was harder compared to the age of FRT, where the availability of records is wider and not manipulated by the time.

Some examples:

It becomes normal to find out that our information has been gathered in unpermitted ways with the deployment of FRT across several countries, and Western countries in particular. But one day you will be shocked when you find out that all information about you, your family, your relatives, and your friends is kept forever. This means the past activities you have done since your birth are archived and visible to everyone who has access to these records (1).

I just want to laugh at you if ever think narcissistic organizations are respectful and going to ask for permission before storing your information. Well, this is the main goal of running FRT and tracking you 24/7. They want to build billions of long-term records about you and me to track changeable and unchangeable activities over our lifetime. They took advantage of weak privacy laws to do such things. So you need to wake up; your good intention alone is not enough (2).

Because of privacy laws like GDPR and CCPA, everyone might lately notice companies who have applied FRT are required to make their customers and visitors know they are under surveillance via warning signs on buildings or pop-up online notifications, but how about their transparency with their consumers about archival rules like what information or how long it will be stored? It is zero and it is intentional behavior to not fall into legal problems (3)

Profiling

Profiling is a concern related to the process of acquiring stored information across multiple sources, combining it with its counterpart that already exists in the database, and connecting it to the users' facial characteristics to find new patterns. There might be a great similarity between profiling-related concerns and surveillance-related concerns in terms of information identification and collection. The central difference is that surveillance seeks to obtain nonexistent information through face recognition surveillance technology, while profiling is more advanced, focusing on the aggregation of information that has been already gathered through face recognition surveillance technology and other approaches (e.g., smartphone apps (2)) to be placed in one database and linked to a personal face for classification, prediction, etc. As confirmed by the users, the emergence and adoption of this technique have been motivated by organizations' realization that restricting information collection to a single method would not paint an extensive picture about personal life.

Those who commented on this concern generally had high confidence in reporting that profiling is not a novel norm but has been moved forward. Several organizations have for a long period of time commenced to produce personal profiles in a traditional mechanism, binding combined information with a real identity (e.g., social security number (2)) that has a limited piece of information about them or with a digital identity (e.g., email (3)) that is changeable or removable in order to start from scratch. In many instances, this information is quite hard to be aggregated in one spot because there is no relationship between the real and digital identity as well as the users' capability to complete daily transactions without needing to use such identities. Yet the power of profiling has been significantly shifted with FRT, where all human-generated information is captured, aggregated, and linked in less than a second through a single image of a targeted individual.

In the review of their communication to get a better understanding of the privacy threats caused by profiling, it turned out that the strength or weakness of the users' privacy is measured by the amount of information others know. A preponderance of those concerned users always strived for following the concept of contextual information—the amount and types about disclosed information are determined by the context—during the decision-making of information sharing to prevent intrusive groups from getting involved in the deep details of their lives (e.g., allowing bankers to access information about a financial situation to issue a credit card but not information about personal purchases (3)). The unfortunate thing was that profiling has created an unhealthy environment for their right to privacy by putting all collected information in a single database, leaving stakeholders able to access contextual and non-contextual information as a means to uncover hidden patterns that users preferred be unknown.

Based on that, healthcare insurance organizations were frequently mentioned as a real example of this breach and its effects. Some of these institutions have applied FRT for public surveillance to track their patients' daily behaviors on the Internet, synthesize this information with the patients' health information that existed in the database, and tied it to facial characteristics. The objective of this movement is to draw an obvious picture of the users' lives and divide them based on their given score into a healthy group (e.g., those who get an annual blood test, frequently go to the gym, and sleep early (3)) and an unhealthy group (e.g., those who seldom get an annual blood test, prefer eating from fast-food restaurants, and sleep late (3)). These score systems, often called Social Credit Systems (SCSs), would increase or decrease the price paid for a health insurance plan or even cancel it.

With the massive application of SCSs to all areas of life, the problem of racial profiling was predicted to grow much more in the next few years, leading to privacy-related disparate treatment between individuals in the same society. In particular, the users threw a light on communities consisting of multi-ethnic groups that vary radically in their characteristics,

religions, traditions, etc. When a few members from one of those groups adopt a behavior that is unacceptable by other groups, such as the majority party, or understood in an way opposite of the intended meaning (e.g., the cultural difference (3)), it is possible to classify it as suspicious behavior and tie this classification to all members belonging to this group. This classification was considered a means of encouraging organizations to invade information privacy for this group through undergoing further investigation (e.g., asking black people to disclose more information than other races for education loans (2)).

Some examples:

If you think FRT is limited to recording your everyday movements, you probably need to rethink this. Health insurance companies, for example, are interested in constructing a digital profile for you to know more than you know about yourself. It does not mean anything to them if you pay your bill for your insurance plan, but they want to combine this with the data they gathered by FRT like who you associate with, how many times you go to the gym in a week, and how many times you do a blood check in a year to decide whether or not you are eligible for the minimum price they are offering to consumers (1).

Profiling has increased discrimination between people. This profiling is so different from traditional profiling that exceeds the basic information we voluntarily submitted to them. Profiling with FRT means to aggregate and link all activities we conducted in different places to decide whether we are good or bad people. But the real issue here is how about if the decision is made based on an incorrect understanding (2)?

I have been working for a car dealer as a profiler for over 5 years. The nature of my current job is to run FRT against the Internet to scrape as much information as possible about applicants who seek a car loan and combine it with the information they have already provided. The applications of some people who belong to groups that are not found behaving and believing in line with our desires are put on hold, and they get more investigation even if their financial status is equal to others. I know it is like racial profiling, but this is the new lifestyle (3).

Security

Security is a concern related to organizations' failure to take necessary measures to bridge security vulnerabilities that could contribute to obliterating the three core principles of information security: confidentiality, integrity, and availability (CIA). According to the users,

maintaining the principles of information security has become a noticeable challenge encountering FRT, which boosted their rejection of the system due to the overlap between information security and information privacy in terms of unauthorized access. The prime source of this problem was believed to be a flaw in the identification accuracy rate that makes the system unqualified to locate, map, extract, and match the users' facial features in the correct way. As a consequence, the strong feeling was that the misidentification in the system would offer a suitable environment for identity theft instead of improving the information protection mechanisms.

The users' comparison of the kinds of information security flaws gave an indication the problem of a false-negative match—that is, the inability to recognize a face template that has been already inputted into a database—is quite acceptable compared to the occurrence of a false-positive match—that is, identifying an individual as another person—because of its negligible damages to information privacy. It was a unified opinion that there has been a moral crisis in FRT algorithms development that drove to witness a growth in the rate of the false positive match issue. FRT algorithms are usually constructed based on the majority groups' photos to lower the false positive match rate as far as possible. Minority groups (e.g., dark females and twin brothers (1)), on this account, are the demographic whose records have a much greater opportunity for unauthorized access, which might end up with the accusation of innocent groups and, in some circumstances, unjust arrest.

On the other hand, a few of those users supposed that training FRT algorithms with a massive corpus of the majority and minority groups' photos would not address unauthorized access issues because of the system's inability to detect identity theft. The current availability of personal profiles, especially in the era of social networking sites, which contain images and identifiable information, has exposed the users' privacy to be hostage to hackers and data exploiters who could access, falsify, disclose, blackmail, and perpetrate other harmful

behaviors against their records. These behaviors may be carried out through various patterns, but a spoofing attack through the production of a 3D mask face, a simulated mask to the targeted person's face, was their biggest fear, since they have no control over information that has been shared on the Internet or stored across organization databases.

Some examples:

When it comes to privacy, it is not reasonable to only focus on surveillance or similar problems, but the thing we should shed a light on is system accuracy. FRT sometimes fails to correctly recognize people regardless of whether this happened by pure chance or intentionally. So this flaw could result in illegal access to information, accusations of innocent people, discrimination against minorities, and so on (1).

Security in FRT is a joke we hear all the time but are not able to see reality. There are many skilled people who can develop a face mask for you or use your image to access your data or get you involved in legal problems. For example, two police officers knocked on my door last year because of a theft that occurred in the company I work for and told me the robber made a fake mask of my face and used it to access the facility (2).

You may forget to mention also how many organizations have fooled us for a long time and keep saying FRT is such an accurate and unique system for identification. I believe they failed to remember that the system has been developed and operated by human beings who are subject to committing many mistakes caused by racism or a lack of skills. If they are pretty sure of the accuracy rate, let them examine it on twin brothers and watch their facial expressions after the result (3).

Secondary use

Secondary use is a concern related to the employment of a legally obtained photo alongside its associated information (e.g., full name, age, and address) for purposes that are out of the privacy agreement context, whether the privacy agreement is in a written or a verbal form. In general terms, voluntary information disclosure has been a common behavior in the users' daily lives for an extended period of time for various purposes (e.g., meeting organizations' requirements or sharing happy moments with others (1)). The voluntary information disclosure has ever been accompanied by their expectation of privacy protection

against secondary use activities under legal norms (e.g., disclosing a personal photo for the issuance of an employee ID under an employer's privacy policy that prevents secondary use behaviors (3)). But it seemed that the expectation of privacy is outdated in the light of organizations' constant desires to get the full benefits of disclosed information.

The users clarified that the decision-making around voluntary information disclosure relies on the comprehensive evaluation of a privacy agreement template that is sometimes derived from the national constitution to predict the chance of privacy violations. One of the significant elements of the evaluation process affecting the users' privacy protection belief and intention of information disclosure was the extent of privacy protection against the secondary use occurrence. If the adopted privacy protection protocol took this practice into account, they likely had no privacy risk belief related to sharing their information with other parties and vice versa. The largest part of those templates, unfortunately, was viewed as a trap allowing organizations to dominate and manipulate acquired information in ways that serve organizations' trends and breach the users' privacy (e.g., using photos on social media profiles for identification, tracking, profiling, and profit gain (1)).

In a deep dive into this point, it was detected that the absence of transparency in the privacy agreement template has been the strategy that most complicated the protection of their right to privacy and prevented them from filing lawsuits against secondary use-related activities. As organizations have realized that some activities perhaps clash with the social value of privacy, they intentionally have prepared privacy agreement templates in language so tricky that the general users are not in a position to recognize what legal and illegal practices lie within this agreement (e.g., collected information might be subject to the future usage for other purposes if considered necessary without the users' notification and consent (2)). And the users' acceptance of such unclear agreements should give a legal excuse for service providers to perform unlimited activities exceeding the boundary of expected norms of privacy (e.g.,

selling information and updating the whole privacy policy without informed consent and notification (3)).

It is important to bear in mind that preventing the occurrence of particular activities after accepting a privacy agreement has not always been an available choice to the users, which was considered a deprivation of an acquired right. The users' interpretation for this situation was categorically linked to the unsuitable ideology followed by several organizations that the retention for information ownership right ends with the voluntary information disclosure, ignoring the personal right in the continuity of control over the published information. Given this point, light was shed on the influence of this ideology on privacy of individuals who their social values, which represent the main factor directing the development process of a privacy agreement template, differ from those of service providers. Those users reckoned that the organizations' failure to communicate with the information owner to ensure that planned activities are not against some individuals' social norms would cross the line of the fair use principle for their information.

Some examples:

There is of course no problem with FRT itself, the problem is whether or not photos are used with personal authorization and knowledge. It has been proven in different contexts that some photos employed for FRT were permitted for other purposes. So the usage span must be clear to consumers the privacy agreement is not a fraudulent document seeking to exploit information (1).

It does not matter if people did or did not read the privacy policy before deciding to disclose information. Almost all privacy policies have been designed in a biased manner that is far from our expected social or legal norms of privacy; they have been designed to protect organizations from lawsuits rather than maintaining privacy principles. Look at Snapchat, Twitter, and other enterprises that depend on pictures and videos. They use the information to train the system to identify their consumers. But they do not clearly state that in their privacy policy (2).

We all know that our photos and other personal information are already stored in a database under an agreement between us and service providers. But you can not ensure

this information will never use in ways we have not given permission for or against our social norms. Try to reread any privacy policy you signed, and you should find terms like necessary access, retrieval, disclosure, and use without your permission. You might be surprised, but this is normal because companies do not acknowledge the right to control over disclosed information (3).

Exclusion

Exclusion is a concern related to the prevention of personal records access upon the users' request to review obtained information in the interest of correcting misleading materials and removing the redundant, sensitive, unwanted, or entire records. Although the difference between the exclusion-related concerns and the retention period-related concerns is not simple to be identified in several contexts, the users' central point in the exclusion-related concerns was the involvement in the decision-making process about information stored on organizations servers rather than being informed of the information retention period to get more control over their published information. The users gave the impression of being completely aware of the fact that the information collection, whether or not it has been legally performed, is no longer a secret process, but denied access to personal records has framed a notable burden on their information privacy safeguard with the possibility of gathering private information that presumed to not be shared with others, fake information during fraud operations (e.g., spoofing attacks (3)), or false information during false matches.

Based on their long-time experiences, it was concluded that information privacy has reached a critical stage and become an inaccessible source for the majority due to the variation in responding mechanisms to the record access requests. Myriad organizations in recent years have sought to construct unbridgeable challenges in front of the users as a means to push them withdrawing their record access requests through unlimited approaches (e.g., requesting huge cash in exchange for the record access or signing on the record access waiver form before getting products (2)). This movement, hence, proved to the users the ploy adopted by those

institutions to minimize their accountability to legal authorities at the lowest level since the allowed access to records may unmask privacy infringements or privacy-related security breaches conducted behind the scene (e.g., scraping information without personal knowledge and consent (2)) which entitles the injured parties to begin filing lawsuits against the privacy violators.

Even though a limited number of organizations have by default granted the full features of personal records including the accessibility, controlling all acquired information appeared a dream with the selective information behavior. The users held an extremely pessimistic belief of making every single data row available upon request in view of their perception of institutions' capability to narrow information range by generating external records, consisting of information legally collected, for their clients' access along with internal records, consisting of information legally and illegally collected, for their own staffs' access. The worst side of the story, however, was that there is no guarantee for permanently information modification or removal as it is uphill to ensure if those actions apply as well to the same information that existed in external records, track partners who have a copy of this information, or even exclude this information from being regathered in the future.

Some examples:

All we need is justice to exercise our right to have control over information that we have missed for decades. It is understood that organizations have the right to implement FRT in some cases, but they also have a legal obligation to let us access our records to know what they know about us and decide what appropriate information can be kept in those records. Not doing this is a privacy breach without question because stored data is basically our property (1).

This is nothing new; it is human nature g to get a preconceived idea of what others know about you to draw the boundaries of any future relationship. But gaining access to your records to review what information was captured by FRT seems an impossible task, one with lots of obstacles organizations prepared for you once you intend to request this so as to not expose their lies about not gathering data without informed consent (2).

You better remember this is not limited to access blocking. You will not even able to figure out how many networks have a copy of your records. If you could do that, then congrats and be ready for the next phases where your access is limited to a basic database including information disclosed with your permission, not the hidden database. And guess what, it is not your prerogative to remove any information. (3).

Information dissemination

Disclosure

Disclosure is a concern related to the divulging of true, embarrassing, and/or distorted information to third parties for a variety of aims, including profits growth and the destruction of personal reputation to isolate targeted groups from their society. By this description, it is apparent that there is a relationship between the disclosure-related concerns and the security-related concerns, as both categories were interested in arguing against the unauthorized expansion of the circle of records access. The variation, however, is that the security-related concerns were motived by low technical attention, while the disclosure-related concerns were motived by low organizational integrity with regard to the information confidentiality principle. That does not mean the moral dimension of organizations is not required to overcome the security-related concerns, as already pointed out, but not always the case in comparison with the disclosure-related concerns.

A closer investigation established that the users who engaged in the disclosure-related concerns were in complete disagreement with those who had the secondary use-related concerns. Their uniform outlook was that the relationship between them and organizations is often governed by privacy protection trust and not by a detailed privacy agreement, given that the majority of information currently stored has been illegally acquired. Once a particular entity has been surrounded by a great reputation in the information market, it unquestionably minimizes their privacy anxieties about information disclosure. In this vein, the well-known Facebook–Cambridge Analytica data scandal was brought to the table as a realistic example

supporting their hypothesis that the existence of a detailed privacy agreement without complying with ethical obligations imposed by human and social values has nothing to do with the weight of privacy protection.

Notwithstanding the fact that the users' disclosure-related concerns were reported differently concerning situations where organizations have exploited advanced instruments, available chances, acquired power, and privacy lawlessness to get information revealed, much attention was paid to the leakage of collected photos to other networks. The basis of this traced back to the users' awareness of the structure of the deep learning algorithms used for the development of FRT that make the distinguishing between nonidentical objects from the same sort impossible if those algorithms have not been fed with a massive set of photos for a targeted item. And since the amount of current photos that existed in databases (e.g., DMV (1)) was detected as not sufficient to meet this need, there was an implicit allusion repeatedly raised in the users' conversations to signal a foreseeable increase in private communication loops between allied organizations and data brokers in the era of FRT to improve its identification accuracy.

Surprisingly, the disclosure of the photos was not considered a form of confidentiality violations in the other users' sight as long as photos are shared with their consent to benefit the community (e.g., medical research to find common patterns among cancer patients (3)). Their paramount concerns, rather, revolved around the exposure of gathered information about their activities, including true, embarrassing, and distorted information, to public and nonpublic spaces with the ease of access to human-generated information through face recognition surveillance technology that suffers from security vulnerabilities. It was claimed that everyone on the planet has an equal chance to experience changes in emotions, behavior, opinions, etc., from a day to another or to get falsification in their records by hackers (e.g., deepfake technology (3)). Leaving such information available to other parties without regard to its

sensitivity and reliability, consequently, would contribute to destroying the users' reputation or drawing a picture contrary to the reality, leading to social discrimination and isolation.

Some examples:

I would say it becomes possible these days to find out that consumers' information has been shared with third parties. Companies, especially those known as data brokers or at least deal with data brokers, seem very aware of the impact of data sharing on annual revenue. So FRT should provide a new opportunity to grow their profits through selling consumers' photos to those who implement the system. This behavior will, unfortunately, will be standard practice for the next decades unless there is a new privacy law (1).

This technology basically works like the human brain that needs repetition to be able to distinguish between two different things in the same class, like gender. Agencies have been always interested in reaching this point by training the system with a couple of billion people's photos to make FRT under service. This means the creation of a shared dataset between organizations is likely to happen to increase the identification accuracy (2).

Information disclosure behaviors, without doubt, must be immediately stopped for society's privacy protection. But we have to be a little bit fair and acknowledge that industry competitions, in general, would not exist if particular information is not shared. I am not here encouraging companies to develop the industry based on sensitive or fake information or even true information about our behavior that we have not agreed for but basic information, like photos, with our consent to support the wheels of industry (3).

Invasions

Decisional interference

Decisional interference is a concern related to the exploitation of gathered information to model personal life in an approach that is incompatible with personal choices, interests, and values. To put the matter in a straightforward way, decisional interference is the use of sensitive information about personal behaviors that has been already inserted into databases, including shaming and private information, as a weapon to put pressure on its owners in order to let other groups control their private affairs. The analysis revealed that decisional interference-related

concerns were frequently mentioned by the users as a form of coercion, as both coercion-related behaviors and decisional interference-related behaviors are directly linked to others' influences in the personal decision-making process. However, the major frame of their debate was about the post-information collection phase, not the pre-information collection phase.

Considering the risks surrounding the system, such as the high availability of information and the existence of security vulnerabilities, it was summarized that decisional interference-related behaviors would turn out to be a phenomenon on a large scale to serve others' desires. In the users' threads, the majority emphasized that FRT has brought a unique direction of privacy boundaries through shifting the control over personal life from one party to another to oppress and enslave several groups. Some of them admitted their heavy weakness in front of blackmailers whose power is derived from the possession of others' records, that consist of private activities or activities against social and legal norms (e.g., blackmailing individuals by hackers or data collectors to get involved in a dangerous or shamed actions in exchange for not disclosing to the public their records about an intimate relationship captured by hidden face recognition surveillance technology (3)).

At the same time, other users called attention to indirect decisional interference-related behaviors that represent equally important to direct decisional interference-related behaviors. Organizations were anticipated to increase the application of selective attention mechanisms to facilitate the process of human mind control (e.g., the continuous flow of advertisements to persuade society about a particular topic against some values (2)). This is in view of the fact that the identification of personal choices, opinions, attitudes, etc., is not a complicated task with the emergence of profiling that relies on facial features. These behaviors, unfortunately, sometimes comprise an intrusion into personal isolation (e.g., pop-up advertisements while watching a movie (2)). All types of indirect decisional interference-related behaviors were

believed to generate repressive and slave societies where individuals are unable to exercise their right to personal decision-making, which is guaranteed by numerous privacy laws.

Some examples:

If there is a way to ensure that FRT is used in appropriate ways, I then agree with others who believe the goal of its diffusion is for our security. But all events surroundings us show opposite things and confirm that we are delusional if we think this way. Using systems like the social credit system to evaluate citizens based on some values adopted by organizations would enslave the entire society. Groups who have different values and beliefs will absolutely suffer and have to change them in exchange for receiving a good credit score (1).

I think FRT has created a great environment for blackmailers, since everyone has a weakness. I've heard too many stories about people whose lives have been controlled by blackmailers because of some sensitive information. A friend of my brother for example was identified by FRT betraying his wife with another girl. The person who worked behind the system on that day was his neighbor. You can imagine how he has become a slave to the neighbor since then to not have that information exposed to his wife (2).

Well, tell me how companies know all places I visited one day and got so many advertisements about those places to post positive reviews. Please do not say through GPS, because my family and I have never taken our smart devices with us. If you have no answer, it is all about surveillance by FRT to get to know everything about you and design your life as they wish. Is not that an invasion of privacy, trying to control people's minds and decisions? (3)

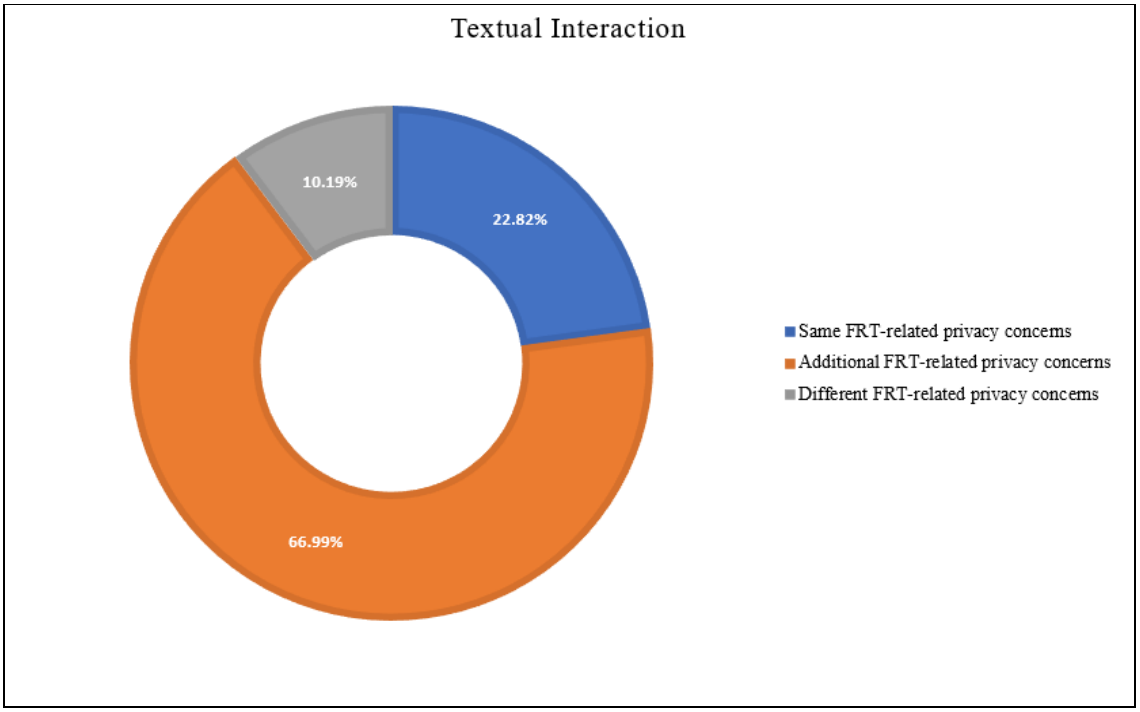
Quantitative findings

A total of 198,833 user-generated text, composed of 206 video transcripts, 123,301 top-level comments, and 75,326 low-level comments, were analyzed in an automated pattern to generalize the above findings. The classifier that was developed through the SVM algorithm successfully captured and distributed 94,379 (47.47%) out of 198,833 user-generated text into the nine predefined categories. The classified corpus was extracted from 206 (100%) out of 206 video transcripts, 48606 (39.42%) out of 123,301 top-level comments, and 45567 (60.49%) out of 75,326 low-level comments. It is important to stress that this does not necessarily mean

other unclassified records held positive attitudes toward FRT, but it might be connected to other sources such as non-English, duplicate, irrelevant, and non-contextual content (e.g., smartphone-related privacy concerns), or even misidentification, as indicated earlier that the classifier accuracy was not 100%.

In a general sense, the initial statistical analysis (Figure 8) suggested that sticking to discussed FRT-related privacy concerns by speakers was not the users' preferred choice in dozens of videos. There were 47 (22.82%) out of 206 videos in which speakers, commentators, and repliers shared the same FRT-related privacy concerns; 138 (66.99%) videos in which commentators and repliers took speakers' FRT-related privacy concerns into consideration alongside other FRT-related privacy concerns; and 21 (10.19%) videos in which commentators and repliers did not touch on any of speakers' FRT-related privacy concerns. At any rate, it was noted that repliers (62%) practiced this behavior more than commentators (36%) owing to the fact that approximately 95% out of 47 videos had no or less than 10 low-level-comments, while 84% out of 138 videos and 79% out of 21 videos had at least 300 low-level comments.

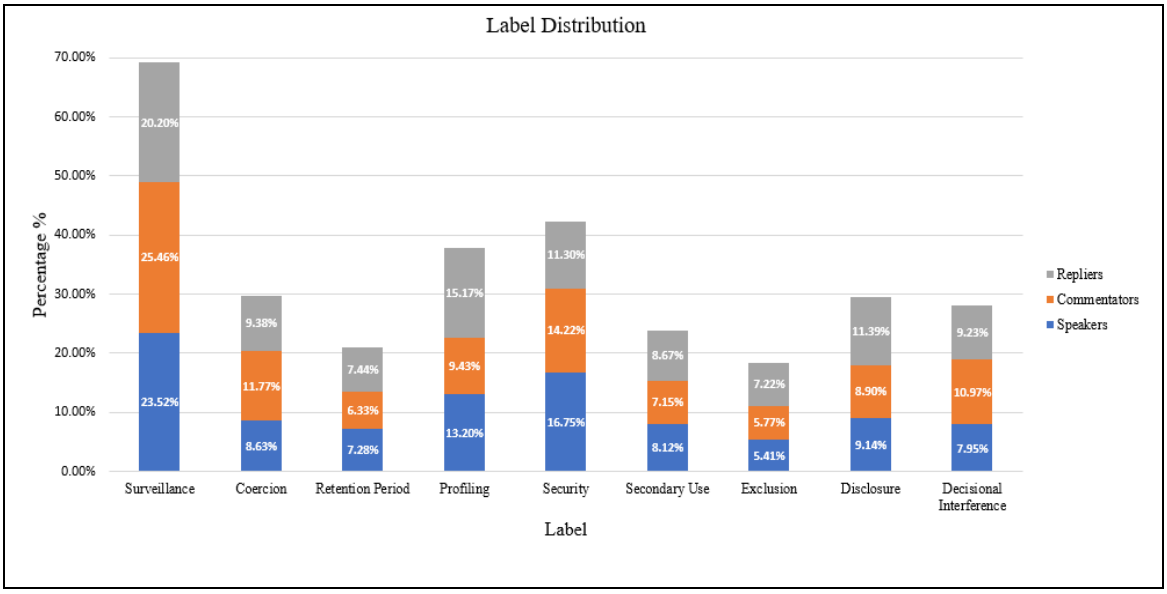
Figure 8. The flow of user-generated text



As can be seen in Figure 9, surveillance-related concerns received the majority of the users' attention (23.52% out of 591 as the sum of FRT-related privacy concerns mentioned in video transcripts, 25.46% out of 57,029 in top-level comments, 20.20% out of 48,654 in low-level comments). This was followed by the occurrence of security-related concerns (16.75% in video transcripts, 14.22% in top-level comments, 11.30% in low-level comments), profiling-related concerns (13.20% in video transcripts, 9.43% in top-level comments, 15.17% in low-level comments), coercion-related concerns (8.63% in video transcripts, 11.77% in top-level comments, 9.38% in low-level comments), disclosure-related concerns (9.14% in video transcripts, 8.90% in top-level comments, 11.39% in low-level comments), decisional interference-related concerns (7.95% in video transcripts, 10.97% in top-level comments, 9.23% in low-level comments), secondary use-related concerns (8.12% in video transcripts, 7.15% in top-level comments, 8.67% in low-level comments), retention period-related concerns (7.28% in video transcripts, 6.33% in top-level comments, 7.44% in low-level

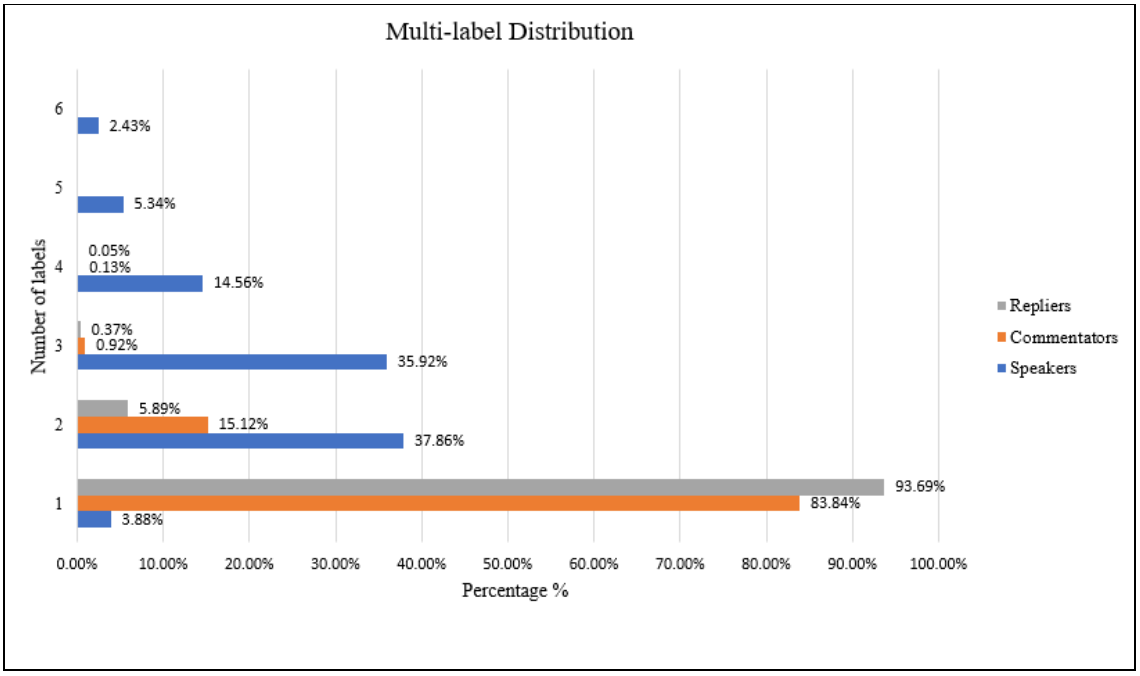
comments), and exclusion-related concerns (5.41% in video transcripts, 5.77% in top-level comments, 7.22% in low-level comments).

Figure 9. The distribution of the most common FRT-related privacy concerns in the quantitative analysis phase



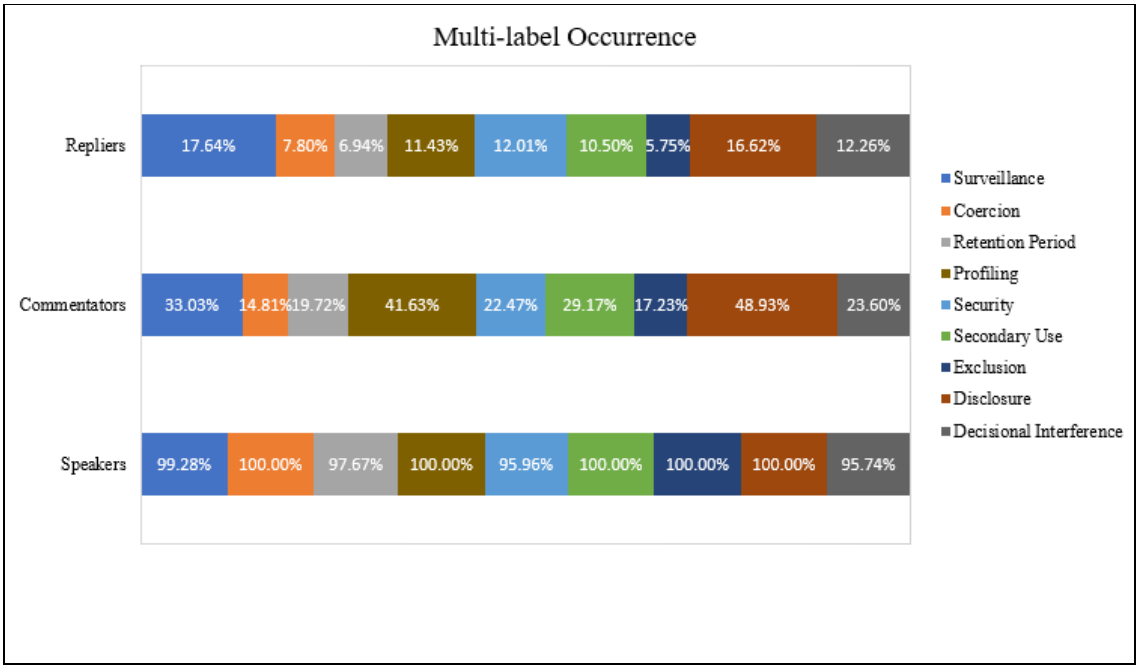
In Figure 10, it is obvious that the number of FRT-related privacy concerns in the same record was totally different among the users. There were 198 (96.12%) out of 206 speakers had multiple FRT-related privacy concerns; 78 (37.86%) out of 206 videos had two FRT-related privacy concerns, 74 (35.92%) had three FRT-related privacy concerns, 30 (14.56%) had four FRT-related privacy concerns, 11 (5.34%) had five FRT-related privacy concerns, and five (2.43%) had six FRT-related privacy concerns. The larger number of commentators and repliers, on the other side, tended to not raise more than a single FRT-related privacy concern in many cases; only 7855 (16.16%) out of 48606 top-level comments and 2874 (6.31%) out of 45567 low-level comments had multiple FRT-related privacy concerns. That is not surprising due to the vast variance between the limitation of video length (15 minutes) and comment characters (500 characters), which made the bulk of commentators and repliers not free to express about more than one FRT-related privacy concern.

Figure 10. The rate of single and multiple FRT-related privacy concerns raised in the user-generated text



Further statistical analysis was conducted in an attempt to detect if there was a particular FRT-related privacy concern constantly joining other FRT-related privacy concerns rather than being alone. Figure 11 offered a piece of evidence confirming that all FRT-related privacy concerns that emerged from video transcripts had almost a high and an equal chance (over 95%) to come into view with other FRT-related privacy concerns. Yet the chance of all FRT-related privacy concerns emerging from top- and low-level comments to accompany other FRT-related privacy concerns was fewer than 50%. For example, surveillance-related concerns (33.03%), profiling-related concerns (41.63%), and disclosure-related concerns (48.93%) were the top three privacy concerns in top-level comments, and surveillance-related concerns (17.64%), disclosure-related concerns (16.62%), and decisional interference-related concerns (12.26%) were the top three privacy concerns in low-level comments.

Figure 11. The dependency rate of particular FRT-related privacy concerns on others



Note. the dependency rate = the sum of the occurrence of particular FRT-related privacy concern with others/the sum of the frequency of such FRT-related privacy concern

In order to get a better understanding of what the most common FRT-related privacy concerns come with each other, the co-occurrence analysis for multi-label was applied to records that were sorted into multiple FRT-related privacy concerns to identify the appearance rate of two FRT-related privacy concerns in one row. What is striking about the data in the co-occurrence matrix (Table 8-10) is that the generality of FRT-related privacy concerns that co-occurred with surveillance-related concerns got the highest percentage among the users. For example, the co-occurrence of surveillance-related concerns and profiling-related concerns was 25.25% out of 198 video transcripts, 15.44% out of 7855 top-level comments, and 16.11% out of 2874 low-level comments. The co-occurrence rate of other FRT-related privacy concerns such as secondary use-related concerns with decisional interference-related concerns (3.54% in video transcripts and 0% in top-and-low-level comments) was very rare by virtue of the slight relationship between them.

Another key point in the co-occurrence matrices is that the overall rate of the co-occurrence of FRT-related privacy concerns in top-and low-level comments was similar, in contrast to video transcripts. As an illustration, the co-occurrence rate of coercion-related concerns and disclosure-related concerns, security-related concerns and profiling-related concerns, and retention period-related concerns and decisional interference-related concerns in video transcripts was three times larger than its counterpart in top- and low-level comments, whereas the difference between top-level comments and low-level comments was in the region of 0.05%. The potential interpretation of the similar co-occurrence rate is the dissimilarity in the flow of the users' communication. In other words, the opportunity for commentators and repliers to directly communicate with speakers about FRT-related privacy concerns is low, particularly for videos that were published by other than speakers, in comparison with the rate of direct communication between commentators and repliers that minimize the difference rate between them.

Table 8. The co-occurrence matrix for multi-labels in video transcripts

	Surveillance	**Coercion**	**Retention Period**	**Profiling**	**Security**	**Secondary Use**	**Exclusion**	**Disclosure**	**Decisional Interference**
Surveillance	100.00%	16.16%	13.13%	25.25%	27.27%	20.71%	10.61%	17.68%	13.13%
Coercion	16.16%	100.00%	6.57%	10.61%	13.64%	5.05%	6.06%	3.03%	4.04%
Retention Period	13.13%	6.57%	100.00%	7.58%	11.62%	5.05%	3.54%	3.54%	3.03%
Profiling	25.25%	10.61%	7.58%	100.00%	18.69%	9.60%	7.58%	6.57%	8.08%
Security	27.27%	13.64%	11.62%	18.69%	100.00%	9.09%	9.60%	12.63%	5.05%
Secondary Use	20.71%	5.05%	5.05%	9.60%	9.09%	100.00%	5.05%	3.54%	3.54%
Exclusion	10.61%	6.06%	3.54%	7.58%	9.60%	5.05%	100.00%	0.51%	3.54%
Disclosure	17.17%	3.03%	3.54%	6.57%	12.63%	3.54%	0.51%	100.00%	5.56%
Decisional Interference	13.13%	4.04%	3.03%	8.08%	5.05%	3.54%	3.54%	5.56%	100.00%

Note. the appearance rate = the sum of the occurrence of two FRT-related privacy concerns with each other / the sum of text rows had multiple FRT-related privacy concerns

Table 9. The co-occurrence matrix for multi-labels in top-level comments

	Surveillance	**Coercion**	**Retention Period**	**Profiling**	**Security**	**Secondary Use**	**Exclusion**	**Disclosure**	**Decisional Interference**
Surveillance	100.00%	4.29%	1.76%	15.44%	13.52%	4.86%	1.57%	14.25%	11.78%
Coercion	4.29%	100.00%	0.11%	3.09%	1.94%	2.37%	0.00%	0.81%	1.54%
Retention Period	1.76%	0.11%	100.00%	0.00%	1.17%	1.92%	2.93%	2.74%	0.00%
Profiling	15.44%	3.09%	0.00%	100.00%	0.81%	1.48%	0.41%	7.93%	3.46%
Security	13.52%	1.94%	1.17%	0.81%	100.00%	0.04%	0.01%	5.33%	1.91%
Secondary Use	4.86%	2.37%	1.92%	1.48%	0.04%	100.00%	2.22%	5.30%	0.00%
Exclusion	1.57%	0.00%	2.93%	0.41%	0.01%	2.22%	100.00%	0.14%	0.00%
Disclosure	14.25%	0.81%	2.74%	7.93%	5.33%	5.30%	0.14%	100.00%	0.11%
Decisional Interference	11.78%	1.54%	0.00%	3.46%	1.91%	0.00%	0.00%	0.11%	100.00%

Note. the appearance rate = the sum of the occurrence of two FRT-related privacy concerns with each other / the sum of text rows had multiple FRT-related privacy concerns

Table 10. The co-occurrence matrix for multi-labels in low-level comments

	Surveillance	Coercion	Retention Period	Profiling	Security	Secondary Use	Exclusion	Disclosure	Decisional Interference
Surveillance	100.00%	3.69%	1.60%	16.11%	13.43%	4.80%	1.53%	14.37%	11.41%
Coercion	3.69%	100.00%	0.00%	3.06%	1.74%	2.37%	0.00%	0.87%	2.26%
Retention Period	1.60%	0.00%	100.00%	0.00%	1.01%	1.98%	2.82%	2.82%	0.03%
Profiling	16.11%	3.06%	0.00%	100.00%	0.80%	1.60%	0.38%	8.18%	3.48%
Security	13.43%	1.74%	1.01%	0.80%	100.00%	0.07%	0.00%	5.43%	2.02%
Secondary Use	4.80%	2.37%	1.98%	1.60%	0.07%	100.00%	2.30%	5.39%	0.00%
Exclusion	1.53%	0.00%	2.82%	0.38%	0.00%	2.30%	100.00%	0.00%	0.00%
Disclosure	14.37%	0.87%	2.82%	8.18%	5.43%	5.39%	0.00%	100.00%	0.03%
Decisional Interference	11.41%	2.26%	0.03%	3.48%	2.02%	0.00%	0.00%	0.03%	100.00%

Note. the appearance rate = the sum of the occurrence of two FRT-related privacy concerns with each other / the sum of text rows had multiple FRT-related privacy concerns

Chapter Summary

The engagement in FRT-related discussions witnessed high growth in 2019 and 2020 compared to prior years (2014-2018). The sequential analysis of the user-generated text (206 video transcripts, 123301 top-level comments, and 75326 low-level comments) revealed that what has motivated the users' privacy risk belief in FRT lies in nine different dimensions (e.g., surveillance, profiling, disclosure, and decisional interference). Although the majority (66.99%) of the flow of commentator-generated text and replier-generated text is not in exact line with the flow of the speaker-generated text as explained in Figure 8, surveillance-related concerns were the apex of FRT-related privacy concerns among speakers, commentators, and repliers in both the quantitative and qualitative analysis phase.

Furthermore, it was evident that not all user-generated text contains greater than one FRT-related privacy concern. Speakers had more tendency to bring to light multiple FRT-related privacy concerns in their discussion, whereas commentators and replies were interested

in conversing about a single FRT-related privacy concern. For example, 100% of profiling-related concerns and disclosure-related concerns mentioned in the speaker-generated text were accompanied by other FRT-related privacy concerns. The co-occurrence analysis showed that surveillance-related concerns and security-related concerns represented the most frequent two FRT-related privacy concerns appearing with each other in the speaker-generated text. On the other hand, the co-occurrence of surveillance-related concerns and profiling-related concerns was the highest among the other two FRT-related privacy concerns in commentator-generated text and replier-generated text.

Chapter 5: Discussion

The new framework of FRT-related privacy concerns

FRT has been rapidly and globally deployed among organizations aiming to arrive at the highest security protection standard. A recent report has foreseen that the annual growth rate of the investment in this system during the period of 2020 to 2025 is on its path to hit 17.2% ("Facial Recognition Market," n.d.). Different privacy researchers (e.g., Nissenbaum, 1998; Smith, Milberg, & Burke, 1996; Turner & Dasgupta, 2006; Westin, 2003) have a consensus that advances in information technologies have a direct influence on personal attitudes toward privacy protection. Auxier et al. (2019c), moreover, revealed that 70% of individuals have considered their PII become less protected in recent years compared to the past five years. This feeling is likely to be related to Edward Snowden's critical leaks about the NSA plan of gathering millions of photos for FRT (Feeney, 2014). Although a relatively significant body of literature has paid close attention to individuals' privacy concerns surrounding FRT, there has been an obvious failure to investigate the roots that caused FRT-related privacy concerns.

The aforementioned research gap was, however, addressed in this dissertation by examining the most common FRT-related privacy concerns raised by YouTube users and how those concerns reflect difficulties in the control over personal information in terms of information collection, use, access, and disclosure. This examination was accomplished through the sequential exploratory mixed-method approach to develop a new scheme mapping the users' FRT-related privacy concerns in the qualitative phase and to apply the qualitative outcomes to a larger sample for generalization purposes in the quantitative phase. The new scheme is comprised of four dimensions and nine subdimensions: information collection (surveillance, coercion), information processing (retention period, profiling, security, secondary use, exclusion), information dissemination (disclosure), invasions (decisional

interference). The discussion of the findings was summarized into two points (FRT-related privacy concerns and difficulties in the control over personal information) to answer the research questions, draw the final conclusions, and locate the dissertation's position within the relevant literature.

FRT-related privacy concerns (RQ1)

The first question in this study sought to determine the most common FRT-related privacy concerns among YouTube users. One interesting finding to emerge from the analysis of this question is that the users' privacy concerns were differentially expressed, which broadly supports BeVier's (1995) claim that "privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests" (p.458). The major part of the users put their privacy concerns in a single theme (surveillance, coercion, retention period, profiling, security, secondary use, exclusion, disclosure, or decisional interference), whereas few of them raised multiple themes (e.g., surveillance and profiling) at the same time. This variation is often due to several variables including the difference in gender (e.g., Hoy & Milne, 2010; Youn & Hall, 2008), age (e.g., Kezer, Sevi, Cemalcilar, & Baruh, 2016; Van den Broeck, Poels, & Walrave, 2015), and cultural values (e.g., Bellman et al., 2004; Harris et al., 2003).

It was observed that the central users' discussion in many instances was revolved around information collection-related concerns, specifically surveillance-related concerns (16.15% in qualitative analysis and 69.18% in quantitative analysis) compared to other FRT-related privacy concerns. Surveillance refers to the process of describing personal identity via facial characteristics to keep gathering information about the users' daily activities and behaviors performed in public and private spaces without their knowledge and authorization (e.g., tracking consumers' behavior). In the 1980s, Mason (1986) voiced his concerns about surveillance systems reinforcement to track individuals in more advanced mechanisms. The users found that face recognition surveillance is an extremely powerful technology and

different from the traditional surveillance system bringing some unique activities that do not meet their expectations of privacy norms. An example of these activities is the obliteration of personal right to anonymity in public that was an available choice with the traditional surveillance system through adopting different approaches (e.g., using a pseudonym on the Internet (2)).

The coercion of self-disclosure of PII alongside the ambiguity in privacy agreements and rules for information archiving (e.g., the duration of information archiving) give an obvious signal for the organizations' desire to employ obtained information for their benefit. In agreement with several privacy scientists (e.g., Manders-Huits & Zimmer, 2009; Nissenbaum, 2009; Véliz, 2020), there was a consensus among the users who raised profiling-related concerns and disclosure-related concerns in their communication that information explosion in the age of FRT has opened an endless door for privacy violations by simplifying the process of generating a detailed profile enabling organizations to know about those users more than themselves or to share collected information with third parties for profit. The thing increased users' concerns, however, is that they were often unable to access those records to remove information that must not be stored (e.g., storing false information that has generated during the system penetration).

The organizations' claim that FRT has been developed and deployed to protect public security did obviously not convince many users. According to the 2018 survey distributed among senior executives, it was discovered that the investment of artificial intelligence and big data analytics shape a primary goal of 97% of large businesses (Davenport & Bean, 2018). Some of the past and recent literature (e.g., Norris, 1997; Véliz, 2020) described this phenomenon as the enhancement in social control level that organizations exploit collected information in a way that guarantees to control individuals' behaviors and choices. Users provided a wide array of examples in connection with social control, but the most common

case was the constant flow of advertisements to control their choices (e.g., pushing ads on consumers' mobile device to control their online purchases).

Difficulties in the control over personal information (RQ2)

The myth of privacy paradox

It is not a secret that the practice of voluntary information disclosure represents an essential component of much of our daily activities (e.g., sharing PII with relevant agencies to report annual tax payments). In the review of previous studies that concentrate on the investigation of personal motivations behind the decision-making of self-disclosure of PII, several theoretical frameworks (e.g., Kim, Ferrin, & Rao, 2008; Lee & Rao, 2007; Ortiz, Chih, & Tsai, 2018) have suggested that voluntary information disclosure often requires data subjects' privacy protection belief in organizational practices of information. Consistent with that, the users were noticed carrying out a cost-benefit analysis, named as privacy calculus theory (Laufer & Wolfe, 1977; Milne & Gordon, 1993), to evaluate the extent of benefits and risks the voluntary information disclosure may bring. One of the significant factors lending a hand to the users to take a proper decision was the transparency degree in privacy agreement, which was also reported in Wronski's (2019) work.

The unfortunate thing is that the users, in many instances, tended to have the privacy risk belief in the age of FRT because of the information use boundary. There has been an ethical crisis in developing privacy agreements among organizations and for-profit organizations in particular to avoid holding legal and social accountability. The vast majority of existing privacy agreements contain vague content (e.g., you authorize us to use your PII for other purposes if considered necessary without your notification and consent (2)) to limit the users' ability to clearly determine the dimensions of information usage. Auxier et al. (2019b) showed that the generality of participants who commonly read companies' privacy agreements face difficulty comprehending every single part of them. Yet it remains uncertain in the literature if the

information withdrawal (opt-out from the agreement), as raised by the users, is an impossible task once the acceptance to privacy agreement is received.

Simultaneously, it was somewhat expected that the transparency in privacy agreement does not always play a critical role in the users' decision of self-disclosure of PII. Organizations that prepare their privacy agreement in a simple pattern understood by all spectrums of society are not guaranteed to process disclosed information in an approach that does not violate privacy. Facebook, whose privacy statement is characterized by an acceptable degree of transparency with regard to information disclosures process, for instance, infringed the legal norms of privacy, exposing over 45 million profiles to a third party for the purpose of analysis without their users' knowledge (Cadwalladr & Graham-Harrison, 2018). The users' privacy protection belief, on that account, was formed by the reputation surrounding a target organization in terms of information handling. As a consequence of Apple's visible efforts in privacy protection, a joint survey confirmed that technology consumers' privacy protection belief in Apple's in information processing has not been affected despite the presence of controversial issues including the iCloud hack that occurred in 2014 (Tripathi, 2018).

The aspect that must be practically examined is the extent of the reflection of the users' privacy belief to their behavioral reality. A certain number of privacy scholars assumed that individuals with a privacy protection belief do not differ from their peers who have the privacy risk belief in terms of behavioral intention. The researchers' interpretation typically stemmed from the privacy paradox theory (Dinev, 2014; Norberg et al., 2007), which indicated independent groups keep disclosing their information while holding the privacy risk belief of organizational practices of information. Less than 55% out of those who expressed their privacy anxiety about sharing their contact information across online platforms, as a case in point, had the intention to use another phone number for privacy protection ("The Privacy Paradox lives on according to new survey," 2018). However, the levels observed in those

investigations are far below those observed by this and Solove's (2020) project, which concluded that the privacy paradox theory is a myth and nonexistent.

It, of course, could not be denied that a few users have still viewed privacy as a luxury commodity controlled by an individual more than being a legal or social norm, but over half of the users have predominantly found themselves in a position that has only one-way orientation, where they are left with no option other rather than self-disclosure of PII to a cluster of organizations. A variety of studies have noted that individuals are commonly encouraged to disclose PII through offering some benefits (e.g., joining a store's app for a convenient payment process (3)). The users, at any rate, reckoned that the low consequence from the traditional marketing strategies has pushed several organizations to replace it with the deprivation approach by trading off between privacy and basic life needs. A realistic example of this behavior is telecommunication services in China, where its citizens have been obliged by a new rule to use facial characteristics for identification as a means to get served (Goh, 2019).

Unsurprisingly, the social influence factor theorized by Kelman (1958) took a central place in the users' discussion. The decision-making of self-disclosure of PII in the community is, almost in all circumstances, ruled by the majority groups' beliefs. In their analysis of the correlation between peers' behavior and information disclosure intention, Kroschke and Steiner (2017) outlined that the high acceptance to the use of technology in the community put significant pressure on other individuals to disclose PII. The users, however, went beyond this point by delving into the basis of the social influence phenomenon to broaden our insights into how the majority groups' belief is formed. Their conclusion was that the majority of groups who support FRT should never been blamed, since they are a victim of a loop of organizational propaganda that has brainwashed individuals to follow some orders (e.g., focusing on September 11 attacks and the flaws in traditional surveillance systems to get the population' acceptance to FRT (2)).

Control over the flow of disclosed PII

Some active privacy scientists (e.g., Nissenbaum, 2004, 2009; Zimmer, 2007) have concluded that self-disclosure of PII must not be construed as the data subjects' willingness to give up their right to privacy. Information owners, under certain norms, usually expect to have a control over the flow of disclosed PII. In line with Auxier et al. (2019c) and Bacchi (2019) who surveyed this argument, the current study yielded that the users' control over disclosed PII has been extremely limited or sometimes nonexistent by virtue of the organizations' misconception about information ownership. Most organizations have never seen privacy agreements as a material for elucidating the purpose of gathering PII, the retention period of PII, and the boundary of using PII to preserve the individuals' legal right. Rather, the acceptance of the privacy agreement has been considered a waiver contract of information ownership from the users to organizations to be manipulated in consonance with their interests.

The high attention paid to surveillance-related concerns in both quantitative and qualitative analysis clarifies the vast gap between the users' and organizations' understanding level of information ownership. The users have been disclosing PII to multiple organizations, regardless of whether self-disclosure of PII was accomplished by a forced or a voluntary pattern, with the expectation that PII would never slope off its natural course. The natural course of PII in a particular context is overwhelmingly determined by either social or legal norms that the community adopts. Organizations were detected exploiting the users' disclosed PII for facial scanning and movement tracking through linking face features with traditional surveillance systems without their knowledge and informed consent. That was also emphasized in an earlier document, which revealed that driver's license photos stored in DMV databases have been accessed by allied U.S agencies to be employed for facial scanning without counseling the information owners (Harwell, 2019).

It is not difficult to discern that the global trend to deploy face recognition surveillance technology for public security, as reported by industry researcher IHS Markit (Nash, 2020), puts a great burden on our ability to exercise the right to privacy in public. As a response to flawed arguments in connection with privacy in public (e.g., nothing to hide), authors (e.g., Nissenbaum, 1998; Solove, 2007; Zimmer, 2007) have mentioned that individuals' privacy protection requires relevant parties to reconsider privacy in public as parallel to privacy in private owing to the fact that private information might be generated in both spaces. This view was heavily supported by the users, who believe that face recognition surveillance technology in public could capture incalculable private activities (e.g., recording sensitive activities conducted inside a personal vehicle that is parked in a public empty place surrounded by a network of face recognition sensors (3)).

The comprehensive surveillance of the community, consequently, has reinforced the belief of using security as an excuse for more intervention in private life. A myriad of Western countries, as argued in the users' conversation, have turned face recognition surveillance technology into profiling (e.g., social credit system) to predict suspect groups based on the analysis of a long record of personal behaviors that give organizations a right to additional access to information about an individual's life. We, nevertheless, must realize at some point that the prediction frequently relies on biased algorithms (racial profiling) that view privacy as a collective factor not an independent factor. For example, if the majority of members of a group are known to carry out certain behaviors, the algorithm has a tendency to classify other individuals belonging to this group into the same pattern, causing a disparate treatment in the right to privacy between individuals in one society, since some groups (e.g., black women) would be subject to constant inspection than others (e.g., white men).

The part that remains unclear is the extent of information quality in the decision-making process. It has been admitted that FRT "may not be sufficiently reliable to accurately locate

other photos of the same identity, resulting in an unacceptable percentage of misidentifications." (Prest, 2019, p. 15). The sources of the false-positive match that identified in the literature—including but not limited to the similarity in physiological characteristics, ethical issues, and spoofing attacks—seemed familiar to the users who reckoned that the misidentification keeps their records at constant risk of unauthorized access. Hackers, for instance, have a sizeable chance to gain access to personal records through the 3D masks for the purpose of blackmails and distorted information generation. This finding doubtless needs to be carefully scrutinized to identify whether organizations follow some strategies that are not announced to the public to handle error match issues. But security-related concerns help us to understand the reason behind the current organizations' desire to make records inaccessible by the information owner.

Despite the fact that disclosure-related activities were the common pattern between profiling-related concerns and security-related concerns, the most interesting finding is that privacy violations have been assessed in a contextual frame. It was noted that many of the users who raised disclosure-related concerns followed Nissenbaum's (2009) contextual integrity framework; that framework suggests the evaluation of privacy violations needs to identify the actors, attributes, and transmission principles parameters in their discussion. For instance, sharing photos under the data subjects' informed consent among health organizations who sought to benefit the public health (e.g., medical research) was not considered a privacy breach, while sharing information about personal shopping behaviors without the data subjects' informed consent among advertisement organizations was an unacceptable activity. This action, therefore, provides further support for the hypothesis that privacy violations lie in deviating information flow from social or legal norms, not in the self-disclosure of PII, as proposed by outdated theories such as the privacy paradox.

Implications

Conceptualizing privacy has never been a simple assignment over the past decades. Investigators have performed an extreme effort since the early 1890s to produce a theoretical framework describing the notion of privacy in an evident form. Early examples of the theoretical approaches to privacy include the right to be let alone (Warren & Brandeis, 1890) and control over personal information (Westin, 1967). But it has been argued by modern philosophers of privacy (e.g., Solove) that the conceptualization of privacy in a single dimension is limited to painting a thorough description of traditional privacy challenges, seeing that privacy is a dynamic (Altman, 1977), multifaceted (Heravi et al., 2018) and complex (Wang et al., 1998) perception. Smith et al. (1996) and other privacy scholars boosted this principle by launching a various array of multidimensional privacy models that were developed based on the common individuals' privacy concerns in the age of information technologies.

In addition to describing the privacy notion as a multidimensional factor, Nissenbaum (2009) affirmed that the conceptualization of privacy requires taking norms of a particular context into account to provide a valuable point of reference for the assessment of privacy violations. The sensitivity degree of using PII is quite dissimilar from one technology or context to another (e.g., the employment of personal photo for passport issuance is less sensitive than being used for training face recognition surveillance technology). Given that, this dissertation initially adopted the multidimensional framework established by Solove (2006) that consist of 16 elements (surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion, or decisional interference). Solove's taxonomy was then revised based on the analysis of the users' FRT-related privacy concerns to effectively reconceptualize privacy in the context of FRT.

In general, the new (revised) framework seems similar to Solove's taxonomy in terms of structure, but the difference lies in the level of context and modernity. The academic literature (e.g., Massey & Antón, 2008) on the conceptualization of privacy has revealed that the wide boundary of themes that emerged from Solove's taxonomy made this taxonomy unable to map the meaning of privacy or evaluate the state of privacy in an intelligible approach. Some themes include uncommon conditions in the age of information technologies such as gathering information about a person through outdated observation methods. In contrast to this taxonomy, the current study provides a contextual and modern framework that is eligible to serve as the basic rule of the theoretical frameworks for future FRT-related and similar studies. For example, this framework consists of elements (e.g., surveillance, data retention, profiling, security, and secondary us) that are described to correspond with privacy concerns surrounding a massive number of information technologies including smartphones and IoT.

Since the identification of privacy concerns forms a theoretical basis for the enactment of privacy laws, the new framework should offer a comprehensive insight of current privacy laws flaws that are of interest to policymakers; one hopes this will motivate them to enact new privacy laws or reform existing privacy laws to address organizations' abuses and protect the individuals' right to privacy in the era of FRT. Though there has been a global increase in the rate of privacy legislation, as indicated in many studies (e.g., Greenleaf, 2017, 2019), the present privacy laws have not been capable yet of being compatible with age of information technologies (Zimmer, 2005), including FRT. This has something to do with the fact that several privacy regulations have been legislated in a general frame, meaning the variation in information flow from one technology to another has not been considered, which allowed organizations to exploit legal loopholes in some contexts to serve their interests and act against personal privacy.

The majority of approaches used in the relevant literature to assess privacy concerns has, unfortunately, been limited to the privacy calculus theory, which arose from an outdated privacy theory (privacy as control over personal information). The conclusion of the privacy calculus theory in almost all contexts is misleading since, as shown in this chapter, personal intention to disclose PII does happen with a lack of privacy protection. Instead, individuals who hold the privacy risk belief and share PII with others often rely on the legal or social expectation to have control over the disclosed PII. In contrast, this study applied the sequential exploratory mixed-method design to get a more appropriate understanding of sources that caused the privacy risk belief of PII surrounding FRT. Strategies and instruments used in the dissertation, including the classifier, are anticipated to be replicated to different privacy frameworks with the objective to continue reconceptualizing privacy and create a valid assessment matrix for a certain context.

Limitations

The research limitations lie in three aspects; data collection, data preprocessing, and data analysis. This seems quite common in social media research, particularly those studies that have applied supervised machine learning algorithms. First, the review of several statistical analyses about the proportion of actual and active users on YouTube as well as their locations show that the generalizability of the findings is limited. Even though YouTube is the apex of online video-sharing platforms and hosts upwards of 1.5 billion users worldwide, it has a very narrow population in that not all the spectrum of society is involved to represent their peers' perspective toward FRT. For example, YouTube has been an inaccessible source to many regions in China, so those users' voices were absent in this dissertation. Over and above that, it is important to recall that not every YouTube user is interested in interacting with videos or other users; some of them prefer to keep inactive.

An additional uncontrolled factor was the confidence of excluding duplicate values from the corpus as the result of some behaviors adopted by the users, illustrated in the methodology chapter, or unintended errors during the data collection process. In the realm of NLP, there are two main approaches for the removal of duplicate text, content duplication detection and content similarity detection; each has its own limitations. The exclusion of duplicate content in content duplication detection algorithms, used in this project to minimize the noise on the findings, is completed if the value of two inputs is matched. This means very tiny changes in content (e.g., adding a letter, space, and period or changing grammatical tense for a word) will not be considered a duplicate. The developers of content similarity detection algorithms have devoted their time to addressing this dilemma by training the machine to look for the similarity between two inputs. Yet such algorithms sometimes delete similar materials that might change the conclusion.

In the same vein, the performance of the applied classifier was not ideal, as expected at the beginning. Further analysis took place to ensure that similar findings between the users were accurate and not stemmed from the classifier failure. The analysis confirmed that around three in 25 text rows in video transcripts, seven in 100 text rows in top-level comments, and six in 100 text rows in low-level comments were either misidentified (a false negative) or misclassified (a false positive). Some dimensions of FRT-related privacy concerns were more prone to fall into this category (e.g., 6% of retention period-related concerns were classified as exclusion-related concerns) than others. This problem is likely related to the number of data points created by similar examples that confused the classifier in some cases. Even so, this limitation did not negatively influence the quantitative findings but was mentioned from the standpoint of scientific integrity to take into account in future studies.

Conclusion and future work

This dissertation appears to be the first study that has provided a deeper insight into FRT-related privacy concerns. Overall, it has been concluded that the rapid implementation of FRT across countries is a double-edged sword. There is no reason to doubt that this system has positively influenced security levels in some settings, such as safeguarding mobile phone content (Haifeng Li & Zhu, 2016), and detecting identity frauds (Chen et al., 2010). But the ways that FRT has been approached by organizations made it quite far from being in a position to balance public security and privacy interests. Nine common dimensions (surveillance, coercion, retention period, profiling, security, secondary use, exclusion, disclosure, decisional interference) of privacy issues surrounding FRT were found among YouTube users. These issues, perhaps, will drive us to witness a huge increase in privacy violations in the future unless the enactment or reform of privacy laws is achieved.

There is a persistent need for further research to analyze the interaction between the different dimensions. Some FRT-related privacy concerns, as shown in Figure 11, were constantly accompanied by other FRT-related privacy concerns. For instance, 100% of cases that speakers raised their coercion-related concerns, profiling-related concerns, and disclosure-related concerns came into view with other FRT-related privacy concerns. The co-occurrence analysis (Table 8-10) statistically illustrated the relationship between different FRT-related privacy concerns. Nevertheless, the roots of their interaction in the same theme (e.g., security and profiling) or in different themes (e.g., profiling and disclosure) remain unexplored. Future studies on the current topic are therefore recommended to qualitatively identify the fine lines between FRT-related privacy concerns in order to fully understand their relationship and the impact of particular FRT-related privacy concerns on others. Duplicating this analysis on user-generated text across different platforms (e.g., Twitter and Reddit) should also help to generalize the findings to Web 2.0 users.

Moreover, further investigation and experimentation need to apply the contextual integrity theory (Nissenbaum, 2009) to the findings as a means to get a comprehensive assessment of FRT-related privacy concerns. It was observed during the qualitative analysis that the degree of the users' privacy concerns with regard to each dimension differed from one organization to another. For example, the majority of disclosure-related concerns shed light on the Clearview AI company, while Facebook received more concerns in cases that mentioned profiling-related violations. A possible explanation for this behavior might hark back to the variation and transparency in privacy protection protocols that an organization has processed. For that reason, future researchers is strongly recommended to sequentially examine the nine dimensions using Named Entity Recognition for Social Network Analysis to create a map illustrating the relationships between FRT-related privacy concerns and organizations.

References

Adams' Argument for the Defense: 3–4 December 1770. (n.d.). Retrieved March 5, 2020, from https://founders.archives.gov/documents/Adams/05-03-02-0001-0004-0016

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, N.J.: Prentice-Hall.

Albarracin, D., & Shavitt, S. (2018). Attitudes and Attitude Change. *Annual Review of Psychology*, *69*(1), 299–327. https://doi.org/10.1146/annurev-psych-122216-011911

Allen, A. L. (1988). *Uneasy access : privacy for women in a free society*. Rowman & Littlefield.

Alschuler, A. W. (2002). Racial Profiling and the Constitution. *University of Chicago Legal Forum*.

Alsulaiman, L. A., & Alrodhan, W. A. (2014). Information Privacy Status in Saudi Arabia. *Computer and Information Science*, *7*(3). https://doi.org/10.5539/cis.v7n3p102

Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, *33*(3), 66–84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(2), 1–23. https://doi.org/10.1145/3214262

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019a). 1. How Americans think about privacy and the vulnerability of their personal data | Pew Research Center. Retrieved May 6, 2020, from https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019b). *Americans' attitudes and experiences with privacy policies and laws*. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019c). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved April 8, 2020, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bacchi, U. (2019). Privacy concerns pushing people to change online behavior, poll shows - Reuters. Retrieved February 28, 2020, from https://www.reuters.com/article/us-global-tech-privacy/privacy-concerns-pushing-people-to-change-online-behavior-poll-shows-idUSKBN1Y803D

Bacchini, F., & Lorusso, L. (2019). Race, again: how face recognition technology reinforces racial discrimination. *Journal of Information, Communication and Ethics in Society*, *17*(3), 321–335. https://doi.org/10.1108/JICES-05-2018-0050

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Bernstein, B. (1960). Language and Social Class. *The British Journal of Sociology*, *11*(3), 271–276. https://doi.org/10.2307/586750

BeVier, L. R. (1995). Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection. *William & Mary Bill of Rights Journal*, *4*, 455–506. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/wmbrts4&id=463&div=&collection=

Bhatia, R. (2013). Biometrics and Face Recognition Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5).

Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism. Congressional Hearing, 2001-11-14, 2001-11-14, 2001-11-14. (2001). Retrieved from https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/html/CHRG-107shrg81678.htm

Bok, S. (1989). *Secrets : on the ethics of concealment and revelation*. New York: Vintage Books.

Bowyer, K. W. (2004). Face recognition technology: Security versus privacy. *IEEE Technology and Society Magazine*, *23*(1), 9–20. https://doi.org/10.1109/MTAS.2004.1273467

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification . In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (Vol. 81, pp. 77–91). PMLR.

Byford, K. S. (1998). Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment. *Rutgers Computer & Technology Law Journal*, *24*(1).

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved February 28, 2020, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Chalakoski, M. (2017). Will and William West conundrum: How two unrelated but identical inmates showed need for fingerprinting. Retrieved March 28, 2021, from https://www.thevintagenews.com/2017/09/29/will-and-william-west-conundrum-how-two-unrelated-but-identical-inmates-showed-need-for-fingerprinting/

Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. London: Sage.

Chen, R., Kuang Hsieh, K., & Tsai, C. (2010). The implementation of face recognition technology and its effect on e□quiz credibility. *Asian Journal on Quality*, *11*(2), 125–136. https://doi.org/10.1108/15982681011075934

Cheng, X., Dale, C., & Liu, J. (2008). Statistics and social network of YouTube videos. In

IEEE International Workshop on Quality of Service, IWQoS (pp. 229–238). https://doi.org/10.1109/IWQOS.2008.32

Clarke, R. (1993). Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law and Information Science*, *4*.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67. https://doi.org/10.1145/293411.293475

Cooper, P. (2020). How Does the YouTube Algorithm Work? A Guide to Getting More Views. Retrieved September 27, 2020, from https://blog.hootsuite.com/how-the-youtube-algorithm-works/

Daugherty, T., Eastin, M. S., & Bright, L. (2008). Exploring Consumer Motivations for Creating User-Generated Content. *Journal of Interactive Advertising*, *8*(2), 16–25. https://doi.org/10.1080/15252019.2008.10722139

Davenport, T. H., & Bean, R. (2018). Big Companies Are Embracing Analytics, But Most Still Don't Have a Data-Driven Culture. *Harvard Business Review*, *6*, 1–4.

Davis, A. (1997). The Body as Password. *Wired*. Retrieved from https://www.wired.com/1997/07/biometrics-2/

Davis, D. (2019). Facial recognition technology threatens to end all individual privacy. Retrieved February 28, 2020, from https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

De Assis Rodrigues, F., & Sant'Ana, R. C. G. (2016). Use of taxonomy of privacy to identify activities found in social networks' terms of use. *Knowledge Organization*, *43*(4), 285–295. https://doi.org/10.5771/0943-7444-2016-4-285

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

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes.* Orlando, FL, US: Harcourt Brace Jovanovich College Publishers.

Executive Summary: Data Growth, Business Opportunities, and the IT Imperatives | The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things. (2014). Retrieved March 17, 2020, from https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Facial Recognition Market. (n.d.). Retrieved March 3, 2020, from https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html

Facial Recognition Market Size, Share and Global Market Forecast to 2025 . (n.d.). Retrieved March 16, 2021, from https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html

Fazio, R. H. (1986). How do attitudes guide behavior. In *Handbook of motivation and cognition: Foundations of social behavior* (pp. 204–243). New York: Guilford Press. Retrieved from https://www.researchgate.net/publication/240032990

Federal Trade Commission. (2021). Fraud and ID Theft Maps . Retrieved March 28, 2021, from https://public.tableau.com/profile/federal.trade.commission#!/vizhome/FraudandIDTheftMaps/IDTheftbyState

Feeney, N. (2014). NSA Collects Millions of Facial Photos Daily, Snowden Documents Say. *Time*. Retrieved from https://time.com/2804898/snowden-nsa-facial-recognition/

Freund, P. A. (2017). Privacy: One concept or many. In *Privacy and Personality* (pp. 182–198). Taylor and Francis. https://doi.org/10.4324/9781315127439-10

Fried, C. (1968). Privacy. *The Yale Law Journal*, *77*(3), 493. https://doi.org/10.2307/794941

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, *89*(3), 471. https://doi.org/10.2307/795891

Ghosh, A. K., Badillo-Urquiola, K., Guha, S., Laviola, J. J., & Wisniewski, P. J. (2018). Safety vs. surveillance: What children have to say about mobile apps for parental control. In *Conference on Human Factors in Computing Systems - Proceedings* (Vol. 2018-April, pp. 1–14). New York, USA: Association for Computing Machinery. https://doi.org/10.1145/3173574.3173698

Gill, A. J., Vasalou, A., Papoutsi, C., & Joinson, A. (2011). Privacy dictionary: A linguistic taxonomy of privacy for content analysis. In *Conference on Human Factors in Computing Systems - Proceedings* (pp. 3227–3236). New York, New York, USA: ACM Press. https://doi.org/10.1145/1978942.1979421

Gladney, H. M. (2006). Principles for digital preservation. *Communications of the ACM*, *49*(2), 111–116. https://doi.org/10.1145/1113034.1113038

Godkin, E. L. (1880). Libel and its legal remedy. *The Atlantic Monthly*, *XLVI*(CCLXXVIII), 729–738.

Goh, B. (2019). China's facial recognition rollout reaches into mobile phones, shops and homes. Retrieved February 28, 2020, from https://www.reuters.com/article/us-china-technology-explainer/chinas-facial-recognition-rollout-reaches-into-mobile-phones-shops-and-homes-idUSKBN1Y60MN

Greenleaf, G. (2017). *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*.

Greenleaf, G. (2019). *Countries with Data Privacy Laws – By Year 1973-2019*. *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.3386510

Hale, J. (2019). More Than 500 Hours Of Content Are Now Being Uploaded To YouTube Every Minute - Tubefilter. Retrieved September 13, 2020, from https://www.tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute/

Harris, M. M., Van Hoye, G., & Lievens, F. (2003). Privacy and attitudes towards Internet-

based selection systems: A cross-cultural comparison. *International Journal of Selection and Assessment*, *11*(2–3), 230–236. https://doi.org/10.1111/1468-2389.00246

Harwell, D. (2019). FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches. Retrieved February 27, 2021, from https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/

Heravi, A., Mubarak, S., & Raymond Choo, K. K. (2018). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, *84*, 441–459. https://doi.org/10.1016/j.chb.2018.03.016

Hollenbaugh, E. E., & Everett, M. K. (2013). The Effects of Anonymity on Self-Disclosure in Blogs: An Application of the Online Disinhibition Effect. *Journal of Computer-Mediated Communication*, *18*(3), 283–302. https://doi.org/10.1111/jcc4.12008

Hoy, M. G., & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, *10*(2), 28–45. https://doi.org/10.1080/15252019.2010.10722168

Huete-Alcocer, N. (2017). A Literature Review of Word of Mouth and Electronic Word of Mouth: Implications for Consumer Behavior. *Frontiers in Psychology*, *8*. https://doi.org/10.3389/fpsyg.2017.01256

Institutional Review Board. (n.d.). Retrieved March 21, 2020, from https://uwm.edu/irb/

Ivankova, N. V, & Creswell, J. W. (2009). Mixed Methods. In *Qualitative Research in Applied Linguistics* (pp. 135–161). London: Palgrave Macmillan UK. https://doi.org/10.1057/9780230239517_7

Jain, A. K., Bolle, R., & Pankanti, S. (2006). *Biometrics : personal identification in networked society*. Springer.

Jain, A. K., Ross, A., Pankanti, S., & Member, S. (2006). Biometrics: A Tool for Information Security. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 1(2).

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, *31*(2), 177–192. https://doi.org/10.1002/ejsp.36

Jung, C. G. (1923). *Psychological types or the psychology of individuation*. London: Kegan Paul, Trench, Trubner. Retrieved from https://archive.org/details/psychological_types/page/n6/mode/2up

Kallas, P. (2020). Top 15 Most Popular Social Networking Sites and Apps. Retrieved April 10, 2020, from https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

Kalra, G. S., Kathuria, R. S., & Kumar, A. (2019). YouTube Video Classification based on Title and Description Text. In *Proceedings - 2019 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2019* (Vol. 2019-Janua, pp. 74–79). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCCIS48478.2019.8974514

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Journal of Conflict Resolution*, *2*(1), 51–60. https://doi.org/10.1177/002200275800200106

Kemp, S. (2021). *Digital 2021: Global Overview Report*. Retrieved from https://datareportal.com/reports/digital-2021-global-overview-report

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology*, *10*(1). https://doi.org/10.5817/CP2016-1-2

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Kobielus, J. (2018). Wikibon's 2018 Big Data Analytics Trends and Forecast - Wikibon Research. Retrieved March 21, 2020, from https://wikibon.com/wikibons-2018-big-data-analytics-trends-forecast/

Kordopatis-Zilos, G., Papadopoulos, S., Patras, I., & Kompatsiaris, Y. (2017). Near-duplicate video retrieval by aggregating intermediate CNN layers. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 10132 LNCS, pp. 251–263). Springer Verlag. https://doi.org/10.1007/978-3-319-51811-4_21

Korzaan, M., Brooks, N., & Greer, T. (2009). Demystifying Personality and Privacy: An Empirical Investigation into Antecedents of Concerns for Information Privacy. *Journal of Behavioral Studies in Business*, *1*, 1–17.

Kostka, G., & Antoine, L. (2019). Fostering Model Citizenship: Behavioral Responses to China's Emerging Social Credit Systems. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3305724

Kroschke, M., & Steiner, M. (2017). The Influence of Social Cues on Users' Information Disclosure Intentions – The Case of Mobile Apps. *ICIS 2017 Proceedings*.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, J.-H., & Cha, K.-W. (2020). An Analysis of the Errors in the Auto-Generated Captions of University Commencement Speeches on YouTube. *THE JOURNAL OF ASIA TEFL*, *17*(1), 143–159. https://doi.org/10.18823/asiatefl.2020.17.1.9.143

Lee, J. K., & Rao, H. R. (2007). Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment. *Decision Support Systems*, *43*(4), 1431–1449. https://doi.org/10.1016/j.dss.2006.04.008

Li, Haifeng, & Zhu, X. (2016). Face recognition technology research and implementation based on mobile phone system. In *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, ICNC-FSKD 2016* (pp. 972–976). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/FSKD.2016.7603310

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

Liddy, E. (2001). Natural Language Processing. In *Encyclopedia of Library and Information Science* (2nd Ed). New York: Marcel Decker.

Liddy, E. D. (2005). Text Mining. *Bulletin of the American Society for Information Science and Technology*, *27*(1), 13–14. https://doi.org/10.1002/bult.184

Lin, L., & Purnell, N. (2019). A World With a Billion Cameras Watching You Is Just Around the Corner. Retrieved February 24, 2021, from https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402

Liu, J., Huang, Z., Cai, H., Shen, H. T., Ngo, C. W., & Wang, W. (2013). Near-duplicate video retrieval: Current research and future trends. *ACM Computing Surveys*, *45*(4), 1–23. https://doi.org/10.1145/2501654.2501658

Liu, S., & Silverman, M. (2001). Practical guide to biometric security technology. *IT Professional*, *3*(1), 27–32. https://doi.org/10.1109/6294.899930

Lyon, D. (2005). Surveillance as social sorting : Computer codes and mobile bodies. In *Surveillance as Social Sorting Privacy, Risk and Automated Discrimination* (pp. 27–44). Routledge. https://doi.org/10.4324/9780203994887-6

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Manders-Huits, N., & Zimmer, M. (2009). Values and pragmatic action: The challenges of introducing ethical intelligence in technical design communities. *International Review of Information Ethics*, *10*(2), 37–45.

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 12. https://doi.org/10.2307/248873

Massey, A. K., & Antón, A. I. (2008). A requirements-based comparison of privacy taxonomies. In *2008 Requirements Engineering and Law, RELAW'08*. https://doi.org/10.1109/RELAW.2008.1

McCroskey, J. C., & Richmond, V. P. (1977). Communication apprehension as a predictor of self-disclosure. *Communication Quarterly*, *25*(4), 40–43. https://doi.org/10.1080/01463377709369271

Milne, G. R., & Gordon, M. E. (1993). Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework. *Journal of Public Policy & Marketing*, *12*(2), 206–215. https://doi.org/10.1177/074391569101200206

Calif, S. (2019). Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion. Retrieved March 11, 2020, from https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/

Munir, K. A. (2005). The Social Construction of Events: A Study of Institutional Change in the Photographic Field. *Organization Studies*, *26*(1), 93–112.

https://doi.org/10.1177/0170840605049463

Nash, J. (2020). Global sales of video surveillance equipment projected to surpass billion this year. Retrieved February 24, 2021, from https://www.biometricupdate.com/202001/global-sales-of-video-surveillance-equipment-projected-to-surpass-20-billion-this-year

Niaz, M. (2007). Can findings of qualitative research in education be generalized? *Quality and Quantity*, *41*(3), 429–445. https://doi.org/10.1007/s11135-006-9015-9

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*(5–6), 559–596. https://doi.org/10.2307/3505189

Nissenbaum, H. (1999). The meaning of anonymity in an information age. *Information Society*, *15*(2), 141–144. https://doi.org/10.1080/019722499128592

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*, 119–157.

Nissenbaum, H. (2009). *Privacy in context : technology, policy, and the integrity of social life*. Stanford Law Books.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Norris, C. (1997). *Surveillance Order and Social Control* .

O'Donnell, L. (2019). Facial Recognition 'Consent' Doesn't Exist, Threatpost Poll Finds. Retrieved February 28, 2020, from https://threatpost.com/facial-recognition-consent-doesnt-exist-threatpost-poll-finds/144126/

Ortiz, J., Chih, W. H., & Tsai, F. S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior*, *80*, 143–157. https://doi.org/10.1016/j.chb.2017.11.005

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security and Privacy*, *1*(2), 33–42. https://doi.org/10.1109/MSECP.2003.1193209

Prest, E. (2019). *PIA: NGI-Interstate Photo Systen — FBI*. Retrieved from https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view

Privacy Principles for Facial-Recognition Technology in Commercial Applications. (2018).

Sadeh, N., Acquisti, R., Breaux, T. D., Cranor, L. F., Mcdonalda, A. M., Reidenbergb, J. R., … Wilson, S. (2013). The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About.

Schneier, B. (2006). Essays: The Eternal Value of Privacy . Retrieved March 29, 2021, from https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

Schoeman, F. (1984). Privacy: Philosophical Dimensions. *American Philosophical Quarterly*,

21(3), 199–213. https://doi.org/10.2307/20014049

Shi, P., Xu, H., & Chen, Y. (2013). Using contextual integrity to examine interpersonal information boundary on Social Network Sites. In *Conference on Human Factors in Computing Systems - Proceedings* (pp. 35–38). New York, NY, USA: ACM. https://doi.org/10.1145/2470654.2470660

Shvartzshnaider, Y., Apthorpe, N., Feamster, N., & Nissenbaum, H. (2019). Going against the (Appropriate) Flow: A Contextual Integrity Approach to Privacy Policy Analysis. *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing*, *7*(1), 19. Retrieved from www.aaai.org

Siersdorfer, S., Chelaru, S., Nejdl, W., & San Pedro, J. (2010). How useful are your comments? Analyzing and predicting YouTube comments and comment ratings. In *Proceedings of the 19th International Conference on World Wide Web, WWW '10* (pp. 891–900). New York, New York, USA: ACM Press. https://doi.org/10.1145/1772690.1772781

Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444. https://doi.org/10.17705/1jais.00092

Smith, A. (2019). More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly . Retrieved April 21, 2020, from https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly: Management Information Systems*, *20*(2), 167–195. https://doi.org/10.2307/249477

Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, *90*.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3).

Solove, D. J. (2007). I've Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review*, *44*.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, Mass: Harvard University Press.

Solove, D. J. (2020). The Myth of the Privacy Paradox. *SSRN Electronic Journal*, 1–42. https://doi.org/10.2139/ssrn.3536265

Song, J., Yang, Y., Huang, Z., Shen, H. T., & Hong, R. (2011). Multiple feature hashing for real-time large scale near-duplicate video retrieval. In *MM'11 - Proceedings of the 2011 ACM Multimedia Conference and Co-Located Workshops* (pp. 423–432). New York, New York, USA: ACM Press. https://doi.org/10.1145/2072298.2072354

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

The Perpetual Line Up - Unregulated Police Face Recognition in America. (2016). Retrieved March 23, 2020, from https://www.perpetuallineup.org/

The Privacy Paradox lives on according to new survey . (2018). Retrieved April 5, 2020, from https://www.getkeepsafe.com/blog/new-keepsafe-survey-shows-the-privacy-paradox-lives-on/

The top 500 sites on the web. (n.d.). Retrieved April 13, 2020, from https://www.alexa.com/topsites

Thompson, P. B. (2001). Privacy, secrecy and security. *Ethics and Information Technology*, *3*(1), 13–19. https://doi.org/10.1023/A:1011423705643

Tian, Y. (2010). Organ donation on web 2.0: Content and audience analysis of organ donation videos on YouTube. *Health Communication*, *25*(3), 238–246. https://doi.org/10.1080/10410231003698911

Tripathi, P. (2018). People Trust Apple More Than Google And Facebook. Retrieved April 3, 2020, from https://dazeinfo.com/2018/04/12/apple-google-microsoft-facebook-most-trusted-company/

Turner, E. C., & Dasgupta, S. (2006). Privacy on the Web: an Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. *Information Systems Management*, *20*(1), 8–18. https://doi.org/10.1201/1078/43203.20.1.20031201/40079.2

UN projects world population to reach 8.5 billion by 2030, driven by growth in developing countries. (2015). Retrieved March 25, 2020, from https://www.un.org/sustainabledevelopment/blog/2015/07/un-projects-world-population-to-reach-8-5-billion-by-2030-driven-by-growth-in-developing-countries/

Uryupina, O., Plank, B., Severyn, A., Rotondi, A., & Moschitti, A. (2014). SenTube: A Corpus for Sentiment Analysis on YouTube Social Media. In *LREC*.

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and Wiser? Facebook Use, Privacy Concern, and Privacy Protection in the Life Stages of Emerging, Young, and Middle Adulthood. *Social Media and Society*, *1*(2). https://doi.org/10.1177/2056305115616149

Vasalou, A., Gill, A. J., Mazanderani, F., Papoutsi, C., & Joinson, A. (2011). Privacy dictionary: A new resource for the automated content analysis of privacy. *Journal of the American Society for Information Science and Technology*, *62*(11), 2095–2105. https://doi.org/10.1002/asi.21610

Véliz, C. (2020). *Privacy is Power*. Bantam Press.

Walsh, D., Parisi, J. M., & Passerini, K. (2017). Privacy as a right or as a commodity in the online world: the limits of regulatory reform and self-regulation. *Electronic Commerce Research*, *17*(2), 185–203. https://doi.org/10.1007/s10660-015-9187-2

Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM*, *41*(3), 63–70. https://doi.org/10.1145/272287.272299

Warren, C., & Laslett, B. (1977). Privacy and Secrecy: A Conceptual Comparison. *Journal of Social Issues*, *33*(3), 43–51. https://doi.org/10.1111/j.1540-4560.1977.tb01881.x

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5),

193–220. https://doi.org/10.2307/I256795

Weber, R. P. (1990). *Basic Content Analysis*. SAGE Publications.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072

What happens on the effective date? (n.d.). Retrieved March 25, 2021, from https://faq.whatsapp.com/general/security-and-privacy/what-happens-when-our-terms-and-privacy-policy-updates-take-effect/?lang=en

Winter, G. (2000). A Comparative Discussion of the Notion of "Validity" in Qualitative and Quantitative Research. *The Qualitative Report*, *4*(3), 1–14.

Wronski, L. (2019). SurveyMonkey poll: privacy policies. Retrieved February 21, 2021, from https://www.surveymonkey.com/curiosity/axios-surveymonkey-poll-privacy-policies/

Yang, Y., & Liu, N. (2019). China survey shows high concern over facial recognition abuse. Retrieved February 28, 2020, from https://www.ft.com/content/7c32c7a8-172e-11ea-9ee4-11f260415385

Yang, Y., & Murgia, M. (2019). Data leak reveals China is tracking almost 2.6m people in Xinjiang. Retrieved February 28, 2020, from https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology and Behavior*, *11*(6), 763–765. https://doi.org/10.1089/cpb.2007.0240

Zimmer, M. (2005). Surveillance, privacy and the ethics of vehicle safety communication technologies. *Ethics and Information Technology*, *7*(4), 201–210. https://doi.org/10.1007/s10676-006-0016-0

Zimmer, M. (2007). Privacy and Surveillance in Web 2.0: A study in Contextual Integrity, and the Emergence of "Netaveillance." In *Society for Social Studies of Science 2007 Annual Meeting* (pp. 163–175). Montreal, Canada.

Zimmer, M. (2008). Privacy on Planet Google: Using the Theory of Contextual Integrity to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine. *Journal of Business & Technology Law*, *3*(1), 109–126.

Zimmer, M. (2010). Is it Ethical to Harvest Public Twitter Accounts without Consent? | MichaelZimmer.org. Retrieved March 5, 2020, from https://www.michaelzimmer.org/2010/02/12/is-it-ethical-to-harvest-public-twitter-accounts-without-consent/

Zimmer, M. (2018). Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity. *Social Media + Society*, *4*(2). https://doi.org/10.1177/2056305118768300

Appendices

Appendix A: Survey questions

University of Wisconsin-Milwaukee
Informed Consent to Participate in Research

Study Title: Dictionary-Based Text Analysis in The Context of Facial Recognition Technology (FRT).

Researcher: Yazeed Alhumaidan, PhD candidate-School of Information Studies.

Study Description: The purpose of this research study is to identify the most commonly used privacy-related keywords based on the framework of Solove's taxonomy in the context of Facial Recognition Technology (FRT). Approximately 500 subjects are needed to participate in this survey that should not take longer than 20 minutes of participants' time. This survey will ask participants about demographic information (country of residence, gender, age, first language) and privacy-related keywords. Participants will need to understand the elements of Solove's taxonomy (consists of 4 groups and 16 subgroups explained in this survey along with examples) and then write down synonyms and relevant words and phrases of each subgroup in the context of FRT. If more information about the taxonomy is needed, it is an open-source material: *Solove, D. J. (2005). A taxonomy of privacy. U. Pa. L. Rev., 154, 477*

Risks: There is no risk to participants for participating in this research survey. The survey does not include direct or indirect questions seeking personally identifiable information (PII) such as name or Social Security Number (SSN). However, SurveyMonkey might connect participants' survey responses with their Internet Protocol (IP) address or other PII. Participants must read SurveyMonkey participant and privacy policy so carefully to avoid any privacy risks.

Benefits: There are no costs for participating or benefits to participants. Participation in this survey will drive the researcher to successfully develop a privacy dictionary based on the framework of Solove's taxonomy. Such a dictionary will contribute to facilitating the process of extracting valuable information from a massive number of unstructured datasets surrounding privacy issues (e.g., user-generated content).

Confidentiality and Data Security: Although this survey does not seek PII, the confidentiality of survey responses is taken very seriously. Participants' survey responses will be retained on the SurveyMonkey website server. The only researcher and Dr. Xiangming "Simon" Mu, School of Information Studies, could access those responses. Besides, the Institutional Review Board (IRB) at UWM, the Office for Human Research Protections (OHRP), or other federal agencies may review all the study data to ensure laws and ethical guidelines are followed. Participants' survey responses will be destroyed once the data

analysis process is achieved, and the findings will be reported in aggregate to be shared in publications or presentations with other researchers.

Voluntary Participation: If you decide to be a part of this study, participation in this survey is completely voluntary. You can always change your mind and withdraw from the survey entirely. There are no negative consequences, whatever you decide.

Contact information:
For further questions about the research, complaints, or problems, please do not hesitate to contact:

- **Researcher**: Yazeed Alhumaidan at (414)-306-1519 – alhumai7@uwm.edu
- **Advisor**: Dr. Xiangming "Simon" Mu at (414) 229-6039 – mux@uwm.edu

For questions about your rights as a research participant, complaints, or problems, please contact:

- The UWM IRB (Institutional Review Board; provides ethics oversight) at (414)-229-3173 -irbinfo@uwm.edu.

Please print or save this screen if you want to be able to access the information later.
IRB #:
IRB Approval Date:

Agreement to Participate: By entering this survey, you are acknowledging that you have read the consent form, your age is 18 or older, you are an English speaker, you have appropriate knowledge of how FRT works, and you voluntarily agree to participate in this research survey.

- Agree
- Not Agree

Section A: Demographic & General Information

1- What country are you from?

2- What is your gender?
   - Male
   - Female
   - Other

3- What is your age?
   - 18-29
   - 30-39
   - 40-49
   - 50-59
   - 60-69

- 70 and older

4- What is your first language?
   - English
   - Non-English

Section B: Word & Phrases Extraction

Please read the description and example of each element, and then write down as many synonyms and relevant words and phrases as you can:

Group	Subgroup	Description	Example	Words	Phrases
Information collocation	Surveillance	It refers to the process of gathering information about individuals in public and private spaces without their knowledge and consent.	Tracking and collecting social media users' daily activities using face recognition surveillance technology.		
	Interrogation	It refers to the process of forcing individuals to disclose information that preferred to be private.	Forcing individuals to engage in FRT by disclosing their photos.		
Information processing	Aggregation	It refers to the process of creating personal profiles by combining information about individuals gathered from several sources for analysis.	Combining information about places visited by individuals during a certain period of time and their driver records in one place to identify trustworthy and untrustworthy driver age		
	Identification	It refers to the process of	Linking individuals'		

		linking personal profiles that contain aggregate information about individuals to personal identity.	profiles to their photos in a particular state to identify job applicants and review their past activities to make an appropriate decision.		
	Insecurity	It refers to the process of not providing an appropriate mechanism to prevent unauthorized access to personal records.	Making a 3D-printed mask of an employee's facial features to fool FRT and gain access to personal records.		
	Secondary use	It refers to the process of using the gathered information for purposes that are out of agreement context.	Using personal photos that gathered for the purpose of driver's license issuance for face recognition surveillance technology.		
	Exclusion	It refers to the process of excluding individuals from being involved in the decision-making process about information collection, use, storage, and disclosure.	Not making social media users aware of what information is gathered about them and how this information is processed.		
Information dissemination	Breach of confidentiality	It refers to the process of breaching the promise of	Promising to keep patients' profiles confidential,		

		maintaining the confidentiality of information leading to destroy the trust between organizations and individuals.	but subsequently, their profiles have been leaked to third parties.		
	Disclosure	It refers to the process of disclosing information about individuals leading to change others' judgment of individuals.	Disclosing information about professors captured by face recognition surveillance technology collaborating with rival schools to cause destruction in their reputations.		
	Exposure	It refers to the process of exposing private, sensitive, and embarrassing information about individuals that should not be shared with other parties.	Exposing intimate photos between spouses who captured by face recognition surveillance technology in public or private spaces to embarrass them and restrict their social participation.		
	Increased accessibility	It refers to the process of expanding the access scope of databases that consist of information	Establishing a united database between grocery store owners to access		

		about individuals.	information about a particular group of shoppers that inputted by multiple stores.		
	Blackmail	It refers to the process of threatening individuals to reveal their private information if the blackmailers have not got their demands.	Blackmailing spouses to expose intimate photos if a blackmailer does not get funds.		
	Appropriation	It refers to the process of taking advantage of information about individuals to serve the objectives of organizations and other parties.	Exploiting customers' names and numbers of shoppers captured by face recognition surveillance technology during their store visits for a commercial advertisement as an index of customers' satisfaction with store products.		
	Distortion	It refers to the process of disseminating false information about individuals.	Disseminating false criminal information about individuals that generated and gathered while their own identities were stolen or faked.		

Invasions	Intrusion	It refers to the process of intruding into individuals' private lives and interrupt their daily activities.	Interrupting individuals' seclusion through accessing the phone camera to recognize individuals' identities or displaying ads on the phone screen while individuals work on other apps.		
	Decisional interference	It refers to the process of interfering in personal decision-making.	As a result of identifying and tracking shoppers, the system starts recommending some products to shoppers to influence and change their choices.		

Appendix B: Survey invitation

Data Privacy in The Facial Recognition Technology (FRT) Age Needs Your Immediate Participation!

Hello!

I am presently conducting a research study to identify the most commonly used privacy-related keywords based on the framework of Solove's taxonomy in the context of Facial Recognition Technology (FRT). Approximately 500 subjects are needed to participate in this survey that should not take longer than 20 minutes of your time. This survey will ask you about demographic information (country of residence, gender, age, first language) and privacy-related keywords. Your participation in this survey is completely voluntary and greatly appreciated.

To be a qualified participant for this online survey, you must meet the following criteria:

- Your age is 18 or older.
- You are an English speaker.
- You have appropriate knowledge of how FRT works.

For further questions about the research, complaints, or problems, please do not hesitate to contact:

Researcher: Yazeed Alhumaidan, Dissertator at the University of Wisconsin-Milwaukee, at (414)-306-1519 – alhumai7@uwm.edu

Advisor: Dr. Xiangming "Simon" Mu, an Assistant Professor at the University of Wisconsin-Milwaukee, at (414) 229-6039 – mux@uwm.edu

You could access the online survey through this link:

Thank you in advance!

Yazeed Alhumaidan

Appendix C: Privacy-related keywords

Keywords	TF-IDF	Keywords	TF-IDF	Keywords	TF-IDF
Access	0.1	Exclude	0.46	Privacy policy	0.18
Accountability	0.28	Expectation	0.33	Privacy statement	0.21
Accuracy	0.14	Exploit	0.4	Private	0.11
Advertisement	0.02	Expose	0.19	Profiling	0.04
Aggregation	0.06	Fair use	0.89	Protection	0.17
Anonymity	0.03	Falsify	0.54	Publish	0.31
Approval	0.17	Force	0.32	Recognize	0.26
Attack	0.34	Fraud	0.21	Record	0.15
Authorization	0.11	Gathering	0.01	Release	0.22
Autonomy	0.95	Hacking	0.25	Reliability	0.43
Big brother	0.74	Identification	0.12	Required	0.39
Blackmail	0.42	Identity	0.1	Reveal	0.26
Capture	0.4	Impose	0.43	Safeguard	0.48
Choice	0.16	Inspect	0.39	Safety	0.24
Coerce	0.47	Integrity	0.41	Scan	0.31
Collect	0.00	Intimate	0.23	Search	0.37
Combine	0.22	Intrude	0.34	Seclusion	0.62
Compel	0.26	Invasion	0.15	Secondary use	0.1
Conceal	0.33	Isolation	0.27	Secrecy	0.36
Confidentiality	0.08	Knowledge	0.14	Security	0.19
Connect	0.2	Leak	0.07	Seizure	0.41
Consent	0.05	Link	0.12	Sell	0.06
Control	0.01	Mandatory	0.68	Sensitive	0.12
Dataveillance	0.43	Misidentify	0.44	Share	0.05
Deceit	0.87	Misleading	0.3	Snoop	0.48
Delete	0.19	Misrepresent	0.82	Solitude	0.35
Disclosure	0.02	Monitor	0.16	Spy	0.01
Disseminate	0.13	Notification	0.2	Stalk	0.37
Distort	0.5	Oblige	0.39	Surveillance	0.00

Distribute	0.44	Observation	0.13	Third party	0.07
Disturb	0.46	Option	0.27	Threat	0.18
Divulge	0.29	Other purpose	0.21	Track	0.00
Embarrass	0.53	Other use	0.36	Trustworthy	0.44
Enforce	0.17	Permission	0.03	Vulnerability	0.26
Erase	0.34	Privacy agreement	0.09	Watch	0.00

Appendix D: Intercoder agreement

Category	Total of cases	Agreements	%	Disagreements	%
Surveillance	20	18	%90	2	10%
Coercion	20	17	%85	3	15%
Retention Period	20	19	%95	1	5%
Profiling	20	20	%100	0	0%
Security	20	20	%100	0	0%
Secondary Use	20	19	%95	1	5%
Exclusion	20	19	%95	1	5%
Disclosure	20	19	%95	1	5%
Decisional interference	20	18	%90	2	10%
Total	180	169	%93.88	11	6.12%

Appendix E: Confusion matrix

Label	Confusion Matrix
Surveillance	accuracy: 94.15%

	true 1	true 0
pred. 1	66	3
pred. 0	21	320

Label	Confusion Matrix
Coercion	accuracy: 97.80%

	true 0	true 1
pred. 0	346	7
pred. 1	2	55

Label	Confusion Matrix
Retention Period	accuracy: 99.51%

	true 0	true 1
pred. 0	385	1
pred. 1	1	23

Label	Confusion Matrix
Profiling	accuracy: 99.02%

	true 0	true 1
pred. 0	357	4
pred. 1	0	49

Label	Confusion Matrix
Security	accuracy: 98.29%

	true 0	true 1
pred. 0	348	7
pred. 1	0	55

Label	Confusion Matrix
Secondary Use	accuracy: 99.02%

	true 0	true 1
pred. 0	378	4
pred. 1	0	28

Exclusion

accuracy: 97.56%

	true 0	true 1
pred. 0	367	10
pred. 1	0	33

Disclosure

accuracy: 99.27%

	true 0	true 1
pred. 0	359	3
pred. 1	0	48

Decisional Interference

accuracy: 98.05%

	true 0	true 1
pred. 0	359	6
pred. 1	2	43

CURRICULUM VITAE

Yazeed M. Alhumaidan

Place of birth: Riyadh, Saudi Arabia

Education

B.A., King Saud University, August 2011

Major: Information Science

MS., Sacred Heart University, June 2016

Major: Computer and Information Technology

Dissertation Title: A New Framework of Privacy Concerns Assessment in The Context of Facial Recognition Technology (FRT): Mixed-Methods Sequential Exploratory Analysis of YouTube Users.

Publication

Alhumaidan, Y., Dowell, M., Rene, J., Leverett, L., Ridenour, L., Schlais, V., ... & Smiraglia, R. P. (2018). Knowledge Organization and the 2017 UDC Seminar: An Editorial. KO KNOWLEDGE ORGANIZATION, 45(4), 273-280.