2022

Why Congress has not Passed Facial Recognition Technology Legislation for Public Spaces

Kecia Treviri Robertson
Walden University

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Kecia Treviri Robertson

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Michael Brewer, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Joshua Ozymy, Committee Member,
Public Policy and Administration Faculty

Dr. Lydia Forsythe, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Why Congress Has Not Passed Facial Recognition Technology Legislation for Public Spaces

by

Kecia Treviri Robertson

MBA, Troy University, 2001

BS, Troy University, 1998

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Homeland Security

Walden University

May 2022

Abstract

Facial recognition technology (FRT) in public spaces has been a political and social concern for more than 30 years. Conflict exists between the use of FRT for safety and security measures and its possible violation of the First, Fourth, and Fourteenth Amendments. Additional controversial issues surrounding the use of FRT in public spaces include technological development without standardization or regulations; biometric algorithms developed with bias; and the social issues of privacy intrusion, gender and racial bias, data security, accuracy, and privacy concerns. Researchers have concurred a national policy is needed to address FRT issues but have not explained why Congress has been unsuccessful. The purpose of this qualitative case study was to explore the factors explaining this phenomenon. The narrative policy framework was used as the theoretical paradigm for this inquiry. Using Saldana's method of coding, categorizing and theming descriptive narratives, transcripts from hearings conducted by the U.S. House of Representatives Committee on Oversight and Reform tasked with formulating FRT legislation were analyzed. The result of the analysis was the emergence of 10 factors identifying why FRT legislation was stalemated in Congress. The summative assertion from the factors revealed members of the committee were overwhelmed with the complexities of FRT. Several strategies were recommended which may advance the passage of a national FRT policy. If Congress employed these strategies and passed a national policy that alleviated FRT issues to the extent possible, positive social change regarding FRT usage in public spaces may occur.

Why Congress Has Not Passed Facial Recognition Technology Legislation for Public Spaces

by

Kecia Treviri Robertson

MBA, Troy University, 2001

BS, Troy University, 1998

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Homeland Security

Walden University

May 15, 2022

Dedication

It is with genuine gratitude and warm regard that I dedicate this work to my beloved son, Ryan Garrett Robertson, and loving sister, Yataisha Feleese Robertson. An incredibly special appreciation to my rock, the role model that engrained the seed for my life, my loving mother, Bernice Robertson. Thank you for continuously encouraging me to be a better me and showing me how to eliminate any barriers. As a result of you demonstrating arduous work and sacrifice, I was taught to use resilience and fortitude to push through any challenge. If it were not for the three of you being my greatest cheerleaders with encouragement, invaluable wisdom, and advice, I would not have survived this voyage. This dissertation is devoted with unconditional love to you and to my Almighty God. For without him providing me strength, direction, patience, and a brainchild to research, this would not have come to fruition. Again, thank you for your unwavering support and belief in me! Love you all!

Acknowledgements

I want to acknowledge and show appreciation to the faculty and staff at Walden University who assisted me in the right direction of my academic career. A special thank you to my advisors, Binh Ngo, and Jacqueline Cook-Jones. I would like to express my sincere gratitude to my doctoral committee. Dr. Michael Brewer, chair: for your insightful feedback and guidance, even when I wanted to give up. In memory of Dr. Kevin Fandl, who started this journey as my second committee member (SCM) but was called to become one of Gods angels. Dr. Joshua Ozymy, SCM, who jumped right in and picked up where Dr. Fandl left off to conclude this process with me. Dr. Lydia Forsythe, University Research Reviewer (URR) for ensuring this is a quality research study. Without all of you, this endeavor and envision to become a “change agent” would not have developed into a triumph. Pursuing this study taught me we all have the ability; the difference is how we use it. I wish you all much continued success!

Table of Contents

List of Tables v

List of Figures vi

Chapter 1: Introduction to the Study 1

Background 4

Problem Statement 7

Purpose of Study 9

Research Question 9

Framework for the Study 10

Nature of the Study 11

Definitions 12

Assumptions 15

Scope and Delimitations 16

Limitations 17

Significance 17

Summary 18

Chapter 2: Literature Review 19

Literature Search Strategy 20

Theoretical Foundation 21

Theory's Derivation 22

Fundamentals of the Theory 23

Levels of Analysis 24

Impact of the Media on Narrative Politics 25
NPF: The Right Choice 26
Literature Review Related to Key Concepts 27
History of National Facial Recognition Technology Legislation from 1997 – 2020 27
Historical Development of Facial Recognition Technology 32
How Facial Recognition Technology Works 34
Current Facial Recognition Technology Applications in Public Spaces and Formats 35
Controversies Surrounding Facial Recognition Usage in Public Spaces 43
Facial Recognition Usage Addressed by the Courts 52
Facial Recognition Usage Addressed by States and Municipalities 56
Current Federal Facial Recognition Technology Guidelines 58
The Need for a National Facial Recognition Technology Policy 59
The Need for Relevant Research on Issues Preventing the Passage of a National Facial Recogination Technology Policy 60
Summary and Conclusion 61
Chapter 3: Research Method 64
Research Design and Rationale 65
Role of the Researcher 66
Methodology 67
Participant Selection/Sampling Strategy 68

Instrumentation 70
Data Analysis Plan 71
Issues of Trustworthiness 73
Summary 74
Chapter 4: Results 75
Setting 75
Demographics 75
Data Collection 76
Data Analysis 78
Inductive Migration From Codes to Categories and Themes 78
Emergent Codes, Categories and Themes 79
Themes from Analysis of Codes and Categories 81
Evidence of Trustworthiness 84
Results 86
Research Question: Why Has Congress Failed to Pass a National Facial Recognition Technology Policy and How Is the Public Affected? 86
Factors that Explain Why Congress Failed to Pass a National Facial Recognition Technology Policy and How the Public Is Affected? 86
Summary 100
Chapter 5: Discussion, Recommendations, and Conclusion 105
Interpretation of Findings 105
Assertion from the Finding 106

Analysis of the Findings and the Theoretical Framework 113

Limitations of the Study.....114

Recommendations.....114

Implications of Positive Social Change 115

Conclusion 116

References.....118

Appendix A: Hearing Transcript Part I.....143

Appendix B: Hearing Transcript Part II.....160

Appendix C: Hearing Transcript Part III 176

List of Tables

Table 1. Codes and Categories From Data Analysis 80

Table 2. Inductive Migration of Categories to Themes and Factors..... 100

Table A1. Part I: Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces..... 146

Table A2. Part I: How the Public is Affected 155

Table B1. Part II: Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces..... 163

Table B2. Part II: How the Public is Affected..... 171

Table C1. Part III: Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces..... 179

Table C2. Part III: How the Public is Affected..... 186

List of Figures

Figure 1. Hearing Transcript Data Collection Instrument: Why has Congress Failed to Pass a National FRT Policy? 77

Figure 2. Hearing Transcript Data Collection Instrument: How the Public is Affected... 77

Figure 3. Congress is Overwhelmed With FRT Complexities 113

Figure A1. Hearing Transcript Part I: Facial Recognition Technology – Its Impact on our Civil Rights and Liberties 143

Figure B1. Hearing Transcript Part II: Facial Recognition Technology – Ensuring Transparency in Government Use 160

Figure C1. Hearing Transcript Part III: Facial Recognition Technology – Ensuring Commercial Transparency and Accuracy 176

Chapter 1: Facial Recognition Technology in Public Spaces

The use of facial recognition technology (FRT) in public spaces presents controversial problems among the public (Buolamwini & Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015). Controversial problems surrounding the use of FRT include technological development without standardization or regulations (Singh, 2018); biometric algorithms developed with bias (Omoyiola, 2018); and the social issues of privacy intrusion, gender and racial bias, data security, accuracy and privacy concerns, and the chilling effect (Buolamwini & Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017). Prominent among the issues is the privacy protection concern associated with the Fourth Amendment and the expectation of privacy (Wynn, 2015). The issues are considered FRT harms to the individual, which must be mitigated for the fair and accurate use of FRT in public spaces (Collins, 2019; Martinez-Martin, 2019).

The digitization of information, which makes FRT possible along with a multiplicity of applications, is one of the most important technological developments of modern society (Donohue, 2017). At the same time, this “non-option” to participate in this technology has created challenges to its uses, spearheaded by the reasonable expectation of privacy guaranteed by the Fourth Amendment (Donohue, 2017). Challenges permeate multiple aspects of daily living such as the use of computers and the Internet including emails (Donohue, 2017). Owners of smart devices such as cellphones, homes, appliances, televisions, medical equipment, and cars seek the “effects” coverage of the Fourth Amendment (Ferguson, 2017).

However, the proliferation of the use of FRT in public venues without the knowledge or the consent of the public transforms the individual into an unwilling participant in a perpetual line up that probe their biometric characteristics for a match in reference databases containing millions of images (Leavens, 2015). Here, problems of privacy intrusion, misidentification, misinformation, data security, gender and racial bias, and physical and emotional freedom of expression occur (Das et al., 2017). Recognizing that the biometric foundation of FRT is flawed, Kloppenburg and Van der Ploeg (2018) declared these inaccuracies and biases exist because there is no national policy to provide direction.

The need for a federal policy regulating the use of FRT has been recognized as a necessity to safeguard the public's interests, especially since self-regulation of the industry does not work in addressing issues of civil liberties (Wright, 2019). The need for governmental leadership to address the lack of uniformity in guidance and laws across the nation was acknowledged by Nakar and Greenbaum (2017). Despite the concerns, legislation to establish FRT regulations and mitigate related controversial problems have not been enacted at the federal level to date (Nakar & Greenbaum, 2017). The purpose of this qualitative study is to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces in the United States (Hamann & Smith, 2019; Wright, 2019).

This study will aid in informing and influencing political actors to address the controversial problems with FRT (Buolamwini and Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh,

2018; Wynn, 2015) and pass inclusive regulatory FRT legislation (Collins, 2019; Martinez-Martin, 2019). The potential social implications of the study are the emergence of a public that can enter public spaces without concern for FRT activities that interfere with their quality of life (EPIC, 2020; Wright, 2019).

There are five major sections in Chapter 1. The first major section is the problem statement, which establishes the reason for this study and identifies the gap in the literature regarding the factors that interfere with the passing of FRT legislation at the federal level. The second major section of the chapter is the research question, which directed the path and all processes necessary to answer the question. The third major section of the chapter includes the theoretical framework that assisted in identifying the answer to the research question. The fourth major section of the chapter describes the narrative policy framework (NPF), the paradigm used to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces (Shanahan et al., 2018, as cited in Weible & Sabatier, 2018). By applying the rudiments of the NPF through the utilization of the case study research design, these factors were expected to emerge with clarity (Crow et al., 2017; Jones & McBeth, 2020). Important also is the fifth major section of the chapter, which is the assumptions section. Establishing assumptions about what the study contained and what it did not was essential in keeping me focused and directed toward achieving the goal of answering the research question (Bengtsson, 2016).

Background

Selected articles related to FRT development and utilization, and the social issue of privacy intrusion and the expectation of privacy, are described below. The keywords and phrases researched for the study were *facial recognition technology, biometric algorithms, Fourth Amendment, expectation of privacy, recent technology affecting privacy laws, privacy attitudes and behaviors, law enforcement surveillance, federal FRT laws, social issues and FRT usage in public spaces, and Congressional committees.* They were researched in the Walden Library database and multiple peer-reviewed journals.

Carter (2018) reviewed a single law enforcement agency to examine FRT utilization benefits to public safety and the possible reaction by the public to the utilization of real-time FRT in the subway system, joining its use in other public spaces. Carter identified acceptance of real-time FRT utilization by the majority as the challenge facing the agency, although unresolved issues of privacy, data inaccuracies, and misuse by personnel exist. Hamann and Smith (2019) described how FRT works, the investigative uses of the technology, the legal issues associated with FRT utilization, including the Fourth Amendment expectation of privacy, and the First Amendment freedoms, and data aggregation concerns. The need to achieve a balance between FRT utilization and the unresolved concerns that hamper appropriate FRT regulations was identified (Hamann & Smith, 2019).

Horton (2018) examined cell site location information (CSLI) tracking by law enforcement to present a survey of applicable jurisprudence to justify and dispute the legality of the utilization of this digital technology and to assess the expectation of

privacy among individuals regarding CSLI tracking. Litt (2016) reviewed GPS tracking and metadata collection and concluded that these tools of the information age violated an individual's expectation of privacy. Leavens (2015) questioned the use of technological advancement in surveillance and other safety measures that may be invasive and outside the textual construct of the Fourth Amendment, which could be considered outdated for modern society. Leavens (2015) assisted in identifying the challenges to national security that have been created because of innovative technologies and the expectation of privacy by American citizens.

Kloppenburg and Van der Ploeg (2020) indicated that the functionality of the biometric system is flawed and resulting errors are inappropriately attributed to an ingrained gender and racial bias of the application taunted by privacy advocacy groups and other opponents of FRT utilization. In recognizing the biometric functionality issue, the perception of harms this malfunction creates for the individual is scrutinized (Kloppenburg & Van der Ploeg, 2020).

Martinez-Martin (2019) analyzed the application of FRT in privacy data protection. The use of FRT software for privacy data protection intended to securely predict the behavior, health, and emotions of patients upon presenting themselves to a health environment revealed the following results: data bias questioned the truthfulness and authenticity of the information being collected; the lack of an informed consent process led to ethical issues; and the utilization of the software was challenging (Martinez-Martin, 2019).

Nakar and Greenbaum (2017) emphasized the need for governmental leadership in resolving the fragmentation in guidance and laws regarding FRT development and utilization and addressed the conflicts between privacy and the benefits of FRT, noting the harm inaccurate data and security breaches can create for individuals. Best industry practices are urged until federal regulations can be enacted (Nakar & Greenbaum, 2017). Segovia (2015) urged the unification of privacy law on the national level that will safeguard the privacy of individuals and the formation of a privacy commission before FRT development and utilization legislation can be formulated. With the privacy law and commission in place, assurances that innovative technology can be developed without corporate costs and gains usurping individual privacy protections afforded by the unified privacy law can be realized (Segovia, 2015).

Wright (2019) noted that self-regulation of the FRT industry and utilization was inadequate to ensure that the civil liberties of individuals are not disregarded. Wright urged collaborative federal regulations so the FRT could flourish without creating unwarranted circumstances for individuals. Wynn (2015) concluded that an individual's identity cannot be safeguarded in the presence of FRT in public places for surveillance purposes. Wynn proposed the enactment of a privacy law which included how FRT may be used for surveillance. Once this is accomplished, a federal law regulating the development and utilization of FRT, enhanced by privacy protections, should be enacted (Hamann & Smith, 2019; Wynn, 2015).

Problem Statement

For more than 3 decades, Congress has undertaken legislation to address the use of FRT in public spaces (Congress.Gov, 2020). Among 118 bills, only 12 of them, or 11%, have become law, and none of the laws passed addressed the social issue of privacy intrusion stimulated by FRT usage in public spaces (Congress.Gov, 2020). Wynn (2015) concluded an FRT law cannot pass that mitigates the privacy issue until the identification of jurisprudence regarding obsolete privacy protection laws are reviewed by lawmakers and updated. Segovia (2015) agreed that a privacy protection law updated to accommodate the changes in modern technology must be the precursor to the passage of federal legislation regulating FRT usage in public spaces.

Martinez-Martin (2019) further identified the problem with passing a national FRT policy: the issues need the attention of lawmakers at the federal level that is purposeful and consistently moving toward compatible outcomes. Carter (2018) described this purposeful mobility as finding a balance between FRT and privacy intrusion. However, Wright (2019) noted that not enough is known about the attention these issues are getting from lawmakers at the federal level (Politico, 2020). Hamann and Smith (2019) concurred that identifying the issues with passing federal regulations is necessary for the elimination of the ambiguity that exists among proponents and opponents of a national FRT policy.

Buolamwini and Gebru (2018), Kloppenburg and Van der Ploeg (2018), Murphy (2018), Omoyiola (2018), and Singh (2018) discussed why uncertainty about issues with passing a national FRT policy is a problem. Kloppenburg and Van der Ploeg explained

the biometric foundation of FRT is flawed with inaccuracies and bias and will continue if the United States is void of national direction and policy. Extracted from Kloppenburg and Van der Ploeg's remarks are additional controversial problems rudimentary in the flawed biometric foundation of FRT: technological development without standardization or regulations (Singh, 2018); biometric algorithms developed with bias (Omoyiola, 2018); gender and racial bias (Buolamwini & Gebru, 2018); data security, accuracy, and privacy concerns (GAO, 2020); and the chilling effect (Murphy, 2018).

Wright (2019) declared that rigorous national policy addressing the issues was needed to safeguard the interest of the public. Nakar and Greenbaum (2017) emphasized the need for governmental leadership to resolve the fragmentation in guidance and laws across the nation regarding FRT usage in public spaces and allay the prominent social issue of privacy intrusion. Wright noted that issues must be resolved because self-regulation of the FRT industry and utilization are inadequate to ensure the civil liberties of individuals are not disregarded.

The problem addressed in this study was the consensus that a national FRT policy is needed (Nakar & Greenbaum, 2017; Wright, 2019) but it was unknown why Congress has not passed legislation addressing the use of FRT in public places in the United States (Buolamwini & Gebru, 2018; Kloppenburg & Van der Ploeg, 2018; Murphy, 2018; Omoyiola, 2018; Singh, 2018). The gap in the literature was the unknown factors explaining why Congress has not passed national FRT legislation (Murphy, 2018; Roussi, 2020). This study filled the gap in the literature by identifying obstacles to passing a national FRT policy that include privacy protection legislation at the federal level and

addressed the identified controversial problems surrounding the use of FRT in public spaces (Buolamwini & Gebru, 2018; GAO, 2020; Hamann & Smith 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015). Kloppenburg and Van der Ploeg (2020) described the need to become aware of all the elements involved in implementing the FRT method of establishing a person's identity and to determine how political and ethical (social) questions were defined or redefined to correlate with innovative technologies. Wright (2019) urged collaborative federal regulations through clarity of the issues so the FRT can flourish without creating unwarranted circumstances for individuals. Zeng et al. (2019) concluded that identifying and discussing the controversial and disconcerting issues regarding FRT and its benefits to society is necessary so regulation of the industry can occur.

Purpose of Study

The purpose of this qualitative study was to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public places in the United States. A case study of the concerns, emotions, and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform was conducted to identify factors imploding the passage of legislation during the policy formulation process.

Research Question

RQ: Why has Congress failed to pass a national FRT policy and how is the public affected?

Framework for the Study

The NPF was the theoretical paradigm for this study. NPF is described by Shanahan et al. (2018, as cited in Weible & Sabatier, 2018) as the influential operation that unobtrusively directs the policy formulation process. Described by Blair and McCormack (2016) as a theatrical melodrama, the NPF in action identifies the political arena as a stage of actors consisting of villains and victims who pontificate their political opinions. Through this discourse, political agendas are expounded, and policies are either formulated to become law or "upstaged" and rejected (Blair & McCormack, 2016).

Jones and McBeth (2020) described the NPF as a framework to help the researcher understand the political stage. By studying the narratives of the political actors, the researcher became cognizant of purposeful communication among individuals intended to influence policy formulation (Jones & McBeth, 2020). The factors preventing the passage of federal legislation to regulate FRT and addressing the related issues were imbedded in the narratives of congressional members (Hamann & Smith, 2019). One way to gather information about these narratives and issues was to conduct a case study of the concerns and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform utilizing the archival records of the committee hearings on *The Use of Facial Recognition Technology (FRT) in Public Spaces and the Identification of Obstacles to the Passage of Federal Policy Regulating the Development and Utilization of Facial Recognition Technology*on (Congress.Gov, 2020; Crow et al., 2017). Significant to this study was the application of the NPF to identify the narratives used to explore the factors

that prevented the passage of federal legislation to mitigate the FRT, privacy protection, and other controversial problems (Buolamwini & Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Jones & McBeth, 2020; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015).

Nature of the Study

The qualitative research method was applied for this study. O'Sullivan et al. (2017) described the qualitative research method as one that provides flexibility to the researcher, permitting a change in data analysis procedures toward the direction of the data if applicable. Rather than relying upon statistical significance, the qualitative research method permits the researcher to discover veracity in concepts through words and themes (O'Sullivan et al., 2017). The researcher is also permitted to arrive at conclusions and propose the solution to the research problem through narratives of the research subjects (O'Sullivan et al., 2017). The NPF favored this type of research method. Inferences from narratives and viewpoints were integral to the qualitative research method (Schoonenboom & Johnson, 2017) and the essence of the NPF melodramatic political process (Blair & McCormack, 2016).

The qualitative research method also aligned with the problem statement and the research question through a case study research design (O'Sullivan et al., 2017). The case study facilitated the exploration of the issues affecting the passage of federal legislation that addressed FRT usage in public spaces (see Yin, n.d., as cited in O'Sullivan et al., 2017). The concerns, emotions, and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors were

revealed through the examination of the Committee on Oversight and Reform hearing transcripts utilizing the case study research design (see Yin, n.d., as cited in O'Sullivan et al., 2017). The case study research design facilitated an inductive approach toward why federal legislators have not enacted a solution (Laureate Education [Producer], 2014-a). Harrison et al. (2017) acknowledged that the case study research design provides the researcher with the pliancy to conduct an extensive query if appropriate to define similarities in the case. O'Sullivan et al. (2017) noted the case study research design allows the researcher to observe how and why something happened with the passage of FRT legislation, specifically, the federal lawmakers' issues regarding privacy protection and the assuagement of the identified controversial problems surrounding the use of FRT in public spaces (Buolamwini & Gebru, 2018; GAO, 2020; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015). Following are definitions of terms specific to this study.

Definitions

Anecdotes are short intrinsically persuasive stories told of real incidents to clarify policy and public opinions (Jones & McBeth, 2010). Anecdotal information is acceptable in formulating the narrative in the NPF applicable in this study.

Biometrics are unique physical characteristics (face, voice, fingerprints, iris, etc.) used to digitally identify a person (Blanco-Gonzalo et al., 2018).

Biometric algorithms are mathematical designations of biometric characteristics of individuals which are used in the process of recognizing an individual through digitized technology (Das et al., 2017).

Biometric galleries are biometric database storage systems of samples collected by law enforcement (Introna & Nissenbaum, 2009).

Biometric probes are the digital capture of characteristics or images used to verify or match individuals with characteristics or images already in a reference database. A common probe image is the face (Introna & Nissenbaum, 2009).

Chilling effect is the physical and emotional response by individuals who discover their expectation of freedom and anonymity in public spaces have been curtailed by the presence of FRT filtering their images through a reference database (Nakar & Greenbaum, 2017).

Congressional committee hearings are open meetings or sessions of the Senate, House, or joint or special committee of Congress to conduct investigations, propose new legislation, and evaluate other activities of federal law (Congress.Gov, 2020).

Data aggregation is the process of gathering raw data to create new summarized data (Spencer, 2015).

Data bias occurs when datasets that create biometric templates are not inclusive or extensive enough to eliminate race, gender bias, and lack demographic diversity, making the data systematically prejudiced or erroneous (Buolamwini & Gebru, 2018).

Expectation of privacy is an individual's reasonable presumption of privacy protection of the Fourth Amendment from warrantless searches of places and seizures of persons and possessions (Zeng et al., 2019).

Facial recognition technology (FRT) is technology used to match a digital image of a human face encoded by an algorithm stored in a database to confirm the identity of a face (Congress.Gov, 2020).

Homo narrans is another name for a "storytelling human" (Shanahan et al., 2017).

Narrative policy framework (NPF) is a theoretical postulate consisting of theatrically analyzed stories in the political arena which impact the creation of policy (Shanahan et al., 2017).

Components of NPF include:

1. *Setting* is the space where action takes place (Shanahan et al., 2017). The venue in this study is the floor of the house testimonies.
2. *Plot* is the event in which the characters interact within the setting, and they are unaware or may undergo undue harm (Shanahan et al., 2017). The policy problem is the plot in this study.
3. *Characters* in the study are labeled as victims, villains, and heroes (Shanahan et al., 2017). In this study, the victims harmed by a particular action are the citizens. The villains creating the harm are the lawmakers. The potential heroes advocating the system to provide relief are the Congressional Committee members and other advocates that provided testimony.
4. *Moral of the story* gives purpose to the characters, actions, and motives (Shanahan et al., 2017). The policy solution is the moral of the story in this study.

PEW is a nonprofit, nonpartisan, and nonadvocacy research center that conducts research using public opinions on issues trending in the world (Pew Research Center, 2021).

Political actors are individuals and institutions that perform within political systems and make or influence policy formulation, enactment, publicity, and acceptance. Political actors are intricately involved in the NPF policy formulation process and analysis (Blair & McCormack, 2016).

Public space is an area open and accessible to any individual (Vitiello, 2018).

Purposive sampling technique is applied when the researcher relies on their own judgment to choose a population to study (Etikan et al., 2016).

Textual data are databases comprised of the transcription of collections of written, printed, or published words. The transcripts of the Congressional Committee hearings are the textual data utilized to conduct the case study in this research (Congress.Gov, 2020).

U.S. House of Representatives Committee on Oversight and Reform is the Congressional group that takes subject matters within the legislative jurisdiction to review, monitor, supervise, and investigate federal agencies, programs, and policies to ensure compliance (Congress.Gov, 2020). In this study, the Congressional Committee members are potential heroes in the NPF scenario.

Assumptions

Critical to the meaningfulness of this study was the methodological assumption in conducting the study utilizing the qualitative research process (Qualitative Practice, n.d.). By employing the qualitative research method, each of the composites of the

methodological assumption was applied, namely, inductive reasoning, mutual simultaneously shaping factors, and emerging themes, all of which were context bound but not rigid (Qualitative Practice, n.d.). The case study research design was used to explore the research question. This design permitted the ontological assumption that factors explaining why Congress has not passed a national FRT policy existed and the epistemological assumption that valid factors would be identified (Cleland, 2017).

The research was conducted with the assumption that the case study had an elevated level of reliability because the exploration was conducted within a bound system of archival records (Harrison et al., 2017). Another assumption was the research method and design promoted credibility, dependability, transferability, and confirmability to establish trustworthiness in the study (see Lincoln & Guba, 1985, as cited in Bengtsson, 2016).

Scope and Delimitations

This case study of the concerns, emotions, and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform focused on the factors preventing the passage of federal legislation to regulate FRT in public spaces (Hamann & Smith 2019). Transcripts from the committee hearings were identified from the sample of introduced, read, assigned to committee, and enacted legislation which specifically included the phrase “facial recognition technology” and addressed the controversial problems surrounding its usage in public spaces (Congress.Gov, 2020). Although no enacted legislation was identified, the Congressional Committee hearings on *The Use of*

Facial Recognition Technology (FRT) in Public Spaces and the Identification of Obstacles to the Passage of Federal Policy Regulating the Development and Utilization of Facial Recognition Technology was utilized as the sample for the study because of its ongoing, extensive hearings regarding FRT and related issues (Congress.Gov, 2020). By limiting the study to this purposively selected sample, the researcher remained focused on the source of data relevant to the purpose of the study expressed in the research question (Alpi & Evans, 2019).

Limitations

Potential challenges to the study included assuring the transcripts of the appropriate Congressional committees had been selected and the ability to conclude the research while efforts to formulate a federal policy were still stagnated in Congress (Congress.Gov, 2020). A limitation of the study was the lack of direct affiliation with members of the committee. The lack of affiliation with members of the committee facilitated objective monitoring of the research process and diminished any bias or other ethical issues (Gerke et al., 2020; Qualitative Practice, n.d.).

Significance

This research filled a gap in knowledge by exploring and identifying the obstacles to passing a national FRT policy that included privacy protection legislation at the federal level and address the identified controversial problems surrounding the use of FRT in public spaces (Buolamwini & Gebru, 2018; GAO, 2020; Hamann & Smith 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015). By conducting a case study of the appropriate FRT-related Congressional committee, the research provided

insight into the stagnated policy process for federal regulation of FRT (Harrison et al., 2017). The analysis also provided insight into the obstacles that must be mitigated to pass federal legislation that addressed the FRT use in public spaces and the prominent social issue of privacy intrusion/expectations of privacy, as well as the controversial problems rudimentary in the flawed biometric foundation of FRT (Kloppenburg & Van der Ploeg, 2018).

Summary

The use of FRT in public spaces presents controversial problems among the public, including the issue of privacy protection. Literature related to the scope of the problem was presented in the background to support the problem and the purpose of this study (Buolamwini & Gebru, 2018; GAO, 2020; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015). The research question and theoretical framework to answer the question were discussed (Shanahan et al., 2018). The qualitative research method and the case study research design were introduced in the nature of the study (Crow et al., 2017; O'Sullivan et al., 2017). Definitions of terms and processes used in conducting the research were presented to assist in providing clarity in the research study, especially in the assessment of trustworthiness (Walden University, 2016). Assumptions about the study and its qualitative peculiarities were presented, including the study's scope and delimitations, limitations, and significance (Qualitative Practice, n.d.).

Chapter 2 presents a review of the literature relevant to the problem, purpose, and research question of the study. The chapter also includes the literature search strategy, the theoretical framework for the study, and a summary.

Chapter 2: Literature Review

The problem researched in the Literature Review was the unknown factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces in the United States (Wright, 2019; Wynn, 2015). The purpose of this qualitative study was to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces, including the prominent privacy protection problem and other controversies surrounding the use of FRT, which include technological development without standardization or regulations, biometric algorithms developed with bias, gender and racial bias, data security, accuracy and privacy concerns, and the chilling effect (Buolamwini & Gebru, 2018; Hamann & Smith 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015).

In this chapter, legislation involving FRT was surveyed from 1997 to 2020. The purpose of the survey was to review the types and extent of the authorizations by the government to use biometric data and to determine if any of the authorizations addressed the privacy and other controversial problems (Congress.Gov, 2020). The history of the development of FRT (Dharaiya, 2020) and how the technology works (Singh, 2018; Wright, 2019) were reviewed to enhance knowledge of the technology and the concern with standards for development.

The expansion of the use of FRT by the government was reviewed beginning with those necessitated by the events of 9/11, namely the terrorists watch list, custom and border protection, and airport security (Department of Justice [DOJ], 2020). Other common uses of FRT were studied, including law enforcement surveillance, social media

enhancements, mobile phones authentication, and patient and student management and safety (Andrejevic & Neil, 2019; Hamann & Smith, 2019; Martinez-Martin, 2019; Norval & Prasopoulou, 2017; Robertson, Kramer & Burton, 2015). A major section of the chapter is the review of court cases at all levels of government for content to determine if any of them regulated the development of FRT or addressed the controversial problems (Nakar & Greenbaum, 2017). Emphasis was also repeatedly placed on the controversies surrounding the use of FRT in public places; however, the privacy intrusion and the expectation of privacy were prominently reiterated in this review because of the strong Fourth Amendment underpinning elements for all the allegations of FRT harms (Zeng et al., 2019). For this reason, the court cases reviewed have been decided based upon the Fourth Amendment's expectation of privacy interpretation relevant to the specific case (Justia, 2019). Research and reports concerning the identification of the issues preventing the passage of FRT were also emphasized (Wright, 2019).

Literature Search Strategy

Selected articles related to FRT development and utilization, related court cases, and the controversies surrounding FRT usage, especially the social issue of privacy intrusion and the expectation of privacy, are described below (Wynn, 2015). The keywords and phrases researched for the study were *facial recognition technology, biometric algorithms, biometric databases, facial recognition technology legislation, Fourth Amendment, expectation of privacy, innovative technology affecting privacy laws, privacy attitudes and behaviors, law enforcement surveillance, federal FRT laws, court*

cases involving FRT usage, social issues and FRT usage in public spaces, 9/11 and *The USA PATRIOT Act.* These were researched in the Walden Library database and multiple peer-reviewed journals.

A wide range of articles and other resources were reviewed for this study. Terms were also researched through Google Scholar and ProQuest for dissertations. These terms included *narrative policy framework, policy narratives, narrative methodology, theories of the policy process, Congressional hearings related to FRT development and utilization, case study, legislation, privacy intrusion, privacy issues, privacy protection laws, national policies, social issues, digitized technology, sharing of information, social awareness, policy making process, policy formulation, policy implementation, policy evaluation, policy decision making, advocacy coalition, positivist approach, Congressional members, the U.S. House of Representatives, Committee on Oversight and Reform and transcripts.* These terms led to supplementary resources through exploring the keywords of *government policy, narratives, democracy, postmodernism, policy sciences, political systems, frame analysis, policy reframing,* and *theory of change*. The theoretical foundation, literature review of the key concepts, summary, and conclusion relevant to the issues preventing the passage of FRT federal legislation are presented in this chapter.

Theoretical Foundation

The framework for this study was the NPF reported by Shanahan et al. (2018, as cited in Weible & Sabatier, 2018) as the focal point of the policy process that influenced policy formulation at different intervals of political decision-making through descriptive

stratagems from policymakers and advocacy coalitions (Weible & Sabatier, 2018). Blair and McCormack (2016) described the rudiments of NPF as corresponding to the theatrical presentation of a melodrama, complete with political victims, villains, and heroes who employed their narratives to avow or oppose political views, set political agendas, and formulate or impede policies (Blair & McCormack, 2016).

FRT, privacy protection, and other controversial problems were inundated with narratives from political actors (Congress.Gov, 2020). Efforts to identify these narratives in the examination of the transcripts from the U.S. House of Representatives' Committee on Oversight and Reform committee hearings were employed in this study. Further exploration of the NPF policy process provided insight into achieving the balance between FRT use in public spaces and the social issue of privacy intrusion/expectations of privacy prominent in this study (Wright, 2019).

Theory's Derivation

The NPF emerged as an alternative method to shaping public policy through the application of anecdotes (Jones & McBeth, 2010). Although under development in 2004, it was not fully developed until 2010 and was rapidly adopted in many peer reviewed academic journals (Shanahan et al.,2011). After several deviations of the method were applied, the final structure of the anecdotes was created and implemented by Mark K. McBeth, Michael D. Jones, and Elizabeth A. Shanahan (2011). McBeth, Jones, and Shanahan (2014) established the NPF to study the role of narratives in the policy process by pinpointing qualities customary to most narratives in policymaking and hypothesizing when narratives transpired and in what manner policy outcomes were regulated.

Shanahan et al. (2017) recognized the impact narratives have on political responses and listed five core assumptions of NPF operationalization as:

1. Perception of social construction.
2. Bounded relativity.
3. General structural elements.
4. Three levels of analysis; and
5. Homo narrans model of the individual (p. 333).

These core assumptions were an integral component in the conclusion of the study.

Fundamentals of the Theory

Understanding and operationalizing the fundamentals of the NPF theory mean developing a script for a play or movie and assuming the role of director (Shanahan et al., 2017). The storyline is composed of a beginning, a middle, and an end (Shanahan et al., 2018, as cited in Weible & Sabatier, 2018). Through the lens of NPF, the strategic story of policy formulation can be told (Shanahan et al., 2018, as cited in Weible & Sabatier, 2018). The lens signifies all stories have four facets: a setting, a plot, characters, and a moral (Shanahan et al., 2018, as cited in Weible & Sabatier, 2018). The setting is the context of the policy, its position on the political stage or the surroundings in which the policy is discussed (Ney, 2006; Ney & Thompson, 2000; Verweij & Thompson, 2006; Verweij et al., 2006, as cited in the Policy Studies Journal, 2018). The venues of the house testimonies served as the setting of this study. The plot is the interaction of events with the actions of the characters and setting (McBeth et al., 2005; Roe, 1994; Stone, 2002, as cited in the Policy Studies Journal, 2018). Characters in the political story

include victims that are harmed by the problem; villains, better known as enemies, cause the problem; and the heroes or allies who promise relief by mitigating the problem (Jacobs & Sobieraj, 2007; McBeth et al., 2005; Ney, 2006; Stone, 2002, as cited in the Policy Studies Journal, 2018). The moral of the story provides purpose to the characters, actions, and motives (Ney, 2006; Ney & Thompson, 2000; Stone, 2002; Verweij & Thompson, 2006; Verweij et al., 2006, as cited in the Policy Studies Journal, 2018). Once the union of political ideologies occurs, policy can be formulated (Kloppenburg & Van der Ploeg, 2018).

In this study, the venues in which the Congressional Committee hearings were conducted served as the setting (Shanahan et al, 2017). The plot was the interaction of events with the actions of the characters involved in formulating a policy while unaware of the obstacles preventing their success (McBeth et al., 2005; Roe, 1994; Stone, 2002, as cited in the Policy Studies Journal, 2018). The characters included: victimized society and citizens harmed by the use of FRT., villainous lawmakers opposing change in how FRT issues were managed, and the heroic Congressional Committee advocating change in FRT development and use without harming citizens (Shanahan et al., 2017). The moral of the story was a pathway to the elimination of the policy void by addressing the stagnating factors and the bipartisan passage of a national FRT policy (Shanahan et al., 2017).

Levels of Analysis

NPF is analyzed through the human interaction of three foundational levels. The levels are micro, meso, and macro (Shanahan et al., 2017). The micro level entails an

individual's interaction to the environment (Crow et al., 2017). Micro research is concerned with how individuals inform and are informed by policy narratives with the emphasis only on one's self-perception (Crow et al., 2017). Group or coalition interaction is known as the meso level (Shanahan et al., 2017). Meso research focuses on policy narratives with policy actors and outcomes (Shanahan et al., 2017). The macro level is comprised of cultural and institutional interaction (Crow et al., 2017). Macro research concentrates on how policy narratives are embedded in cultures and institutions to shape public policy (Crow et al., 2017). The components function concurrently at all three levels in the development of hypotheses (Jones & McBeth, 2010).

Impact of the Media on Narrative Politics

The media has a major impact on any policy change (Yeung, 2018). Forms of media include journals, magazines, newspapers, speeches, letters, television news reports, and social media – Facebook, Twitter, Instagram, Snapchat and TikTok – and provide a range of entertainment and information with and without bias (Yeung, 2018). Media has become so impactful in American society that it molds the conscientiousness and behavior of American citizens, including in the political environment (Shanahan et al., 2011, 2017).

An example of the influence media can have on the narrative of policy change is demonstrated using social and mainstream media by President Donald Trump to govern the United States in an extraordinary manner (Jones & McBeth, 2020). President Trump performed at all three levels of NPF analyses (micro, meso, and macro) as his narrative

navigated policy change in all facets of the governmental environment (Jones & McBeth, 2020).

NPF: The Right Choice

The framework hypothesis (Hanko, n.d.) and the advocacy coalition framework (ACF) were considered as the frameworks to conduct this study. In 1924, the framework hypothesis was first proposed by Dr. Arie Noordzij of the University of Utrecht (Hanko, n.d.). In the late 1950s, Nicolaas Ridderbos redefined its purpose in Europe (Hanko, n.d.). At the same time, the thoughts of Meredith Kline were viewed in the United States (Hanko, n.d.). The framework was thought to be an attempt to reinterpret the biblical text of Genesis 1 (McCabe & Chaffey, 2011).

The ACF focuses on the formation and change of coalitions (Shanahan et al., 2011, as cited in Policy Studies Journal, 2018). To influence outcomes, the ACF focuses on belief systems, policy learning, coalition resources, and strategy (Hirch et al., 2010; Jones & Jenkins-Smith, 2009; Policy Studies Journal, 2018; Sabatier & Jenkins-Smith, 1993). ACF is best utilized in positivist-oriented policies (Pierce et al., 2017).

Although the ACF has been updated to an actor centered approach, it does not assert the fundamentals of narratives – setting, plot, character, and the moral of the story (Chikowore, 2018) – and is not the best fit for this study. Behavioral considerations are fundamental to policy changes through the NPF (Moyer, 2019). Opinions help to define the policy problem (Moyer, 2019). The narrative portrays a vital position in human cognition and communication (Shanahan et al., 2017).

Prior applications of NPF have been used in various environmental topics (Moyer, 2019). Climate change, hydraulic fracturing, and recycling are just a few of those topics. The theory is beneficial in both policy analysis and policy process (Moyer, 2019). With the controversial policy debates surrounding FRT, NPF is the right choice to conduct a case study (Crow et al., 2017). It is also the right choice for the practical and methodological implications of the study (Shanahan et al., 2017).

Literature Review Related to Key Concepts

History of National FRT Legislation From 1997 – 2020

For more than 3 decades, the United States Congress has undertaken legislation to address the use of FRT in public spaces (Congress.Gov, 2020). Among approximately one hundred bills, only twelve of them have become law, and none of the laws passed addressed the controversial problems stimulated by FRT usage in public spaces with the issue of privacy intrusion at the forefront (Congress.Gov, 2020). Congressional action regarding FRT began in the 105th Congress (1997-1998) with the Department of Defense Appropriations Act, 1998. Introduced in and passed by the United States Senate (Senate) in July 1997, the act provided funds for the Defense Department to begin a FRT program throughout its defense purview. Two subsequent amendments to this act provided $5 million specifically for Research, Development, Test and Evaluations, Defense-Wide to establish the facial recognition program (Congress. Gov, 2020).

FRT or related legislation has been introduced in every Congress since the Department of Defense Appropriations Act, 1998 (Congress.Gov, 2020). During the 106th Congress (1999-2000), the 21st Century Justice Act of 1999 introduced in April

1999 contained a multiplicity of subtitled acts authorizing development and improvement in technology to fight crime (Congress.Gov., 2020). Specifically, Subtitle C: Crime Identification Technology Act funded systems technological improvements to capture real-time street crime (Congress.Gov, 2020). The Airline Security Act of 2001 was introduced in the 107th Congress (2001-2002) (Congress.Gov, 2020). The bill was introduced in the House and referred to the Committee on Aviation but was never passed (Congress.Gov, 2020). It contained directives to the Federal Aviation Administration to develop FRT to automatically profile travelers in efforts to airport security and thwart the boarding of potentially dangerous individuals (Congress.Gov, 2020).

The Senate of the 108th Congress (2003-2004) introduced and passed the Intelligence Reform and Terrorism Prevention Act of 2004 (Congress.Gov, 2020). Among many titles and subtitles was Title V: Border Protection, Immigration, and Visa Matters-Subtitle A: Advanced Technology Northern Border Security Pilot Program requiring the testing of advanced technologies to enhance border security (Congress.Gov, 2020). The House introduced and passed their version of the bill entitled 9/11 Recommendations Implementation Act (Congress.Gov, 2020). Both versions of the bill were negotiated in committee and became Public Law No: 108-458 signed by President George W. Bush (Congress.Gov, 2020). Stimson and Habeck (2016) described this Intelligence Reform and Terrorism Prevention Act of 2004 as legislation that did not go far enough to engage the opposition facing the intelligence community because of the 9/11 terrorists' attacks on the United States.

Senate bill S.1261- PASS ID Act was introduced in the 111th Congress (2009-2010) in June 2009 (Congress.Gov, 2020). The bill was read twice and assigned to the Committee on Homeland Security and Government Affairs (Congress.Gov, 2020). Appropriations for the Vital Records Digitization Grant Program for FY2011-FY2013 were included but failed to get out of committee (Congress.Gov, 2020). The Coast Guard Authorization Act of 2010 introduced in the 111th Congress (2009-2010) authorized the Coast Guard to use FRT to identify suspected terrorists and other individuals to improve security at the borders (Congress.Gov, 2020).

The Passport Identity Verification Act was introduced in the 112th Congress (2011-2012) Senate in April 2011 (Congress.Gov, 2020). The bill directed a study to be conducted to determine if biometric information should be required to obtain or renew passports (Congress.Gov, 2020). After two readings, the bill was referred to the Committee on the Judiciary but received no further action (Congress.Gov, 2020). The Department of Homeland Security (DHS) Reform and Improvement Act was introduced in 114th Congress (2015-2016) House in November 2016 (Congress.Gov, 2020). The bill was last referred to the Subcommittee on Biotechnology, Horticulture, and Research and received no further action (Congress.Gov, 2020). The use of FRT was required in screening VISAs and for use with other security measures (Congress.Gov, 2020).

The Securing America's Future Act of 2018, introduced in the 115th Congress (2017-2018) in January 2018, required the establishment of a biometric database to screen individuals departing the country at the borders (Congress.Gov, 2020). After two roll call votes, the bill failed to pass in the House (Congress.Gov, 2020). House bill

H.R.6136-Border Security and Immigration Reform Act of 2018 had similar intent (Congress.Gov, 2020). The bill was introduced in the 115th Congress (2017-2018) in June 2018 and included a provision for a Biometric Identification Transnational Migration Alert Program (Congress.Gov, 2020). After review by eight committees, including the Committees on Armed Services, Homeland Security and Foreign Affairs, followed by two roll call votes, the bill failed in the House (Congress.Gov, 2020). In November 2018, the Federal Police Camera and Accountability Act of 2018 was introduced in the House, referred to the Committee on the Judiciary and received no further action or summary of the bill (Congress.Gov, 2020). The intent of the bill was to authorize the use of video cameras in patrol cars and the wearing of body cameras by federal law enforcement officers (Congress.Gov, 2020).

Some of the more recent attempts to remedy this nihility at the national level included the Commercial Facial Recognition Privacy Act of 2019, which was introduced in the 116th Congress (2019-2020) Senate and sat dormant in the Committee on Commerce, Science, and Transportation (Congress.Gov, 2019). The intent of the bill was to restrict the sharing of FRT data obtained by commercial entities but did not include governmental restrictions (Conger, Fausset, & Kovaleski, 2019). Since March 2019, there has been some bipartisan attempts to introduce and pass FRT legislation to obtain consent from commercial customers before subjecting them to FRT and to require a search warrant if law enforcement intended prolonged surveillance of an individual (Senate RPC, 2019).

To limit the use of FRT for surveillance without a warrant, the Facial Recognition Technology Warrant Act of 2019 was introduced in the Senate 116th Congress (2019-2020) in November 2019 (Congress.Gov, 2020). The bill was referred to the Committee on Judiciary after two readings (Congress.Gov, 2020). No further action has been taken to date on this bill (Congress.Gov, 2019). Similarly prohibiting warrantless action was the Ethical Use of Facial Recognition Act which was introduced in the Senate in February 2020 in the 116th Congress (2019-2020) (Congress.Gov, 2020). The bill was read twice in the Senate and referred to the Committee on Homeland Security and Government Affairs with no further action (Congress.Gov, 2020). The bill prohibited the use of FRT by an agent of the Federal government without a warrant until rules establishing the use of the technology are made by a congressional commission (Congress.Gov, 2020).

The Artificial Intelligence (AI) Act of 2020 was introduced in the 116th Congress (2019-2020) Senate in May 2020 (Congress.Gov, 2020). It was referred to the Committee on Commerce, Science, and Transportation but received no further action and a summary of the bill was unavailable (Congress.Gov, 2020). Also introduced in the 116th Congress (2019-2020) House in May 2020 was the Advancing Facial Recognition Act (Congress.Gov, 2020). The bill authorized a study on FRT followed by a report of recommendations concerning public and private use (Congress.Gov, 2020). The bill was referred to the Committee on Energy and Commerce, Committee on Science, Space, and Technology, and the Committee on Foreign Affairs, and received no further action (Congress.Gov, 2020). At the other end of the spectrum, a bill entitled “To prohibit

Federal funding from being used for the purchase or use of facial recognition technology, and for other purposes" was introduced in the 116th Congress (2019-2020) House in July 2020 (Congress.Gov, 2020)**.** It was referred to the House Committee on Oversight and Reform and has received no further action (Congress.Gov, 2020).

In June 2020, the Facial Recognition and Biometric Technology Moratorium Act of 2020 was introduced in the 116th Congress (2019-2020) House and referred to the Committee on the Judiciary and the Committee on Oversight and Reform with no timetable set for action (Congress.Gov, 2020)**.** The bill prohibited the use of biometric surveillance and withheld federal funds from any state that used biometric surveillance (Congress.Gov, 2020). Simonite (2020) reported concern among some Congressional members that the bill was not strong enough to address possible misuse by law enforcement and disregarded rights of citizens. Schaffhauser (2020) reported that a University of Michigan study also recommended a ban on the use of FRT, especially in schools, because of the uncertainty of its use and its potentiality for bias against people of color.

Historical Development of FRT

FRT has undergone a metamorphosis of development beginning with the placement of face photographs on the RAND tablet, a predecessor of the iPad developed by the RAND corporation in the 1960s (Hochreutiner, 2019). Dharaiya (2020) discussed this system designed by Woodrow Wilson Bledsoe in which facial features such as mouth, nose, and eyes could be manually recorded with the emission of electromagnetic pulsations initiated by movement of a stylus across a computerized grid. Bledsoe's

introduction of a database to save the manual records contributed to Harmon, Goldstein, and Lesk's ability to expand the facial components in the 1970s to twenty-one markers, such as the density of the lips, for automatic facial detections (Dharaiya, 2020; West, 2017). In 1988, Sirovich and Kirby developed the Eigenface method of facial recognition by employing linear algebra to generate a composite of common features among multiple photographs (Kline, 2017). Additional development of the Eigenface method in 1991 improved its functionality and Pentland and Turk were credited with the first impactful attempt to automate facial recognition (Kline, 2017; Turk & Pentland, 1991).

Important to the historical development of FRT was closed-circuit television (CCTV), which had appeared in the technological industry as early as 1942 when Germany used it to observe weaponry behavior (Mesnik, 2016). By 1970s, the commercial use of CCTV, companioned with the videocassette recorder (VCR), was widely used in the retail industry as a surveillance tool to thwart theft (Bradford, 2020). CCTV was a low-cost technology that was highly labor intensive and would be impractical as the foundation of FRT (Wright, 2019).

The digitalization of video in the early 2000s hurried the use of FRT with the combination of CCTV basics and biometric technology (Bradford, 2020). Biometrics is the automated analysis of biological and behavioral attributes of individuals such as the face, fingerprints, the iris, and the voice (Blanco-Gonzalo et al., 2018). This computerized analysis of attributes is intended to identify and verify an individual based upon traits unique only to that individual (Kloppenburg & Van der Ploeg, 2018). The enthusiasm of the retail industry to use FRT went beyond surveillance and included ways

to increase revenue, such as access to databases that might create VIP lists to promote customer culture and spending (Future of Privacy Forum, 2018). The retailers' two-folded concern prompted the merger of the private and public sectors in developing FRT in the United States (Wright, 2019). The Defense Advanced Research Projects Agency (DARPA) funded this private-public research merger for about thirty years beginning in the 1960s through the 1990s (DARPA, 2018). The military concentrated on FRT to identify adversaries on or near military bases (Wright, 2019), while retailers, homeowners, property owners and law enforcement focused on surveillance for a variety of reasons such as monitoring customers, home security, protecting property and identifying criminals (Bradford, 2020).

How FRT Works

Today, facial recognition is a multi-step process which captures facial images, employs algorithms and existing databases of information about people such as driver's license, criminal and financial records, family members and purchases to match the captured images to a specific face in the database (Singh, 2018). Through statistical analysis, the automated system verifies that the image or "faceprint" selected is highly likely to be the face in the database (Singh, 2018). With this level of confidence, the user determines the identification of the individual (Singh, 2018; Wright, 2019). The user also assumes that the information in the databases is accurate for the identified individual, but the information could be indelibly incorrect (Nakar & Greenbaum, 2017). The biometric technology is considered to have the ability to distinguish human differences in facial images, but this ability has not been without inaccuracies, especially related to racial and

gender differences (Introna & Wood, 2004, as cited in Kloppenburg & Van der Ploeg, 2018); Magnet 2011; Pugliese 2010).

Current FRT Applications in Public Spaces and Formats

Terrorists Watch List

September 11, 2001 (9/11) catapulted the obligation of the U.S. to immediately implement an identification system with the capability of prewarning officials that a potential terroristic threat was imminent (Bowyer, 2004; Maranzani, 2019). The terrorists watch list, mildly in existence before 9/11, escalated exponentially to include individuals, organizations and countries considered threatening to the security of the U.S. (FBI.gov, 2020; Steinbock, 2006). Individuals and entities on the list whose names were captured in a super database were automatically assumed to be perpetrators of national security and subjected to criminal charges (FBI.gov, 2020; Steinbock, 2006). Adjoining and strengthening the terrorists watch lists was the passage of The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act of 2001) that authorized the use of advanced technology for strategic surveillance (DOJ, 2020).

To assist with protecting the United States from terrorists and address opportunities of vulnerability to attack, DHS was created in 2002 and readily assumed a transnational responsibility to protect the nation with the terrorists watch list as a major defense tool (Anderson, 2019; Givens, Busch, & Bersin, 2018). The newly formed DHS challenged private enterprises engaged in biometric technology to channel their energies from the advancement of FRT to enhance the retail and other commercial businesses to

designing equipment to detect weapons and identify terrorists or suspected terrorists (Bennett, 2001; Bowyer, 2004; FBI.gov, 2020). The private enterprises were already involved in biometric applications such as iris scanning, voice recognition and digital fingerprinting (Mayhew, 2018). Transitioning to applications to advance the political and security objectives of the U.S. was uncomplicated (Gates, 2006; Mayhew, 2018). By 2004, DHS operationalized the US-VISIT system which enhanced the IDENT, the Automated Biometric Identification System and expanded its biometric identification capabilities to include facial recognition (Thales Group, 2019). Today, DHSs Office of Biometric Identification Management (OBIM) oversees all biometric identification and data storage activities of the organization and has expanded its biometric surveillance to include terrorists or suspected terrorists, certain immigrants, and criminals (Coburn, 2015; Thales Group, 2019).

U. S. Customs and Border Control

Coburn (2015) noted the responsibility of DHS to protect the Unites States borders by air, land and sea is delegated to the Customs and Border Protection (CBP) agency. Kolker (2020) outlined the legislative biometric history of the CBP that began in response to the events of 9/11 when the USA PATRIOT Act was passed in October 2001. The act required the establishment of a border enter-exit system using biometric technology (Kolker, 2020). Building upon similar legislation in 2002 and 2004, The Implementing Recommendations of the 9/11 Commission Act of 2007 required air travelers in the Visa Waiver Program to be screen biometrically upon departure (Kolker, 2020). Related legislation requiring biometric border surveillance was passed in 2008 and

2015, and in 2017 President Donald Trump signed Executive Order 13780, Protecting the Nation from Foreign Terrorist Entry into the United States ordering the implementation of a completed automated biometric entry and exit tracking system as expeditiously as possible (Kolker, 2020). U.S. citizens' participation in the tracking system was optional (Kolker, 2020). In 2020, the CBP expanded its use of FRT to identity verification of pedestrian travelers across the borders at ports of entry in southern Texas and California (CBP, 2020).

Airport Security

Airport screenings and the development of the no-fly list of known or suspected terrorists were implemented with the assistance of biometric technology (FBI.gov, 2020; Steinbock, 2006). Today, FRT is a standard identification and security check in airports, including iris scanning (Ologunde, 2015). However, FRT e-passports are problematic when individuals have had facial plastic surgery (Ologunde, 2015). While the use of FRT is an effective method of terrorists' identification at airports, it lacks the ability to avoid subjecting those who are not terrorists to FRT scanning, which may evoke a question of the constitutionality of such use (Bennett, 2001; Bowyer, 2004).

Law Enforcement Surveillance and Public Safety

Law enforcement uses FRT in efforts to ensure public safety and to fight crime (Garvie et al., 2016). FRT is employed for general surveillance to identify criminals in public spaces (Garvie et al., 2016). Targeted photo comparisons are used in investigating identity fraud, such as the discovery of individuals with multiple drivers' licenses, by applying FRT to the databases maintained by motor vehicle departments (Hamann &

Smith, 2019). FRT has been effective in active case investigations to establish probable cause regarding a crime or suspected crime (Garvie et al., 2016). Surveillance cameras mounted inside facilities such as nightclubs, businesses, private residences, on the outside of buildings, and on poles have been reviewed to identify likely perpetrators or suspects (Hamann & Smith, 2019). The introduction of FRT in criminal cases allowed by local or state law is successful for the prosecution because current jurisprudence does not include a procedure to contest the identification of the defendant in the FRT environment (Jackson, 2019).

Murphy (2018) acknowledged that body-worn cameras by law enforcement officers, intended to provide a first-hand account of officers' activities, have been applauded by community groups and the courts as conceptually appropriate to address the public's long-standing allegations of police brutality and other misconduct. The use of body-worn cameras using FRT during public protests is controversial because of the possible use of FRT to identify protesters with potential retaliation by delayed arrests, which may be an infringement upon their First Amendment right to assemble and their Fourth Amendment right to privacy (Murphy, 2018). At the same time, law enforcement departments are ubiquitously launching drones for aerial surveillance that are questionably invasive (Laperruque & Janovsky, 2018). Regardless of these concerns, the proliferation of the development and use of FRT for safety, security and crime control will not ebb (Garvie et al., 2016), especially since the results are considered more beneficial than the risks to the general public with regulatory policies (IJIS Institute, 2019; Selinger & Hartzog, 2019).

Social Media Enhancement

Social media networks lauded the diffusion of biometric technology from the spheres of security and law enforcement into an instrument for orchestrating new acceptable information norms (Norval & Prasopoulou, 2017). FRT was incorporated in the social media platform to enhance the socialization experience for its users (Sherman, 2012, as cited in Norval & Prasopoulou, 2017). Facebook introduced this justification for the implementation of its "tag suggestion" tool in which users' uploaded photographs are subjected to FRT analysis and the names of others in the photos are identified by FRT as "tag suggestions" or potential "friends" (Singer & Isaac, 2020). Facebook initially presented the "tag suggestion" tool in Europe as an identify security device but was forced to disable it. Facebook users and watchdog groups in the United States such as the Electronic Privacy Information Center (EPIC) posed potential privacy violations regarding the omission of prior notification and consent from users to scan their facial images (Norval & Prasopoulou, 2017; Singer, 2018). Some commercial enterprises disregard informed consent by using FRT to market their products to potential customers based on their targets' social media profiles (Collins, 2019).

Mobile Phones Authentication and Unlocking Key

The evolution of the mobile "smart" phone has revolutionized society in immeasurable ways in all phases of life (Soliman et al., 2013). The instrument has become more than a communication device: it is the instrument of an individual's organized or disorganized life, including social, financial, and historical data, and general awareness of world events (Soliman, et al., 2013). FRT is an application (app) that

provides some security to the mobile phone by serving as the key to unlocking the phone (Soliman, et al., 2013). FRT provides authentication that the user of the phone has the right to open it and access all its apps (Soliman, et al., 2013).

Robertson et al. (2015) conducted two experiments using face averages imitated from celebrity faces and real faces of smart phone users to determine the reliability of each FRT source. The researchers found that face averages were 100% reliable in authenticating the user and 100% accurate in rejecting the user with false identify (Robertson et al., 2015). The environment in which the tests were conducted also revealed that face averages enhanced user recognition and had an advantage over real faces (Robertson et al., 2015). The results indicated the FRT in mobile phones could be more efficiently incorporated by using face averages to develop the algorithms rather than the individual's real face (Robertson et al., 2015). FRT is also used for mobile banking, other apps and in various settings that utilize the mobile phone as its basic tool of access to services, such as monitoring patient safety for at-home patients (Jeon et al., 2019).

Health Care Management and Patient Safety

FRT is used in health care settings to assist with patient identification, diagnoses, clinical care management, and monitoring of patients (Martinez-Martin, 2019). The comparison of a patient's pre-stored biometric information in a database for FRT scanning upon entering the health care setting can expedite the registration process and curtail waiting time to see a physician (Martinez-Martin, 2019). FRT applications can predict certain genetic diseases by analyzing features in the patient's face that resemble

the facial effects of the genetic disease (Martinez-Martin, 2019). Other FRT applications can detect health ailments of the medical provider (Martinez-Martin, 2019). FRT on a mobile phone application in an emergency room environment resulted in the verification and identification of a patient in milliseconds, even when the patient was nonverbal (Nwosu, 2016). When mobile FRT is paired with Google glass eyewear, providers have instant access to the patient's cloud-stored electronic medical record, can scan vital signs, and collaborate with other physicians in a live-streaming platform (Nwosu, 2016). Another study involving 277 patients subjected to iris only recognition indicated exactness in identifying patients and medical conditions with only two exceptions (Latman & Herb, 2013).

FRT patient identification is important in reducing the risk to patient safety and to malpractice because medical care was omitted or provided to erroneously identified patients (Jeon et al., 2019). FRT can assist health care management to protect against fraud by verifying the correct patient is getting the correct tests, diagnosis, and treatment while protecting the use of facial images (Jeon et al., 2019). Although the Health Insurance Portability and Accountability Act (HIPPA) includes a provision to protect the facial image of a patient as part of the patient's medical record, there are additional issues of concern regarding the use of FRT in health care (Martinez-Martin, 2019). Issues include prior notification that FRT is used, written consent by the patient to be a subject of its use in every aspect of the health care process, biometric data protection, gender and racial bias in the diversity-deficit algorithms that may curtail appropriate diagnosis and related health care (Martinez-Martin, 2019). The apprehension of some economically

disadvantaged group members to have their faces incorporated as biometric data have also been problematic in certain FRT-use healthcare settings but was assessed to be mitigatable with appropriate information and education aimed at the apprehensive group (Nwosu, 2016).

School Security and Educational Enhancement

The major utility of FRT in schools is to enhance student security by identifying individuals who are not enrolled in the schools or whose identity and presence on the campus initiate a security alert (Andrejevic & Neil, 2019). FRT in schools can facilitate enrollment and registration (Andrejevic & Neil, 2019). The use of FRT for daily roll call have been found to save time for the instructor as well as the student (Andrejevic & Neil, 2019). FRT can be used to measure emotions and potential behaviors of students (Krithika et al., 2017). By defining facial features, face points and face feature distances, facial expressions are categorized as symbols of emotional conditions, such as nervousness, confusion, excitement, or discontent (Krithika et al., 2017). From this swift FRT analysis, an instructor can determine the attentiveness and interest of students regarding the topic, the manner in which the information is presented, or the instructional effectiveness/ineffectiveness in real time, allowing for adjustments in classroom dynamics (Krithika et al., 2017).

FRT in schools have met with controversy from education professionals, law enforcement officials, parents, students, and the community at-large (Ropek, 2019). These abilities of FRT to make the educational environments more secure and to enhance the instructional and learning experiences are diminished by the concerns for privacy,

bias, accuracy, and the potential emotional trauma to students subjected to FRT scans and surveillance on a routine basis (Engle, 2020). Deputy Director of the Education Policy Center for the New York Civil Liberties Union, Stefanie Coyle, described the potential harmfulness of FRT in schools as an instrument of bias and insecurity (Engle, 2020).

Other FRT Applications

FRT is a ubiquitous emergent in the digital and artificial intelligence technologies. FRT appears in home appliances, keys and authentication to commercial, military, and governmental secure areas, and advanced engineering such as the robotics industry (Dharaiya, 2020). With so much promise for FRT applications looming, the legal and ethical issues related to privacy, gender and racial bias, data aggregation and other concerns will accompany these progressions (Harwell, 2019). A PEW inquiry indicated that security-intended implementation of FRT can be overused and deemed intrusive (Pew Research Center, 2021). For example, a tenant management company planned to install FRT to replace key fobs for a housing area already equipped with surveillance cameras, a door attendant and security guards (Wiltz, 2019). The tenants reacted with disdain, claiming that the FRT key to their residence and the surveillance cameras were overuse, created a constant tracking system, and resulted in the tenants' unaccompanied control over their captured data (Wiltz, 2019).

Controversies Surrounding Facial Recognition Usage in Public Spaces

Technological Development Without Standardization or Regulations

Kortli et al. (2020) surveyed facial recognition systems and reported three methodologies, namely local, holistic and hybrid, which differ in their use of 2D or 3D

imaging, illumination, level of difficulty to implement and maintain, minimal operational knowledge, and the types of databases utilized by each type. Each methodology is also distinguished by the number of features utilized to identify a subject (Kortli et al., 2020). The local methodology uses a small portion of the subject's face such as the mouth, nose, and eyes (Kortli et al., 2020). The holistic methodology uses the face in totality to obtain an identification while the hybrid methodology uses both local and holistic techniques (Kortli et al., 2020). The functionality or performance rating of each methodology distinguishes the effectiveness of the FRT (Kortli et al., 2020).

Singh (2018) discussed additional facial recognition systems that produce variant results when employed. The Histogram Oriented Gradient (HOG), another form of local feature's extraction (Fathi et al., 2016, as cited in Singh, 2018) and the Fusion algorithm/RF classifiers in which thermal images are incorporated in the identification process (Seal et al., 2016, as cited in Singh, 2018) have unusual characteristics but both yield high functionality rates compared to other designs (Singh, 2018).

By applying various degrees of illumination and 3D images, Zaeri et al. (2015) experimented with thermal facial recognition utilizing moments invariants technology which statistically analyzes facial expressions radiated through thermal energy. Like other facial recognition systems, Zaeri et al. found that the functionality rating for performance varied, even by researcher involved in the same experiment.

In the wake of the 2020 global coronavirus pandemic with widespread COVID-19 infections and deaths, developers have rapidly expanded the facial recognition system to include thermal and infrared technology (Van Natta et al, 2020). Van Natta et al. reported

that contactless thermal facial recognition was developed in response to efforts to minimize the transmission of COVID-19 in hospitals, airports, other types of public transportation, schools and in public spaces such as shopping malls. The thermal FRT incorporates temperature readers and accomplishes multiple surveillance tasks, including identifying undesirable suspects and those who may have a temperature over 99 degrees Fahrenheit indicating possible COVID-19 infection (Van Natta et al., 2020). Although more sophisticated designs of this transparent technology are not widely used in the U.S. to date due to cost constraints (Van Natta et al., 2020), less expensive design by businesses in Ohio for temperature screenings for possible coronavirus are flourishing in a variety of private and public spaces (Raudins, 2020).

With each development of facial recognition technology, controversies arise regarding the differences in functionality ratings and effectiveness (Zaeri et al., 2015). From their experiment, Zaeri et al. realized the importance of standards to test the functionality and effectiveness of designs and databases to establish consistence and validity in the product. Zeng et al. (2019) explained that the controversies surrounding the technological development of FRT will continue until there is government regulation formulized with business representatives. Zeng et al. also indicated that governing the development of artificial intelligence is at the core of regulating FRT and mitigating controversies.

Biometric Algorithms Developed With Bias

The operative functionality of FRT is biometrics. Biometrics are characterized by behavioral and physiological traits of the individual which are used to digitally

authenticate the individual's identity (Omoyiola, 2018). Keystroke rhythm, voice patterns and handwriting are distinguished behavioral traits and the face, iris, retina, and fingerprints are prominent physiological traits representative of biometrics (Omoyiola, 2018). The face is the focal characteristic of FRT in which the physiological distinctions of individuals are automatically digitized by scanning features of the face such as the spatial distance between cheekbones, the horizontal dimension of the nose, and the position of the eye sockets (Omoyiola, 2018).

According to Introna and Nissenbaum, (2009), a mathematical encryption is generated by the scanned biometric features in sequence with predetermined algorithms assigned to the biometric traits and communicated to pre-existing images ("biometric templates") of individuals stored in databases called "biometric galleries" (p. 48). This "biometric probe" into the galleries results in the true, false, or voided verification of the individual owner of the scanned biometric traits (Introna & Nissenbaum, 2009, p. 48).

Norval and Prasopoulou (2017) noted three concerns with biometric algorithm technology:

1. Its convergence with the computer migrated the technology from a device for security to social media phenomenon.
2. This diffusion of biometric technology made its use more personal and ventured into the individual's personal information and user habits to create a profile, favorites, and list of contacts.
3. Biometric technology infringes upon privacy and autonomy of the individual.

Lohr (2018) reported the inaccuracy in biometric technology identification of people of color and blamed the like of diversity in the underpinning artificial intelligence development industry. Yeung et al., (2020) found that algorithm bias exists and can affect the outcome of various aspects of endeavor, such as disease and criminal surveillance. Agüera y Arcas et al., (2017) foreshadowed Yeung et al.'s algorithm bias findings in their discussion of physiognomy, the judgement of an individual's propensities based on external appearances. Aguera y Arcas et al. recognized that this pseudoscience which separates inferior and superior human beings based on facial characteristics and physiques create "scientific racism" (para. 4). When physiognomy is incorporated in artificial intelligence modeling by the developer, the result is algorithm bias which is scientifically evidenced (Aguera y Arcas et al., 2017). Norval and Prasopoulou (2017) concluded governance which guides the use of biometric technology is needed to set standards and limitations of usage, and with allowance for freedom of choice or consent of the individual.

Social Issues Stimulated by FRT

FRT in public spaces stimulate social issues which are problematic and encapsulate the harms recognized by individuals, local, state, and federal governments, civil liberties proponents, and opposing advocacy groups (Moraes et al., 2020). Social issues include privacy intrusion, gender and racial bias, data security, accuracy and privacy, and the chilling effect (Murphy, 2018; Roussi, 2020).

Privacy Intrusion. FRT influences the privacy of the individual for both proponents and opponents of FRT, and the propensity for Fourth Amendment violations

(Hamann & Smith, 2019). The importance of privacy was addressed by *United States v. Blok* (1951) as a rare trait of the American citizenry (Wynn, 2015). This uniqueness is taken seriously by Americans but has been placed in biometric hands and artificial intelligence (Gerke et al., 2020). With the application of algorithms, individuals are in a perpetual line-up and under incessant surveillance subjected to decisions made by imitational points residing in a database of millions of photos without being informed and without their consent (Harwell, 2019). In 2016, a study conducted by Garvie, et al. (2016) revealed one in four adult Americans' photos are in networks used by law enforcement, and these Americans did not have an opportunity to say "no" to having their photos placed in a line-up or being surveilled. With the exponential increase in the sizes and sources of FRT databases today (Harwell, 2019), the ratio of adults in law enforcement networks without their permission have inductively expanded (Garvie et al., 2016). FRT in commercial settings have increased especially in the retail sector where entering the establishment is assured evidential approval to be exposed to FRT (Future of Privacy Forum, 2018).

Gender and Racial Bias. Buolamwini and Gebru (2018) concurred with Yeung et al. (2020) that algorithm bias exists and cited gender and race bias as primary reprisals. AI systems from which FRT comes are filled with biased data and generate "algorithm discrimination" that can have profound consequences in law enforcement, health care and other requirements for identity verification using FRT (Alalouff, 2020). Datasets creating biometric templates are not inclusive or extensive enough to mitigate race, gender bias, and lack demographic diversity (Buolamwini & Gebru, 2018). The resulting

misidentification of women, young people, and people of color, especially African Americans, has profound consequences including false positives and unsubstantiated searches (Buolamwini & Gebru, 2018). Alalouff also blamed the bias on the AI industry's lack of diversity in the workforce with employees whose phenotypic and demographic characteristics might contribute to an equitable dataset. Reportedly, because of the Spring 2020 death of George Floyd and the Black Lives Matter protests, corporate moguls including IBM and Amazon withdrew sales of FRT based on AI believed to contain biased algorithms (Alalouff, 2020).

Gender and racial bias is an unexceptional concern regarding the limitations of FRT (Lunter, 2020). Whether the liability lies with the algorithmic configurations that analyze facial images or the human examiner who makes the final declarations of identities (Hamann & Smith, 2019), FRT can be unreliable (Lunter, 2020). A study conducted by the Massachusetts Institute of Technology (MIT) resulted in a 35% incorrect identification error rate for dark-skinned women (Crawford, 2019). In the same study, white men were incorrectly identified only 1% of the time (Crawford, 2019). The 28 U.S. Congress members of color who were inaccurately identified in the study initiated by the American Civil Liberties Union (ACLU) resulted in a 40% error rate (Crawford, 2019; Harwell, 2019). FBI co-authored research revealed that FRT is least accurate when matching the identities of individuals between the ages of 18 and 30, African Americans, and women (Garvie et al, 2016).

In research comparing facial recognition techniques by employing 2D and 3D imaging and algorithmic configurations with enhanced accommodations for

characteristics such as aging, poses, thermal imaging, facial occlusions, iris mapping and facial expressions, the accuracy of FRT is high (Singh, 2018). Mileva and Burton (2019) concurred "wide-person variability" in the use of CCTV video based FRT increases the accuracy rate of correct FRT identification as demonstrated in research using random images in a large transportation hub. The results of the two research studies did not address the gender-racial bias observed in other studies (Harwell, 2019), nor applications in the manufacturing of FRT in apparatus, specifically body worn cameras (Crawford, 2019). Augmented to the potential for gender and racial bias is the possibility of character categorization by an algorithm and a database of information may or may not be relevant to the individual, which is harmful (Nakar & Greenbaum, 2017).

Data Security, Accuracy, and Privacy Concerns. The collection, storage, and use of personal data raise concerns about data security, accuracy and privacy make the methodologies employed to accomplish these tasks questionable (Moraes et al., 2020). The United States Government Accountability Office (GAO, 2020) lists the following concerns for datasets that relate to data security and privacy: data breaches or hacks in which personal information and passwords may be stolen; the lack of control over one's personal data when collected by companies during business transactions; data solicited from paid subjects, or obtained by third-party data collectors such as web data miners or scrapers who download volumes of information from Internet searches; job sites (such as LinkedIn, Indeed, Monster); news items; and social media (such as Facebook).

The GAO (2020) also reported public datasets assembled from a variety of sources including government and academia may have a legitimate reason for its

existence but face the same concerns as commercialized datasets: how the data are used, shared, or sold without the individual's knowledge and consent; and if the data are copied or stolen, the individual's information is vulnerable to a multiplicity of uses and misuses (including inaccuracies) unknown to the subject (GAO, 2020). McClellan (2020) described these concerns as a paradox for data. One of the purposes for the use of the technology is to safeguard access to data (McClellan, 2020). Yet, its use becomes unsafe due to the lack of regulations to control the way biometric information is collected (McClellan, 2020).

The Chilling Effect. "Chilling" is the descriptive adjective for individuals' physical and emotional responses to the presence of FRT (Nakar & Greenbaum, 2017). The responses emerge when individuals have the expectation of freedom and anonymity in public spaces, only to discover their faces are nomadically filtering through a database of faceprints to determine if a likeness of them exists with unknown information about them assumed to be factual (Nakar & Greenbaum, 2017). As FRT continues to rapidly evolve, concerns that its presence might "chill" the natural actions and speech of individuals surface, such as during public protests (Murphy, 2018). If this occurs, freedom of speech guaranteed by the First Amendment during public protest is compromised (Murphy, 2018) because the individuals' free expressions while exercising their right to protest are inhibited, altered, or curtailed by FRT scrutiny (Roussi, 2020). The chilling effect initiated by the presence of FRT in the public protest environment is harmful and may have implications for Fourth Amendment violations regarding unwarranted searches (of identities) and violation of individuals' expectations of privacy

(Wynn, 2015). In non-protest situations, the presence of FRT can initiate social separation from the surroundings and individuals, and stifle natural behaviors (Martinez-Martin, 2019).

Facial Recognition Use Addressed by the Courts

Federal and State Level Judicial Actions

National laws and U. S. Supreme Court cases expressly and comprehensively addressing the use of FRT and the controversies surrounding the technology have not been established (Nakar & Greenbaum, 2017). Instead, court cases which have been cited to mitigate legal and ethical issues concerning digitized technology and information including FRT (Celentino, 2016; Bradford et al., 2020) have been applied.

With the Fourth Amendment as the underpinning basis for establishing a position of agreement or opposition for the use of FRT, the issue of the expectation of privacy, specifically in public spaces, has presented a political, legal, and ethical conundrum (Ruhrmann, 2019). Anchored to the expectation of privacy concept of the Fourth Amendment is Warren and Brandeis' paper entitled *The Right to Privacy* which manifests as a guidepost to legal and civil proponents and opponents of FRT use in public spaces applicable to digital information today (Cochran, 2019).

A substantial concern regarding the use of digitized information, including FRT, is its use for governmental or law enforcement surveillance (Brown, 2014). Leavens (2015) questioned the use of technological advancement in surveillance that may be invasive and outside the textual construct of the Fourth Amendment's reasonable expectation of privacy and questioned the relevance of the Fourth Amendment's privacy-

based test (*Katz v. United States* (1967), as cited in Leavens, 2015) deemed to be outdated for modern society. The question of relevancy has not curtailed the application of *Katz* as the framework for legally examining the reasonableness of the individual's expectation of privacy issues (Leavens, 2015). The two-part test to determine a violation of the Fourth Amendment include answering the following questions:

1. Does the individual genuinely have an expectation of privacy?
2. Would society consider the individual's expectation of privacy reasonable? (Bennett, 2001; Hamann & Smith, 2019).

In concurrence with Leavens (2015), Litt (2016) considered the information age which uses GPS tracking and metadata collection as a violation of an individual's expectation of privacy. Spencer (2015) cited these technological data aggregation efforts to obtain information as invasive. Courts which agreed included: the Supreme Court of the United States (SCOTUS) in *United States v. Jones* (2012) ruled the use of data aggregation long-term on warrantless GPS tracking affected the reasonable expectation of privacy and violated the Fourth Amendment; SCOTUS in *Riley v. California* (2014) examined data aggregation to determine warrantless searches of smart phones and cell phones belonging to arrested individuals violated the Fourth Amendment; and the Supreme Judicial Court of Massachusetts in *Commonwealth v. Augustine* (2013) reviewed data aggregation to rule the warrantless cell site location information (CSLI) was a violation of the Fourth Amendment (Spencer, 2015). By intercepting the wireless transmissions of an individual's private conversations, law enforcement was able to locate the individual by using CSLI tracking, constituting continuous surveillance when

the individual expects the conversations to be private (Horton, 2018). In *Carpenter v. United States* (138 S. Ct. 2206 (2018), SCOTUS ruled obtaining CSLI data without a search warrant was a violation of the Fourth Amendment (Hamann & Smith, 2019). *United States v. Jones* and *Carpenter v. United States* are considered the cases which envisaged credibility and validation to opponents of FRT use in public spaces (Senate RPC, 2019).

To examine cases more relevant to FRT, *Katz* has been cited to resolve questions concerning the use of video surveillance in public spaces, such as streets, public schools, and workplaces (Vitiello, 2018). In 1968, SCOTUS established the plain view document in *Harris v. United States* (Justia, 2020). The doctrine states there is no violation of the Fourth Amendment requiring a warrant to seize items relevant to a crime if the items are in plain view and are inadvertently discovered (Hess, 2019). Proponents of the use of FRT in public spaces have relished the plain view doctrine as a sanction for the use of video surveillance (Hess, 2019). Proponents also looked at the failure of the Omnibus Crime Control and Safe Streets Act of 1968, Title III to address video surveillance while focusing on wire, oral and electronic communications as signage the FRT is not regulated (DOJ, 2015). Two court cases unfavorable toward the protection of privacy are important to the discussion about the use of FRT in public spaces and the relevance to privacy protections: the decisions in *Kyllo v. United States* (2001) in which the use of thermal imaging into private spaces was not considered an unwarranted search; and the decisions in *Illinois v. Lidster* (2004) rendered unwarranted surveillance to apprehend suspects more important than maintaining the privacy of the individual (Wynn, 2015).

Putting the legacy of the Fourth Amendment to a more recent test was Patel *v Facebook* (2020) (Justia, 2019). Wessler (2019) described the severity of the discontent with Facebook's implementation of its FRT tag suggestion tool led a cadre of residents of the State of Illinois to file a class-action suit against the social media giant for violating the state's Biometric Information Privacy Act. Gorbonosov (2019) recounted the plaintiffs' allegation that FRT was used on their photos without their consent. In the decision in favor of the plaintiffs, the U S. Court of Appeals for the Ninth District set precedent by stating FRT is harmful to the protection of privacy (Wessler, 2019). The Court upheld the plaintiffs' claim in *Patel v Facebook* that the implementation of the biometric models of their faces without consent was an invasion of privacy (Wessler, 2019). In January 2020 after SCOTUS refused to hear the case on appeal (Birnbaum, 2020), Facebook settled the suit for $550 million to be paid to eligible users along with their court costs (Anghel, 2020; Wessler, 2019).

Civil Liberties and Advocacy Groups Judicial Actions and Petitions

Civil liberties and privacy advocacy groups are also involved in the stagnated approach to defining FRT use in the U.S. and establishing federal regulation (EPIC, 2020). Exemplifying this trend is the ACLU which filed suit in a Massachusetts court against the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI), and the DOJ for access to information about how facial recognition software is used (EPIC, 2020). Harwell (2019) noted the FBI has access to a database of police mugshots containing more than thirty million facial pictures and an additional database from drivers' licenses and other records nationwide totaling more than 640 million facial

pictures. The ACLU contended the potentiality of facial recognition software to create a persistent tracking of individuals could be an affront to constitutional principles (Harwell, 2019). The organization cited the invasiveness and inaccuracy of the software as objectionable characteristics (ACLU, 2019). The organization's allegations were proven when the pictures of 28 of the members of Congress were scanned using a facial recognition software and were mismatched with criminals in the police mugshots, especially people of color (Harwell, 2019).

EPIC (2020) described active engagement in promoting its perspective on the use of facial recognition software in various settings. Along with a coalition of civil liberties and privacy advocacy groups, EPIC noted their petition for the following actions regarding FRT: the exclusion of FRT at the SeaTac International Airport in Seattle; Privacy and Civil Liberties Oversight Board's deferment of FRT used in all federal agencies; a global ban on the use of FRT; and information through the Freedom of Information Act for the Immigration and Customs Enforcement's (ICE) planned expansion of the FRT database.

Facial Recognition Use Addressed by States and Municipalities

State Level Legislative Actions

In the interim, several states have enacted legislation to respond to concerns from the public, businesses and industries, and law enforcement agencies (Ruhrmann, 2019). Laws that limited the use of biometrics have been enacted in several states including Texas, Washington, California, and Illinois which enacted the Illinois Biometric Information Privacy Act **(**Nakar & Greenbaum, 2017). The legislation included three

common provisions: the right to be notified FRT was in use and the freedom to opt out of FRT exposure; restrictions on the use of FRT data by commercial entities; scheduled destruction of the FRT database; and protection of privacy data according to relevant standards of operation **(**Nakar & Greenbaum, 2017). The State Legislature of Massachusetts considered a bill to place a moratorium on the use of FRT (Conger et al., 2019). Introduced in the state Senate in January 2019, no action had been taken on the bill since February 2020 (Commonwealth of Massachusetts, 2020). California, New Hampshire, and Oregon have passed state laws banning the use of facial recognition software in body cameras worn by police officers (Samsel, 2019).

City and County Level Actions

City and county municipalities have also independently assessed and responded to the implementation and use of FRT in public spaces (Conger et al., 2019). In 2019, San Francisco became the first city in the U.S. to ban the police and other agencies from using FRT, although the police department did not employ FRT at that time (Conger et al., 2019). The city's Board of Supervisors determined such use of FRT would be excessive if put into use and was making a pre-emptive strike against FRT usage for that purpose (Conger et al., 2019). Five other municipalities in California and Massachusetts combined approved similar bans on the use of FRT by the police force (Conger et al., 2019).

Current Federal Facial Recognition Technology Guidelines

Executive Orders

While the conglomerate of proponents and opponents of FRT use wait for the formulation and enactment of legislation to regulate FRT, federal governmental agencies have been ordered to take a "light touch" approach to regulatory and non-regulatory developments, outside the federal government, that use AI including FRT (Vincent, 2020). The purpose of the Executive Order issued in 2019 was to urge agencies and companies to develop AI "to sustain and enhance the scientific, technological, and economic leadership position of the United States in AI" (Trump, 2019). A *Guidance for Regulation of Artificial Intelligence Applications* draft memo issued to department and agency executives outlined the stewardship should be followed in the development of AI, which included ensuring public trust and maintaining scientific integrity (Vought, 2019). Omitted from the Executive Orders and *Guidance* were specifications and funding for the promotion of AI and instructions to mitigate the controversies surrounding AI/FRT in the development (Corrigan, 2019).

Departmental Authorizations

The use of FRT has been authorized for other federal departments including the Department of State, the Department of Defense, and the DOJ (Steinbock, 2006). Del Greco (2019) described the use of FRT by the FBI as an effective tool for law enforcement and public safety. The FBI operates the FACE Services Unit to recognize facial images utilizing the FBI's database and other federal databases including the Automated Biometric Identification System of the Department of Defense, Passport

Photo File and Visa Photo File of the Department of State, and criminal mugshots, correction, and motor vehicles photos from state departments (Del Greco (2019). In 2019, the FBI's accessed databases contained 641 million facial images (Johnson, 2019). While operating FRT services, the FBI maintains an awareness of the need to protect civil liberties and privacy of the individual (Del Greco, 2019).

The Need for a National FRT Policy

The resound for a national policy to regulate all aspects of FRT, including mitigating the controversies surrounding its use, are apparent from a broad spectrum of interests (Yeung et al, 2020). From academia, Learned-Miller (2020) and a group of experts in AI authored a white paper entitled, "Facial Recognition Technologies in the Wild: A Call for a Federal Office." The paper offered an ideal policy to address FRT use would also address the controversies that surround FRT (Learned-Miller, (2020). The experts argued current policies by state and local entities do not go far enough, federal regulation should be passed and a federal office responsible for regulating FRT should be established (Learned-Miller, 2020). From independent researchers, Crawford (2019) argued the use of FRT should cease until there is regulation to ensure safeguards to protect the civil and legal rights of individuals, transparency, accountability, and fairness.

From the federal level, the National Institute of Justice (NIJ) (2020) reported FRT expert Anil Jain discussed the need for standards to make decisions about the management of governmental biometric data. In addition, Johnson (2019) reported even the Chairman of the House Oversight and Reform Committee Rep. Elijah Cummings,

while holding hearings on the use of FRT, indicated individuals in the U.S. are exposed to a technology that is not ready for widespread use.

The Need for Relevant Research on Issues Preventing the Passage of a National FRT Policy

According to Hamann and Smith (2019), before the nation can formulate and enact an effective policy to regulate FRT use, it is important to eliminate the ambiguity which exists among proponents and opponents of FRT in consideration of current jurisprudence. The benefits of FRT must be reconciled with the controversies surrounding FRT use considered to be harmful to individuals (IJIS Institute, 2019; Selinger & Hartzog, 2019). Recognizing that the biometric foundation of FRT is flawed will assist policymakers and stakeholders in conducting an expansive analysis of FRT (Kloppenburg & Van der Ploeg, 2018). A genuine exploration of the harms identified by individuals subjected to FRT, including technological development without standardization or regulations, biometric algorithms developed with bias, and specifically, the social issues of privacy intrusion, gender and racial bias, data security, accuracy and privacy concerns, and the chilling effect, requires qualitative validation preceding policy proposals (Das et al., 2017). Relevant research on FRT harms to individuals can provide substance to content that ensures FRT harms are mitigated in federal policy (Martinez-Martin, 2019).

Wynn (2015) concluded a FRT law cannot pass that mitigate the privacy issues (and the other controversial problems) until the identification of jurisprudence regarding obsolete privacy protection laws is reviewed by lawmakers and updated. Martinez-Martin

(2019) concurred with Wynn and further identified the problem with passing a national FRT policy: the controversial problems need the attention of lawmakers at the federal level that is purposeful and consistently moving toward compatible outcomes. Carter (2018) described this purposeful mobility as finding a balance between FRT and privacy intrusion. Wright (2019) noted not enough is known about the attention these issues are getting from lawmakers at the federal level to determine the pathway challenges to FRT regulations (Politico, 2020).

Summary and Conclusion

FRT has been in existence for more than 50 years and has developed into one of the most important and controversial tools available in the global community (Givens et al., 2018). During its time of existence, two events occurred that projected facial recognition to a convenient and essential instrument. The first event was the digitalization of information that became one of the most important technological developments of modern society (Donahue, 2017). The second event was the terrorists attack on the U.S. on 9/11 (DOJ, 2020). This latter event catapulted biometric data identification which included facial recognition to the forefront of safety solutions (McClellan, 2020) but made privacy intrusion prominent on the list of social issues and other controversial concerns (Price, 2016).

Researchers have developed and analyzed algorithmic calculations to formulate biometric databases for facial recognition applications (Bah & Ming, 2020; Li, 2019). Singh and Prasad (2018) compared various technological platforms upon which facial recognition biometrics could be configured to achieve accuracy and efficiency. Bowyer

(2004) and Martinez-Martin (2019) discussed the desire for the standardization of FRT development designed to eradicate facial recognition technological problems and achieve the facial recognition use purpose. Concurrently, other researchers concluded the problems with FRT are encapsulated in political and ethical definitions and differences (Yeung et al., 2020). Wynn (2015) cited concerns for First Amendment and Fourth Amendment violations with the use of FRT and suggested future research in this area was necessary. Industry leaders in FRT development and marketing such as Microsoft (Statt, 2020), agreed with Segovia (2015) that a privacy protection law updated to accommodate the changes in modern technology must be the precursor to the passage of federal legislation regulating the development and use of FRT in public spaces. These studies stand independently stoic and leave the safety-privacy dichotomy of FRT unresolved through federal legislation (Horton, 2018).

What was missing in the literature was research on how to achieve a balance between standards of development and use, and the privacy protection concerns raised by researchers (Bowyer, 2004). Bennett (2001) discussed the need for federal legislation to provide safety and simultaneously avoid an unreasonable intrusion upon privacy. Zeng et al. (2019) identified the need for research and action to include models constantly improve FRT and safeguard the concerns of individuals. Identifying these points of equilibrium for both safety and privacy, and related issues was important to the formulation and passage of FRT legislation (Chin, 2019).

There was no trajectory toward FRT regulations described in the literature, either because the course of action was unidentified or lacked consensus in approach (Wright,

2019). Kloppenburg and Van der Ploeg (2020) described the need to uncover all the facts and envision all the scenarios regarding FRT identity verification and surveillance to determine how political and ethical questions were defined or redefined to correlate with innovative technologies. Wright described a collaborative, negotiated effort among stakeholders to satisfy safety and privacy issues, but did not provide supportive guidelines on how to conduct or achieve this collaboration nor how to turn it into legislative action when obtained.

The need to enact FRT legislation before further proliferation of FRT in public spaces occurred that caused citizens to choose between safety and the loss of freedom (Wynn, 2015) was necessary, but a plan to achieve this task was not offered in the literature (Horton, 2018). The gap in the literature was the unknown factors explaining why Congress has not passed national FRT legislation (Murphy, 2018; Roussi, 2020). A case study of the concerns and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform revealed the identification of factors explaining why Congress has not passed legislation regulating the development and use of FRT and revealed the balance between standards of development and utilization, privacy protection, and the other controversial problems needing attention to enact federal legislation regulating FRT (Wright, 2019).

In Chapter 3, I provided details of the research method. I explained the research design and rationale and the role of the researcher. The methodology including the data collection instruments and issues of trustworthiness was also discussed in this chapter.

Chapter 3: Research Method

The purpose of the study is to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces in the U.S. (Buolamwini and Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wright, 2019; Wynn, 2015). To address the gap in the literature by identifying obstacles to passing a national FRT policy, a case study of the concerns and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform regarding FRT use, and harms was conducted (Congress.Gov, 2020). The case study research design supported an in-depth exploration of the factors investigated that prevented the enactment of regulation during the policy formulation process (Harrison et al., 2017).

The research method section was an essential part of the study (Rudestam & Newton, 2015). In this section, the research design and rationale; role of the researcher; methodology; and any issues of trustworthiness are presented. The section on research design and rationale restate the research question, as well as define the phenomenon of the study (Alpi & Evans, 2019). My role as the researcher is outlined (Rudestam & Newton, 2015). Any probable biases and other ethical issues are explained, managed, and addressed in this section (Rudestam & Newton, 2015).

The methodology section explains the procedural content of the study (O'Sullivan et al., 2017). In the participation selection logic part of this section, the population and sampling strategy are identified (O'Sullivan et al., 2017). Each data collection instrument

and source are acknowledged (O'Sullivan et al., 2017). Published data collection instruments and researcher developed instruments are described (O'Sullivan et al., 2017). The procedures for recruitment, participation, and data collection are explained in detail (O'Sullivan et al., 2017). Finally, I summarized the data analysis plan (O'Sullivan et al., 2017; Rudestam & Newton, 2015).

Issues of trustworthiness are vital to any study (Walden University, 2016). Credibility, transferability, dependability, and confirmability justified the internal and external validity of this research (Walden University, 2016). The analysis determined the reliability and objectivity of the study (Walden University, 2016). The examination of ethical procedures concludes this section of the study (Rudestam & Newton, 2015).

Research Design and Rationale

To explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces, the study focused on the following research question:

RQ: Why has Congress failed to pass a national FRT policy and how is the public affected?

The qualitative research method was appropriate for this study because it aligned with the problem by providing the methodology to address the research question through a case study research design (O'Sullivan et al., 2017). O'Sullivan et al. explained a case study research design can answer the questions of "how" and "why" regarding the obstacles to passing legislation addressing FRT use in public places. I conducted a case study of the concerns and decisions of the U.S. House of Representatives Congressional

committee members and testimonials from other contributors to the Committee on Oversight and Reform to uncover these obstacles (Yin, n.d., as cited in O'Sullivan et al., 2017). I accomplished this study by coding, categorizing, and systematically identifying themes and trends using the committee hearings' transcripts (Bengtsson, 2016; Salanda, 2016).

Role of the Researcher

As researcher, I played a critical role in the research project (Sutton & Austin, 2015). As observer, I collected, analyzed, and coded the data, and presented my findings of the examination of the transcripts of the Congressional Committee (O'Sullivan et al., 2017). I collected the emergent categories from the assessment of codes and examined and grouped them together to display comparable ideas or themes (Saldana, 2016). This approach illustrated coded meanings and relationships of the narratives expressed in the transcripts (Saldana, 2016). Completing the required aspects of the research method process validated the application of the case study design for the research (O'Sullivan et al., 2017; Saldana, 2016).

I do not have any personal or professional relationships with any members of the Congressional committee. I did not have any preconceived knowledge of the thoughts and feelings of the subjects (Sutton & Austin, 2015). As the observer and researcher, I formulated codes and developed categories and themes to illustrate the narratives' relevancy to the problem, purpose, and research question in this study (Saldana, 2016). I looked for the similarities, differences, and trends in the testimonies of experts and

advocacy witnesses and the questions and concerns of the Congressional committee members (Saldana, 2016).

The lack of affiliation with members of the committee facilitated objective monitoring of the research process and diminished any bias or other ethical issues (Gerke et al., 2020; Qualitative Practice, n.d.). To manage any potential bias, my first task was to become aware of the major elements discussed in the hearings regarding implementing the FRT method of establishing a person's identity and determining how political and ethical (social) questions are defined or redefined to correlate with innovative technologies (Congress.Gov, 2020; Shannon et al., 2017). My second task was to translate the major elements and political, ethical, and social issues, which identified factors explaining why Congress has not passed legislation addressing FRT use in public spaces (Hamann & Smith, 2017). My third task was to offer to the literature a trajectory toward finding a balance between FRT and privacy protection that would affect the passage of federal legislation to regulate FRT (Wright, 2019). Accomplishing the three tasks contributed to the management of any impending biases and other ethical issues, as well as extended my study as collaborative research in the future investigations of the hearings on FRT (Gerke et al., 2020; Martinez-Martin, 2019; Schoonenboom & Johnson, 2017).

Methodology

I selected the qualitative research method for this study. Schoonenboom and Johnson (2017) described the qualitative research method as appropriate for the collection and analysis of data, the presentation of viewpoints, and results inferences

regarding the study topic. The qualitative method allows the description of experiences, attitudes, or behaviors of people related to some phenomenon in the universe (Schoonenboom & Johnson, 2017). The method allows subjectivity to be an integral component of developing conclusions through inductive reasoning (Laureate Education [Producer], 2014-a) necessary in describing the phenomenon in this study: the factors explaining why federal legislation has not passed addressing FRT, privacy protection, and related problems in public spaces (Buolamwini and Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015).

Participant Selection/Sampling Strategy

The purposive sampling technique was employed in this qualitative study. Specifically, I used the homogenous method of purposive sampling to identify and select subjects with similarities in responsibilities or effect (Etikan et al., 2016). The sampling pool of subjects in the study was the Congressional members of the House engaged in FRT legislation activities (Congress.Gov, 2020). Legislation or bills reviewed to identify Congressional activities were based on the following criteria: they must contain the words “facial recognition technology;” they must address the controversial problems related to FRT use in public spaces; and passage or ongoing activity regarding the legislation must exists (Congress.Gov, 2020).

A four-phase process was established for this nonrandom sampling. Phase 1 included the identification of Congressional records that contained legislation introduced in the United States Senate and the House of Representatives from 1997 to 2020 that

contained the words “facial recognition technology” (Congress.Gov, 2020). At least 100 pieces of legislation or bills containing this phrase were identified (Congress.Gov, 2020). Phase 2 of the sampling process involved a review of the status of the bills: introduced, read, passed, enacted, failed, assigned to committee, or no further action (Congress.Gov, 2020). Failed bills and those that had been read but had not been assigned to committees were eliminated from the sampling pool (Congress.Gov, 2020). Among the records researched, at least 12 of the bills became law (Congress.Gov, 2020).

In Phase 3 of the homogenous purposive sampling process, each surviving bill was scrutinized to determine their specific inclusion of the phrase “facial recognition technology” and to ascertain if the controversial problems surrounding its use in public spaces were addressed (Congress.Gov, 2020). Issues are, namely, the prominent privacy protection problem; technological development without standardization or regulations; biometric algorithms developed with bias; gender and racial bias; data security, accuracy, and privacy concerns; and the chilling effect (Buolamwini and Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wynn, 2015). The number of laws passed addressing these controversial problems were identified (Congress.Gov, 2020).

Phase 4 included a review of the interest outcome and committee activity relevant to the research question (Congress.Gov, 2020). When reaching saturation of the sampling pool in which no additional bills were available at the time of review (Etika, et al., 2016), one Congressional committee met the criteria relevant to the study and was selected as

the study subjects (Congress.Gov, 2020). The role of the subjects is detailed in the Instrumentation and Data Collection sections.

Instrumentation

The data collection instrument for the research study was the Congressional Records of the U.S. Congress, which are the official records of congressional proceedings and are published every day the Congress is in session (Govinfo, 2020). The reputation of the source of the data is indisputable, serving both as historical and legal documents of the U.S. Congress since publication began in 1873 (Govinfo, 2020). Obtaining the data from the Congressional Records about Congressional activities was the best source of information for the purpose of this study (Govinfo, 2020).

More specific to this study, the data collection instrument was the transcripts from the U.S. House of Representatives' Committee on Oversight and Reform hearings on *The Use of Facial Recognition Technology (FRT) in Public Spaces and the Identification of Obstacles to the Passage of Federal Policy Regulating the Development and Utilization of Facial Recognition Technology* (Congress.Gov, 2020). The source for the data collection instrument was the U.S. congressional records located at Congress.Gov, 2020, specifically the archival records of the subjects' committee hearings.

The data collection instrument was sufficient to answer the research question. The Committee on Oversight and Reform conducted three hearings on the use of FRT, which were cited in the Congressional records (Congress.Gov, 2020). These hearings occurred:

1. May 22, 2019. The specific topic of discussion was "Facial Recognition Technology (Part I): Its Impact on Our Civil Rights and Liberties."

2. June 4, 2019. The specific topic of discussion was “Facial Recognition Technology (Part II): Ensuring Transparency in Government Use.”
3. January 15, 2020. The specific topic of discussion was “Facial Recognition Technology (Part III): Ensuring Commercial Transparency and Accuracy.”

The committee hearings’ resulting transcripts were approximately 14 hours of discourse combined (Congress.Gov, 2020). I analyzed the three transcripts to answer the research question using the procedures discussed in the data analysis section (Bengtsson, 2016). The members of the Committee on Oversight and Reform assigned to participate in each hearing and the witnesses are listed in Appendices A, B, and C.

Data Analysis Plan

I conducted a case study of the concerns, emotions, and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform to analyze the data (see Yin, n.d., as cited in O’Sullivan et al., 2017). This research design was suitable for clarity of textual data, which were saturated with knowledge about the research question (O’Sullivan et al., 2017). The case study research design also facilitated an inductive approach toward what was preventing federal legislation enactment regarding FRT (Laureate Education [Producer], 2014-a).

I employed the case study research design to code, develop categories, and generate themes from textual data and infer conclusions about their meaning (Saldana, 2016). The instrumentation of analysis was Saldana’s (2016) *The Coding Manual for Qualitative Researchers*. I devised a predetermined strategy for coding by identifying

excerpts from hearing transcripts deemed informational and phrases toward the trajectory of answering the research question (Saldana, 2016). The procedural context of the manual guided me in symbolically ascribing summative words and phrases or codes to the narratives presented in the transcripts (Saldana, 2016).

I began the data analysis by establishing the pathway to answering the research question (O'Sullivan et al., 2017). The pathway was initiated by the divergence of the narratives into two dimensions of purpose: narratives playing a role in identifying factors explaining why Congress has not passed legislation preventing or obstructing the passage of federal FRT legislation, and narratives recognizing controversial problems related to FRT usage in public spaces (Buolamwini and Gebru, 2018; GAO, 2020; Nakar & Greenbaum, 2017; Omoyiola, 2018; Saldana, 2016; Singh, 2018; Wynn, 2015). I developed tables to record excerpts from the narratives representing each dimension of purpose. As transcripts were reviewed, I placed the excerpts representing relevancy to the research question in the tables. Descriptive codes, representing a summation of the excerpts and first cycle coding, were assigned to each excerpt. For clarity, I assigned second cycle coding to some excerpts (O'Sullivan et al., 2017; Saldana, 2016). The location of these excerpts in the hearing transcripts was recorded with each passage. The tables displaying the dimensions of purpose, the excerpts, and coding are placed in Appendices A, B, and C.

I examined the narratives and descriptive coding to identify any patterns of similarities in the narratives or repetitiveness of actions presented in the transcripts (Saldana, 2016). The presence of these characteristics two or more times established

patterns of thoughts, concerns, emotions, and actions (Saldana, 2016). Saldana noted researchers who employ the qualitative method welcomed the emergence of patterns because human nature expects orderly, predictable events which facilitate understanding the research analysis and outcome. I found Saldana's assessment of this process to be accurate and helpful. I combined the coded patterns to form categories of information or events merging to articulate the meaning of the collected data (Saldana, 2016). Each category was examined to extrapolate themes or concepts garnered from individual or a group of categories (Saldana, 2016). These themes represented the factors explaining why Congress has failed to pass a national FRT policy and how the public is affected. The inductive migration from categories to thematic factors is displayed in Table 2. The issues of trustworthiness of the data collection and analysis plan are addressed in the next section of this chapter (Walden University, 2016).

Issues of Trustworthiness

Strategies to address issues of trustworthiness were established to ensure confident in this study. The strategy to establish credibility and internal validity was twofold: the prolonged engagement with the stakeholders/subjects through their recorded hearings; and persistent observation of the data collection process through continuous review of data to identify and the related and unrelated factors toward answering the research question (Walden University, 2016).

The strategy to establish transferability and external validity included a thick description of the subjects, data location and collection process, and a detailed description of the data analysis plan for ready recreation of the findings (Walden University, 2016).

The strategy to recognize dependability and reliability of the study was to establish an audit trail by using raw data and coding procedures to reduce, analyze and inductively answer the research question (Walden University, 2016). The strategy to establish confirmability and objectivity in the study included my engagement in conducting the study and in reflexivity by recording notes during and immediately after reviewing subjects transcribed and video comments (Walden University, 2016).

Ethical procedures were applied to ensure no ethical violations occurred. In this study, no human subjects were directly contacted or involved in any aspects of the study. There were no ethical issues related to data collection, data management or confidentiality because all the data included in the study were available for public use at Congress.Gov (2020).

Summary

Chapter 3 contained the components of the underpinning answers to the research question and the processes necessary to answer the question (Alpi & Evans, 2019; Harrison et al., 2017; O'Sullivan et al., 2017). I presented the research design and rationale, and the role of the researcher. I also presented the methodology and the elements of inclusion which were the participant selection/sampling strategy, the data collection methodology, the data analysis plan, and the instrumentation utilized to analyze the data (O'Sullivan et al., 2017). Issues of trustworthiness of the study were also presented (Walden University, 2016). In Chapter 4, a detail of data management, the findings in the data analysis and a summation of answers to the research question are presented.

Chapter 4: Results

The purpose of the study was to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces in the U.S. (Buolamwini and Gebru, 2018; GAO, 2020; Hamann & Smith, 2019; Nakar & Greenbaum, 2017; Omoyiola, 2018; Singh, 2018; Wright, 2019; Wynn, 2015). To explore the factors, the study focused on the following research question: *Why has Congress failed to pass a national FRT policy and how is the public affected?* In Chapter 4, I explain the data collection and data analysis implementations and present the findings in the data analysis and a summation of answers to the research question.

Setting

Since the inception of this study, the chairperson of the U.S. House of Representatives' Committee on Oversight and Reform changed, some of the members of the Committee were replaced, and the House bill which initiated the Committee introduced in the 116th Congress was reintroduced in the 117th Congress by a different Congressperson, but the fervor with the Committee members approached the hearings remained steady throughout the three hearings. These changes did not influence the interpretation of the study results (Congress.Gov, 2021).

Demographics

The number of purposively, non-random subjects selected for this study included 42 members of the U.S. House of Representatives' Committee on Oversight and Reform which met to conduct hearings on *The Use of Facial Recognition Technology (FRT) in Public Spaces and the Identification of Obstacles to the Passage of Federal Policy*

Regulating the Development and Utilization of Facial Recognition Technology (Congress.Gov, 2020). Their appointment to this Committee was relevant to the study because they represented a bipartisan body with the interests and task to propose and pass FRT legislation. Congressional subjects in the three hearings were 31 Committee members in Part I, 34 Committee members in Part II, and 32 Committee members in Part III, respectively. Contributing to the hearings were 13 expert witnesses who answered questions posed by the Congressional Committee members and provided evidential documents and papers pertinent to their responses (Congress.Gov, 2020).

Data Collection

I obtained electronic records of the transcripts from the three hearings conducted by the Congressional committee and electronic copies of the materials provided by the expert witnesses (Congress.Gov, 2020). I viewed video recordings of the hearings, which diminished the absence of face-to-face access to the subjects, promoted a comprehensive understanding of the hearings, and enhanced the data collection process. These electronic records supported the data to be collected. I scrutinized each page and video of the data for 60 days to identify narratives signalizing the pathway to answering the bipartite dimensions of the research question: *Why has Congress failed to pass a national FRT policy and how is the public affected?*

Narratives I deemed to be relevant to factors explaining *Why has Congress failed to pass a national FRT policy?* were recorded on the data collection instruments shown in Figure 1 for each of the three hearing transcripts.

Figure 1

Hearing Transcript Data Collection Instrument: Why has Congress Failed to Pass a National FRT Policy?

PATHWAY TO ANSWERING THE RESEARCH QUESTION: DIMENSIONS OF PURPOSE RECORD		
FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES Hearing Transcript		
Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces		
Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**

Narratives I reasoned to be relevant to the question *How is the public affected?* were recorded on the data collection instrument depicted in Figure 2 for each of the three hearing transcripts.

Figure 2

Hearing Transcript Data Collection Instrument: How the Public is Affected

PATHWAY TO ANSWERING THE RESEARCH QUESTION DIMENSIONS OF PURPOSE RECORD		
FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES Hearing Transcript		
How the Public is Affected		
Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**

The data collection instruments, named the "Pathway to Answering the Research Question: Dimensions of Purpose Record," were designed for each part of the research question and for each of the three hearings for a total of six designs. I recorded selected excerpts from the hearings and their page numbers on the relevant data collection

instrument and employed the descriptive coding method to develop a first cycle coding for each selected excerpt. The first cycle coding consisted of one or more words that denoted the premise of the excerpt. The excerpts and the descriptive coding were reviewed to ascertain the appropriateness of each entry to the dimension of the research question. The data collection process followed the plan presented in Chapter 3.

The unusual circumstance encountered in data collection was the emergence of extensive narratives in the transcripts that recognized the following pertinent questions raised by the Congressional Committee members and addressed by the expert witnesses:

1. Why FRT legislation is needed?
2. What is wrong with FRT currently – technically, politically, and administratively?
3. What is needed in FRT legislation?
4. What recommendations and preferences should be adopted for the content of FRT legislation?

These questions were considered in the data analysis of this chapter.

Data Analysis

The data analysis process began with first cycle coding. The excerpts from the narratives contained in the three hearing transcripts were assigned one or multiple words or phrases to summarize the selected excerpts.

Inductive Migration from Codes to Categories and Themes

To migrate inductively from the codified data to larger representations including categories and themes, the excerpts from the narratives contained in the three hearing

transcripts, and codes were organized in the order they appeared in each transcript. The number of times each code appeared in the first cycle coding was calculated and ranked from 1 to 10. Some codes were renamed to better describe the excerpts. This renaming process represented second cycle coding and a refinement of the first cycle coding. Codes representing similar excerpts from the transcripts were grouped and apposite categories to summarize the similarities were developed. The categories were ranked according to quantitative representation of appearance. This schematic enhanced my ability to inductively answer the research question. Generalized themes from the grouped codes and ranked categories were developed, and their trajectory toward answering the research question was assessed.

Emergent Codes, Categories, and Themes

The data analysis process generated emergent codes, categories, and themes producing clarity toward answering the research question. The emergent characteristics in Table 1 summarized the codes from the first cycle coding, the ranked categories, and the corresponding generalized themes. There were no qualities of discrepant cases identified during the data analysis process, although an unusual circumstance was encountered in data collection with the emergence of extensive narratives represented by questions presented in the data collection section. These questions focused on some of the narrative excerpts already selected for coding and categorizing and did not require additional attention.

Table 1

Codes and Categories From Data Analysis

Category 1: Not enough is known about how FRT works			
Code:	Congress and users need facts	Code:	More research and clear regulations are needed
Category 2: Concerns for privacy, freedoms, and liberties			
Code:	Fourth and First Amendments' protection	Code:	Privacy issues
Code:	Fourth Amendment litigation	Code:	Effects of FRT on liberties
Code:	Fourth Amendment violation	Code:	Legislation must have privacy standards
Code:	First Amendment offense	Code:	Concern about the zone of privacy transformed by FRT
Code:	Constitutionality of FRT	Code:	FR systems exceed privacy issues and complex regulatory challenges exist
Code:	SCOTUS guidance on drafting a law		
Category 3: Concerns for consequences of FRT usage			
Code:	Flaws in FRT technology	Code:	Equal and fair treatment
Code:	Ethical issues	Code:	Algorithm effects on demographic differences
Code:	FRT expansion for surveillance will reshape dynamics of the country	Code:	Americans in jeopardy
Code:	Protections toward expansion for surveillance	Code:	FRT not ready for prime time
Code:	Surveillance needs racial justice	Code:	Accuracy, transparency, and privacy protection
Code:	Transparency concern creates anger among Americans	Code:	Important to understand and have accurate data
Category 4: Diversified congressional responsibility			
Code:	No opt-in option	Code:	FRT used with social consequences is harmful
Code:	Conflicting tasks	Subcode:	Expand FRT and ensure algorithm accuracy
Subcode:	Community safety without violating First and Fourth Amendments	Subcode:	Promote innovation and protect privacy and safety
Subcode:	Address threats before talking about good uses	Subcode:	Keep innovation going responsibility and respect people's liberties
Subcode:	Protect citizens and recognize the value of FRT to law enforcement	Subcode:	Balance security with liberty
Code:	Challenges	Code:	Valuable technology recognition
Category 5: Cessation of FRT usage preference			
Code:	Stop using FRT	Code:	Stop and assess harms and benefits
Code:	Need rules of use	Code:	Stop and perfect the process
Category 6: Ubiquitous usage of FRT			
Code:	Too late	Code:	Government behind the eight ball
Category 7: Dissatisfaction with federal government involvement and responsiveness to FRT and its usage			
Code:	Congress has not paid attention	Code:	NIST test algorithms not systems
Code:	Disclosure of FRT use by federal agencies needed	Code:	NIST algorithm testing not set for demographic effects
Code:	FBI noncompliant	Code:	Level of testing for algorithm accuracy not performed by NIST
Code:	FBI limited assessment of FRT	Code:	Authority for TSA pilot program unknown
Code:	No consent to be in FBI searchable databases	Code:	Government agencies need to work together
Code:	Authority source for use of searchable database unknown	Code:	Level of testing for algorithm accuracy not performed by NIST
Code:	FBI reporting requirements and oversight not present	Code:	Authority for TSA pilot program unknown

Category 7: Dissatisfaction with federal government involvement and responsiveness to FRT and its usage (cont.)			
		Code:	Standard bearer needed
Code:	FBI assessment of FRT usage benefits and penalties not present		
Code:	FBI unresponsive to GAO	Code:	Do not blame funding if not requested
Code:	Government accountability not evident	Code:	Urgent to rein in unchecked government use
Code:	Need NIST evaluation of any system purchase by government	Code:	Brick wall for information from government and corporate sector about technology
Category 8: Collaboration in congress			
Code:	Agreement among members	Code:	Working with both sides
Code:	Bipartisan solution needed	Code:	Bipartisan discussions to define role for federal government and Congress
Code:	Republicans and Democrats concerned	Code:	Republican and Democrat support wanted
Code:	Committed to FR legislation. Hope for bipartisan way		
Category 9: Unspecified responsible parties			
Code:	Who should enact FRT legislation?	Code:	Congress taking a leading role
Code:	Who should be at the table?	Code:	Congressional policy making is best
Code:	Suppliers' responsibility	Code:	NIST's role is not policy making
Category 10: Fear of technology			
Code:	Scary	Code:	FRT too powerful
Code:	FRT intimidating	Code:	Fear

Themes From Analysis of Codes and Categories

Ten themes emerged from the categories developed from the coding of the excerpts from the hearing transcripts. These themes are supported by the following quotations from the hearing subjects emphasizing their importance.

1. Knowledge Insecurities

> Rep. Carolyn B. Maloney (2019): To me it is extremely important we know whether the use of this technology leads to any benefits for society, especially in determining whether there is a crime this is helping to solve, or are we just weighing in on constitutional rights of people and creating constitutional risk? We cannot know this unless there is a sufficient data base for law enforcement that uses this. (Part II, p. 21)

2. Constitutional Ambiguities

Rep. Jim Jordan (2019): I thank the gentleman for yielding. So, we have got fifty million cameras in the country, a system that, as we said earlier, is—makes mistakes all the time. Those mistakes disproportionately hurt people of color. Violates First Amendment—I think violates First Amendment liberties, Fourth Amendment liberties, due process standards. (Part I, p. 28)

3. Consequences Without Remedies

Rep. Jim Jordan (2020): Increasingly, local, state, and Federal Government entities are utilizing facial recognition technology under the guise of law enforcement and public welfare, but with little to no accountability. With this technology, the government can capture faces in public places, identify individuals, allowing the tracking of our movements, patterns, and behavior. All of this is currently happening without legislation to balance legitimate Government functions with American civil liberties. That must change. And while this hearing is about commercial uses. (Part III, p. 2)

4. Diversified Congressional Responsibility

Rep. Jody B. Hice (2020): I mean, it is one thing to have policies, to have things written down. It is another thing to implement these things to protect the public, protect individuals who are not—have not consented to this type of technology. So, how will these facial recognition products, as they develop, inform individuals they are being exposed, potentially without their knowledge? (Part III, p. 26)

5. The Moratorium Solution

Andrew G. Ferguson, witness (2019): Unregulated facial recognition technology should not be allowed to continue. It is too powerful, too chilling, too under mining to principles of privacy, liberty, and security. (Part 1, p. 7)

6. Forfeited Opportunities

Rep. Kelly Armstrong (2020): I should also say this isn't the first time the government has been behind the eight ball on these issues. We are so far behind on online piracy. We are so far behind on data collection, data sharing, and those types of issues. And one of the dangers we run into with that is by the time we get around to dealing with some of these issues, society has come to accept them. And how the next generation views privacy in a public setting is completely different than how my generation and generations above us viewed privacy in a public setting. And the world is evolving with technology, and this is going to be a part of it going forward. (Part III, p. 50)

7. Governmental Pretermit

Chairman Elijah E. Cummings: In April, the Government Accountability Office sent a letter to the Department of Justice with open recommendations on the FBI's use of facial recognition technology. As that letter stated the FBI had not implemented these recommendations despite the fact that GAO initially made them three years ago. We will also hear from GAO, not only on the importance of these recommendations which focus on transparency and accuracy, but also, on the dangers associated with failing to implement them. (Part II, p. 2)

8. Bipartisan Support Necessity

Chairman Elijah Cummings: I do expect that we are going to be able to get some legislation out on this. I talked to the ranking member. There is a lot of agreement. (Part I, p. 44)

9. Purview Uncertainty

Rep. Robin L. Kelly: …as we talk about having legislation, who do you think should be at the table? Of course, we should be at the table but who else should be at the table? Because we are not the experts, so as we come up with rules and regulations. (Part I, p. 32)

10. Trepidation

Rep. Jim Jordan: And as the chairman mentioned, the potential for mischief when you think about folks exercising their First Amendment liberties at some kind of political rally, whether it is on the right or the left, as the chairman talked about, I think is scary….Stop and think then, not just the cell phone now but actually facial recognition in real-time video, as the chairman talked about, that is a scary thought. That is 1984 George Orwell kind of scenario that I think troubles us all. (Part 1, p. 3)

Evidence of Trustworthiness

There were no adjustments to consistency strategies stated in Chapter 3 regarding trustworthiness. The credibility and internal validity of the study were undisputable. The stakeholders/subjects were obtained directly from the Congressional records of the Congress of the United States and included members of the U. S. House of

Representatives (Govinfo, 2020). Prolonged engagement with the stakeholders/subjects and persistent observation of the data (transcripts) were accomplished during the 60-day study, the review of more than 14 hours of in-person testimony under oath, and video review of three hearings recording in real time (Congress.Gov, 2020).

Obtaining the data from the Congressional Records about Congressional activities was the best source of information for the purpose of this study (Govinfo, 2020). The inclusion of thick descriptions of the subjects, data location and collection process, and detailed description of the data analysis plan facilitate ready recreation of the finding. The reputation of the source of the data is indisputable, serving both as historical and legal documents of the U.S. Congress since publication began in 1873 (Govinfo, 2020). Because the data collected can be limitlessly accessed and the study may be replicated by any researcher or interested body, the transferability and external validity of findings were evident (Walden University, 2016).

Dependability and reliability of the study were evidenced by an audit trail of raw data and coding procedures to reduce, analyze, and inductively answer the research question (Walden University, 2016). By coding, categorizing, and theming the raw data, recognized occurrences of recording concerns, emotions and decisions of the subjects facilitated inductive progression toward answering the research question (Walden University, 2016). Confirmability and objectivity of the study were unchallenged because of my direct involvement in conducting the study and engagement in reflexivity by recording notes during and immediately after reviewing subjects transcribed and video comments (Walden University, 2016).

Results

Research Question: Why Has Congress Failed to Pass a National FRT Policy and How Is the Public Affected?

The data analysis process resulted in a multiplicity of calculable findings simulating reasons FRT legislation has stalled in Congress. Representative of the calculable findings was the emerged factors from themes and supporting quotes from the transcripts (Congress.Gov, 2020). These factors appear in order of significance based upon their repetitive iteration in the hearing transcripts. The factors explain and present clarity to why Congress has failed to pass a national FRT policy and how the public is affected.

Factors that Explain Why Congress Failed to Pass a National Facial Recognition Technology Policy, How the Public Is Affected, and Supporting Quotes

Factor: Knowledge Insecurities

The major concern of the Congressional committee members was the lack of information they already possessed and made available to them prior to and during the hearings. They expressed a knowledge deficit in the effects of FRT on privacy, freedom, and due process; how and why FRT affects marginalized communities and demographically diverse individuals; and how facial recognition technology works. They were devoid of knowledge about how FRT software performs; transparency, accuracy, and security issues; biometric aggregation of information; testing and standards; law enforcement and surveillance; current federal government oversight and use of FRT; and a plethora of related concerns and questions.

Knowledge insecurity was also prompted by information overload in which they expressed not enough of the right information and having too much information. The more they knew, the more they needed and wanted to know. Contributing to their insecurity were policy questions that would have to be addressed by them once an understanding of significant issues occurred. These questions included: Why FRT legislation is needed? What is wrong with FRT currently – technically, politically, and administratively? What is needed in FRT legislation? What recommendations and preferences should be adopted for the content of FRT legislation?

Quote From the Transcripts Supporting the Knowledge Insecurities Factor

> Rep. Harley Rouda (2019): And that is a fair statement. My concern is that bad actors are always going to use the tools that they can access, and if they can access these tools even though we want to prohibit it from happening, they are going to access it. So, my sense is better that we need to figure out what is the proper legislation for proper use of it and if we do move to that question—proper use, law enforcement versus private—law enforcement has been using digital enhancement of photos for years and years and I do not think anybody is suggesting that that is stepping over the line. There was mistakes that are made all the time as well. And so, my question is how do we make sure that law enforcement, in using this technology, is using it in the proper way? (Part II, p. 26)

Factor: Constitutional Ambiguity

Questions concerning the violation of the First Amendment, the Fourth Amendment and due process guarantees of the Fourteenth Amendment are rudimentary in the discussion about the use of FRT in public spaces. Included in these discussions are the deployment of searchable databases containing individuals' faces without the consent of the individuals therein, and the surveillance of suspects and the general public unknowingly by law enforcement. Congressional committee members contemplate whether to address the issue of privacy by seeking a SCOTUS interpretation of the Fourth Amendment specifically to address FRT or apply the privacy interpretations for digital technology and surveillance already decided by SCOTUS. Some Congressional committee members who participated in the protests of 2020-2021 were appalled by the use of FRT during public protests to identify and arrest participants and violate their First Amendment rights to assemble and free speech. Some were concerned the false identification of suspects by FRT, especially resulting from biased and inaccurate algorithms, are a violation of the Fourteenth Amendment. Congressional committee members know national legislation must contain privacy standards to protect the public, but they are unsure how to accomplish the task.

Quote From the Transcripts Supporting the Constitution Ambiguity Factor

> Chairman Elijah Cummings (2019): We need to do more to safeguard the rights of free speech and assembly under the First Amendment, the right to privacy under the Fourth Amendment, and the right of equal protection under the law under the Fourteenth Amendment. (Part 1, p. 2)

> Rep. Justin Amash (2019): The Supreme Court recognized recently that a person does not surrender all Fourth Amendment protection by venturing into the public sphere. Face recognition surveillance threatens to shatter the expectation Americans have that the government cannot monitor and track our movements without individualized suspicion and a warrant. (Part I, p. 41)

Factor: Consequences Without Remedies

FRT has been hailed by law enforcement, private developers, and some federal government agencies as a valuable technology. Members of the Congressional Committee raised doubt in this declaration because of the technological and deployment mistakes made by the developers and users and the harmful effects on the public. Flaws in the development of technology and the dependent algorithms that match people to biometric probes and galleries of faces have created alarms among governments and agencies at all levels of activity, and among the general public. FRT in public spaces to surveil people labels everyone a suspect and puts individuals in a perpetual lineup.

Algorithms designed with bias misidentify individuals, especially women, people of color, racial and gender diversity. Transparency, accuracy, and data security are concerns because of the lack of standards, regulations, and flawed technological design and software. No opt-in or opt-out opportunity is offered to individuals and informed consent is absent. Socioeconomically marginalized communities and people of color are subjected more to surveillance and the intrusion of FRT in their private lives. Identifying how the public is affected by FRT use in public spaces was an overwhelming concern among the subjects from personal and political viewpoints.

Quotes From the Transcripts Supporting the Consequences Without Remedies Factor

> Chairman Elijah Cummings (2019): More than half of American adults are part of facial recognition data bases and they may not even know it. (Part I, p. 2)
>
> Rep. Wm. Lacy Clay (2019): The technology identifies people's faces and runs them against a watch list of images which can include suspects, missing people, and persons of interest. But privacy campaigners have described the technology as Orwellian. I was allegedly misidentified using this technology along with twenty-seven other Members of Congress—disproportionately black and brown members. So, I have questions about the accuracy that protections against misidentification and, obviously, civil liberty issues. (Part 1, p. 22)

Factor: Diversified Congressional Responsibility

Congressional committee members were charged with the formulation of legislation which would be presented to the entire Congress to standardize the development and use of FRT. Their assignment was complex attributable to the need to mitigate an array of issues regarding FRT. Among the items were the multiplicity of simultaneous tasks which must be accomplished by the legislators during the policy formulation process. Many of these task's conflict, making it impossible to succinctly conduct the decision-making process.

Conflicting tasks challenging the Congressional committee members included: ensuring community safety without violating First and Fourth Amendment freedoms, rights and liberties; addressing threats from FRT use before discussing the beneficial uses of FRT; deciding how to protect citizens and recognizing the value of FRT to law

enforcement; balancing the need for security with the right to liberty; recognizing the expansion of FRT and ensuring algorithm accuracy; promoting innovation and protecting privacy and safety; and keeping innovation going responsibility while respecting people's liberties. Other challenges facing the legislators included formulating policy amid the vast use of FRT and accepting others' positions that FRT is valuable.

Quote From the Transcripts Supporting the Diversified Congressional Responsibility Factor

> Rep. John P. Sarbanes (2019): The second theme is whether recognizing that the technology is barreling ahead anyhow and is being adopted and applied increasingly across many different platforms, let's say, and uses, whether it is being developed in a way that ensures that when it is used, it is not being used in a discriminatory fashion, it is not being applied unfairly, et cetera. And that depends on the algorithms being developed in a way that is respectful of accurate data, and we are not there yet, as I understand it. So, it just increases the anxiety level. So, we are going to be paying a lot of attention. I am glad the Chairman is going to have you all come back, because he is right this is a moving target here. We are going to be paying a lot of attention to how the data gets digested and how the algorithms that flow from that data are being applied, whether they are accurate and so forth. So, we appreciate your testimony, but obviously this is not the end of the inquiry. (Part II, p. 51)

Factor: The Moratorium Solution

The magnitude of the Congressional committee's responsibility to formulate an all-encompassing policy rectifying all that is troubling about the FRT industry and deployment into public spaces prompted many members to call for a moratorium on the use of FRT by the federal government. This cessation of involvement would rectify their inability to act succinctly because of their depth of knowledge insecurities, concerns for potential privacy, freedoms, and due process violations, and the unaddressed consequences of FRT usage without foreseeable remedies. A standstill position was adopted by some committee members as a response to the political and social enormity of the task. Others optioned for an interruption in FRT development and use while significant issues could be resolved.

Quote From the Transcripts Supporting the Moratorium Solution Factor

> Rep. Mark Desaulnier: So, I really think, Mr. Chairman, and I am so encouraged by what I have heard in a bipartisan way today that we need to stop—that it has gone down too far. We are not starting at a metric where we are just beginning the deployment of this. It has already been deployed. And to Mr. Lynch's comments, it is being deployed not just for facial recognition but for everything we do. And there are benefits for that and we can see that, but we need a time out societally, as Europe has led us on, to say no….So, to me, this is a moment for us in a bipartisan way to say stop. (Part 1, pp. 48-49)

Factor: Forfeited Opportunities

The ubiquitous development and use of FRT with its supporting biometric and algorithmic components have almost rendered the attempt to place a moratorium on the technology or develop standards and regulations of design and application impractical. This private sector commercialized innovation meandered its way into federal government agencies such as the FBI, the Internal Revenue Service (IRS), and the Transportation Security Administration (TSA) especially in its CBP and airport security activities. State and local municipal governments and law enforcement agencies readily adapted to FRT presence to enhance public safety. Corporations, schools, health care facilities and providers, housing administrators, and other entities are using FRT to facilitate safety and identification protocols. For these organizations, FRT is a valuable presence. Congress has forfeited the opportunities to reign this technology into controllable conduct and it is too late.

Quotes From the Transcripts Supporting the Forfeited Opportunities Factor

> Rep. Gerald E. Connolly (2019): If I can pick up sort of on where we just were, Ms. Guliani. The ubiquity of this technology strikes me. Maybe we have already kind of mostly lost this battle. (Part I, p. 49)
>
> Rep. Eleanor Holmes Norton (2019): I must say I think we are already a little bit pregnant, and I agree with the ranking member, and we have got these cameras everywhere. We are a little late in saying, well, you really shouldn't be surveilling people when there is nowhere that we don't surveille people. I think we are already doing what we are already afraid of and that we ought to look very closely

> at regulation. Watch out because you will be regulating stuff that is already done by law enforcement and that nobody—and that we have given a pass to. (Part I, pp. 17-18)

Factor: Governmental Pretermit

Pertinent to the success of the Congressional committee in formulating relevant FRT policies is knowing the extent of the involvement of federal agencies in FRT use. This knowledge should include who and how the technology is used; how transparency, accuracy and security are maintained; with which agency support and oversight belong; the authorizing statue or policy for the use of FRT; and how the public is protected from violations of their rights to privacy, freedoms, and due process. Congressional committee members discovered the federal government had neglected the basic expectations of best practices in the absence of standards and regulations to proliferate the expansion of FRT through law enforcement agencies across the nation. Their dissatisfaction with federal government involvement and lackluster responsiveness to FRT and its usage was vast and strong.

The FBI specially appeared to offer the most disappointment. The agency was noncompliant and unresponsive to GAO recommendations, conducted limited assessments of FRT equipment and software, offered no informed consent to individuals to be included in the FBI searchable database, had no identified authority to develop and distribute the searchable database, no reporting requirements and oversight protocols established for users, and did not conduct assessments of FRT usage penalties and benefits.

The Congressional committee had no interest in affecting private industry development and commercialization of FRT. Their interests resided in the federal government requiring private developers to meet certain requirements before federal dollars are expended. This expectation was abandoned by the federal agencies. Collaboration among federal agencies, federally funded organizations that test FRT software, and private FRT developers was nonexistent. The Congressional committee learned there was no "go-to" federal source of knowledge and support.

Quotes From the Transcripts Supporting the Government Pretermit Factor

> Rep. Carolyn B. Maloney (2019): The American people deserve government accountability, and I actually agree with the questioning of the minority party leadership on this, that you don't have answers on how it is working, how it was set up, what is coming out of it, whether it is hurting people, helping people. You don't even have information on whether it is aiding law enforcement in their goal for hunting down terrorists. So, we need more accountability. (Part II, p. 22)
>
> Gretta L. Goodwin, witness (2019): "We also reported on accuracy concerns about FBI's face recognition capabilities. Specifically, we found that the FBI conducted limited assessments of the accuracy of the face recognition searches before they accepted and deployed the technology. For example, the face recognition system generates a list of the requested number of photos. The FBI only assessed accuracy when users requested a list of fifty potential matches. It did not test smaller list sizes, which might have yielded different results. Additionally, these tests did not specify how often incorrect matches were

> returned. Knowing all of this, the FBI still deployed the technology. (Part II, pp. 5-6)

Factor: Bipartisan Consensus

Congressional committee members were cognizant of the importance of bipartisan consensus in the formulation of FRT policy. The multitude of FRT issues and the organizational stakeholders in FRT existence, including federal, state, and local governments, civil liberties advocates, and corporate FRT developers and users, demanded a national policy had support on both sides of the aisle to be viable. Committee members were in bipartisan agreement on the thematic factors which emerged from the hearing transcripts. Throughout the proceedings, gratitude and compliments were expressed by various members for the harmonious environment and willingness to reach a bipartisan decision. Bipartisan discussions and reconciliations were essential to define the role for the federal government and Congress in the FRT arena.

Quote From the Transcripts Supporting the Bipartisan Consensus Factor

> Rep. Jimmy Gomez (2020): So, we will start having these important discussions in a bipartisan way to figure out how and what can the Federal Government do. What can Congress do? What is our responsibility? I also appreciate the ranking member's commitment to legislation because I know that this issue is a tough one, and it only could be done in a bipartisan way. (Part III, p. 4)

Factor: Purview Uncertainty

When the Congressional committee members asked the following emergent questions in the hearing transcripts, the identification of the responsible party or lead

agency to provide answers was nonexistent: Why FRT legislation is needed? What is wrong with FRT currently – technically, politically, and administratively? What is needed in FRT legislation? What recommendations and preferences should be adopted for the content of FRT legislation? Federal response was vague and responsibility unassigned. This purview uncertainty added to the factors that explain why a national policy to regulate FRT has not passed.

Quotes From the Transcripts Supporting the Purview Uncertainty Factor

> Rep. James Comer (201): My first question is to Professor Ferguson. Should states and localities be able to enact their own facial recognition technology laws?... So does all the panel agree that the Federal Government needs to set the floor before states and localities create their own rules and regulations with respect to this? Is that a consensus among everyone on the panel? Yes or no. (Part I, pp. 27- 28)
>
> Rep. Robin L. Kelly (2019): As we talk about having legislation, who do you think should be at the table? Of course, we should be at the table but who else should be at the table? Because we are not the experts, so as we come up with rules and regulations. (Part 1, p. 32)
>
> Clare Garvie (2019), witness: I fundamentally believe it is up to communities to decide to take a close look at how this technology is being used, what its capabilities and limitations are and decide whether the risks outweigh the benefits. That may be an appropriate use for this technology. But fundamentally, that needs

> to be a decision made by legislatures, not by law enforcement agencies. (Part 1, p. 32)
>
> Dr. Cedric Alexander (2019), witness: Yes, ma'am. I certainly do think a couple of things. One here is that certainly you need to be at the table. The technology developer of that software needs to be at the table. Public safety needs to be at that table. ACLU needs to be at that table, and other legal persons as well, too, so that if we are going to utilize this technology in public safety, in law enforcement, I think one thing needs to be made clear to these software manufacturers is that if you are going to develop this technology it is going to have to meet a standard that you hear being articulated at these—at this table by the scientists and those in the legal communities that are here. It needs to meet that standard. If it can't meet that standard, then there is no place for it in our society. Police need to be at the table so they can clearly understand if you decide—your jurisdiction decide to pay for and acquire this technology, you are going to be held to a standard as well, too. (Part I, pp. 32-33)

Factor: Trepidation

Congressional committee members experienced knowledge insecurities about a technology that threatened to violate the First, Fourth and Fourteenth Amendments, which had no standards or regulations, no responsible administrator, and no oversight, caused them to become apprehensive in their decision-making responsibilities. For those who expressed this consternation, their emotions were a genuine reflection of those who favored the moratorium solution to FRT policy formulation. Fear of the technology

created a disquietude among some of the committee members that one of them was compelled to compare FRT usage to George Orwell's *1984* novel.

Quotes From the Transcripts Supporting the Trepidation Factor

> Rep. Jim Jordan (2019): The potential for mischief when you think about folks exercising their First Amendment liberties at some kind of political rally, whether it is on the right or the left, as the chairman talked about, I think is scary.
>
> We learned in that hearing also that the IRS was actually involved in using this technology—the same IRS that a few years ago targeted people for their political beliefs. We found that—we found that very scary. Stop and think then, not just the cell phone now but actually facial recognition in real-time video, as the chairman talked about, that is a scary thought. That is 1984 George Orwell kind of scenario that I think troubles us all. (Part I, p. 3)
>
> Rep. Rashidam Tlaib (2019): Thank you, Mr. Chairman. I have to tell you—and through the Chairman, I hope this is okay—this stuff freaks me out. I am a little freaked out by facial recognition, Mr. Chairman. I hope that is okay, I can say that. Chairman Cummings (2019): Yes, that is okay. (Part II, p. 46)

Table 2

Inductive Migration of Categories to Themes and Factors

INDUCTIVE MIGRATION OF CATEGORIES TO THEMES AND FACTORS		
	CATEGORIES	THEMATIC FACTORS
1	Not enough is known about how FRT works	Knowledge Insecurities
2	Concerns for Privacy, Freedoms, and Liberties	Constitutional Ambiguity
3	Concerns for Consequences of FRT Usage	Consequences Without Remedies
4	Multiplicity of Simultaneous Tasks	Diversified Congressional Responsibility
5	Cessation of FRT Usage Preference	The Moratorium Solution
6	Ubiquitous Usage of FRT	Forfeited Opportunities
7	Dissatisfaction with Federal Government Involvement and Responsiveness to FRT and Its Usage	Governmental Pretermit
8	Collaboration in Congress	Bipartisan Consensus
9	Unspecified Responsible Parties	Purview Uncertainty
10	Fear of Technology	Trepidation

Summary

The answer to the research question was summarized in two dimensions of purpose. Knowing the answer to the foremost portion of the research question, *Why Congress has failed to pass a national FRT policy?* is important in closing the gap in the literature which recognized the stagnation in federal FRT legislation but offered no explanation. The study answers the research question by identifying the factors explaining why Congress has not passed federal legislation for FRT usage in public spaces. The following factors emerged from the data analysis and inductive processes:

1. Congressional committee members failed to pass legislation regulating a technology for which they have knowledge insecurities about how it works.
2. Congressional committee members experienced constitutional ambiguity and could not pass legislation that would not assure individuals FRT legislation would safeguard their privacy and protect their rights

guaranteed by the Fourth Amendment, the First Amendment, the Fourteenth Amendment, and civil liberties.

3. Congressional committee members failed to pass a national FRT policy because they were unable to reconcile their concerns about the consequences of FRT without offering remedies to FRT adversities. Eliminating gender, racial, and algorithmic biases inherent in FRT was beyond their forte.
4. Congressional committee members failed to pass legislation regulating a technology because of the multiplicity of issues they had to simultaneously address. An example of their diversified responsibilities occurred when discussing the value of FRT. Congressional members acknowledged the usefulness of the technology in air transportation, border crossings, and in warranted surveillance, but questioned the societal benefits of FRT usage in public spaces. They had to secure the country's safety and guarantee individual liberties concurrently.
5. Congressional committee members failed to pass legislation because they were divided on the issue of declaring a moratorium on the use of FRT in public spaces until their concerns could be satisfied, including the establishment of standards and regulations that protected privacy. Alexander (2019) noted that this act would be "like the horse that have already gotten out the gate and now we are trying to catch up with it" (Part I, p. 19). Members in favor of a moratorium were not deterred. This

contributed to the Congressional committee members inability to pass a national FRT policy.

6. Congressional committee members failed to pass legislation regulating a ubiquitous technology. The proliferation of FRT in the private sector and at every level of government made the task useless. Congress had forfeited its opportunities to regulate the technology in its initial stages of existence.
7. Congressional committee members failed to pass legislation because the support needed to execute the policy and provide oversight responsibilities could not be identified or confidently assigned to an agency. This governmental pretermit could not be overlooked. This became obvious to them when they were disappointed in the noncompliance by the FBI to the GAO recommendations regarding FRT management and transparency issues.
8. Congressional committee members failed to pass legislation regulating a technology without bipartisan consensus. The committee members on both sides of the aisle supported the passage of FRT legislation and supported a moratorium as a solution. They were in bipartisan agreement with the controversial issues related to FRT usage. The committee was concerned with bipartisan consensus among the body of members of the U. S. House of Representatives once proposed legislation was out of committee and introduced as a bill.

9. Congressional committee members failed to pass legislation that established technological development and operational accuracy standards about which they did not possess expertise. Recognizing this factor, they were undecided who should be responsible for developing FRT rules and which group of subject matter experts should join them to establish standards and regulatory requirements. Purview uncertainty was another stoppage to the formulation of a national FRT policy.
10. Because of their knowledge insecurities, the ubiquitous nature of FRT in governmental and private industry, and the potential adverse impact of FRT usage on the public, Congressional committee members saw FRT as scary. The trepidation they expressed contributed to their inability to pass FRT legislation.

The second portion of the research question was answered proliferatively by Congressional committee members and expert witnesses and contributed to their inability to formulate and pass a national FRT policy. *How is the public affected?* by the use of FRT in public spaces included the following items identified in the data analysis and inductive processes:

1. FRT use in public spaces threatens First Amendment rights to assemble for peaceful protests, free speech, and other civil liberties.
2. FRT use in public spaces threatens the right to privacy guaranteed by the Fourth Amendment.

3. Misidentification of individuals is a grave concern and can lead to legal and criminal problems.
4. Biometric data are sometimes altered, and algorithms are developed with human biases. These occurrences promote racial and gender biases. Women and people of color are particularly adversely impacted by these biases.
5. Communities with economic insecurities are disproportionately affected by FRT used for surveillance.
6. Affirmative consent so individuals can have a choice to be placed in a data bank regulated by algorithms or be surveilled without cause is ignored in FRT usage in public spaces.

Conclusively, the synergistic nature of regulations to individual protections from FRT harms is obvious because the consequences of FRT use do not have readily available remedies. Federal legislation to regulate FRT use in public spaces must be augmented by a plan to simultaneously enforce the protection of the public against controversial issues associated with the use of the facial recognition technology in public spaces.

In Chapter 5, I interpreted the findings, described the limitations encountered while conducting the study, stated recommendations for future research, described the implications of social change at various levels of society, and presented the conclusion to the study.

Chapter 5: Discussion, Recommendations, and Conclusion

The purpose of this qualitative study was to explore the factors explaining why Congress has not passed legislation addressing the use of FRT in public spaces in the United States. I conducted a case study of the concerns and decisions of the U.S. House of Representatives Congressional committee members and testimonials from other contributors to the Committee on Oversight and Reform to identify factors imploding the passage of legislation during the policy formulation process. I focused on the research question: *Why Congress has failed to pass a national FRT policy and how is the public affected?*

The nature of the qualitative study provided flexibility and permitted a change in the data analysis procedures toward the direction of the data. I was able to arrive at conclusions and propose the solution to the research problem through the narratives of the research subjects. The nature of the study also facilitated the observation of the essence of the NPF melodramatic political process (Blair & McCormack, 2016) underpinning this study and included the emergence of inferences from narratives and viewpoints of the subjects.

Interpretation of Findings

The U.S. House of Representatives Congressional Committee on Oversight and Reform was charged with the responsibility of formulating a national FRT policy to standardize the development and use of FRT and protect the rights of the public simultaneously. After a series of hearings and testimonials from expert witnesses, the Congressional committee was unable to propose a policy. Because of the national

controversy about FRT at all levels of government and private industry, I conducted a case study analysis of the transcripts from the hearings. Through the emergence of themes from coding and categorizing excerpts from the hearing transcripts, the research question about why Congress has failed to pass a national FRT policy and how the public is affected was answered. The findings extended knowledge in the discipline by filling the gap in the literature citing the lack of a needed national FRT policy but neglected to state why the void existed.

Assertion From the Finding

The findings from the case study analysis of the hearing transcripts and the video viewing of the records of the hearing presented the following assertion about why Congress has failed to pass a national FRT policy: the members of the Congressional committee were overwhelmed with the complexities of FRT. Kabigting (2019) noted that "feeling overwhelmed arises as an engulfing turbulence" (p. 55). Conflict and confusion regarding FRT encircled the Congressional committee members, rendering them unknowing how to react to create national FRT legislation.

Overwhelmed With the Inundation of Information

In the Congressional hearings, the expert witnesses and fellow members imparted a vast array of knowledge. Congressional committee members became engulfed with their new learning, but the presented information was not enough, and the more they knew, the more they needed and wanted to know. Information overload ensued. More hearings and subcommittee meetings were requested from members who were uncomfortable with their new-found knowledge or lack of it. Wright (2019) noted in the

literature review not enough is known about the attention these issues are getting from lawmakers at the federal level (Politico, 2020). Hamann and Smith (2019) concurred identifying the issues with passing federal regulations is necessary for the elimination of the ambiguity that exists among proponents and opponents of a national FRT policy. Congressional committee members requested more facts and more hearings before attempting decision-making regarding FRT legislation (Appendix A, Table A1, Narratives 22-23, 66; Appendix B, Table B1, Narrative 22; Appendix C, Table C1, Narratives 26-27).

Overwhelmed by Privacy Protections Versus Security and Safety

The Congressional committee members were overwhelmed by the predicament in which they found themselves. They knew any decision they made regarding standards and regulations may infringe upon the privacy, freedoms, and due process guarantees of the constitution. FRT influenced the privacy of the individual for both proponents and opponents of the utilization of FRT, and the propensity for Fourth Amendment violations emphasized in the literature review by Hamann and Smith (2019). The uncertainty of the application of the amendments to FRT development and use made decision-making incredulous. The harms FRT development and use in public spaces cause and threats to constitutional protection while providing security and safety to society were overwhelming to Congressional committee members when presented by the expert witnesses and from personal testimony of some committee members (Appendix A, Table A1, Narratives 1, 12, 14-15, 18, 27; Table A2, Narratives 5, 11-12, 36; Appendix B, Table B1, Narrative 1).

Overwhelmed by the Adversities Created by FRT Without Remedies

Making legislative decisions about privacy intrusion, biased algorithms, equipment flaws, transparency, data accuracy and security issues, surveillance of suspects and the general public, and other adversities without remedies were overwhelming. Kloppenburg and Van der Ploeg (2020) supported this concern by stating the functionality of the biometric system is flawed and resulting errors are inappropriately attributed to an ingrained gender and racial bias of the application taunted by privacy advocacy groups and other opponents of FRT use. How to remedy these adversities was beyond the scope of knowledge of the Congressional committee members, as indicated in the excerpts from the hearing transcripts (Appendix A, Table A1, Narratives 2, 4-5, 7, 19; Table A2, Narratives 21, 24).

Overwhelmed by Their Lack of FRT Expertise

Multi-tasking to address every issue relevant to FRT standardization and regulations in a series of meetings and void of expertise in this industry was overwhelming to the Congressional committee members. To balance the value of FRT to law enforcement with the need to protect the public from surveillance and misidentification was difficult, and the committee members were not confident to perform the task or resolve similar situational conflicts. Wright (2019) concurred those issues must be resolved because self-regulation of the FRT industry and utilization is inadequate to ensure the civil liberties of individuals are not disregarded. Recognizing their limitations to resolve these issues became a reasonableness for inactivity (Appendix

A, Table A1, Narratives 39, 44; Appendix B, Table B1, Narratives 9, 18, 36; Appendix C, Table C1, Narratives 15, 46, 49).

Overwhelmed Enough to Support the Termination of FRT Usage

Calling for a moratorium on the use of FRT signified the extent to which some Congressional committee members were overwhelmed. Some members vocalized a desire to cease further development and use of FRT. Others desired to interrupt the use of the technology until the conflicts with it could be resolved. Crawford (2019) agreed the use of FRT should cease until there is regulation to ensure safeguards to protect the civil and legal rights of individuals, transparency, accountability, and fairness. Congressional committee members viewed the withdrawal of the development and use of FRT as the only viable solution to their insurmountable problems regarding enacting FRT legislation (Appendix A, Table A1, Narratives 6, 24, 38, 54, 58, 63).

Overwhelming Tasks to Rectify a Ubiquitous Situation

Congressional committee members became cognizant of the vanished opportunities to enact FRT regulatory legislation in the early development and use of FRT. These missteps contributed to the overwhelming tasks of rectifying a situation that was already awry in some respects. The need to enact FRT legislation before further proliferation of FRT in public spaces occurred causing citizens to choose between safety and the loss of freedom was supported by Wynn (2015) as necessary, but a plan to achieve this task was not offered in the literature (Horton, 2018). Congressional committee members acknowledged they were too late to stop or start the FRT implementation anew (Appendix A, Table A1, Narratives 13, 25-26, 29, 42, 48).

Overwhelmed by the Lack of Existing and Prospective Support

Finding out how government agencies usually relied upon had neglected or abandoned their expected duties regarding FRT development and use was disappointing to the Congressional committee members. They were overwhelmed by the lack of existing and prospective support for FRT policy administration and oversight in federal government. Nakar and Greenbaum (2017) emphasized the need for governmental leadership to resolve the fragmentation in guidance and laws across the nation regarding FRT use in public spaces and allay the prominent social issue of privacy intrusion. Vincent (2020) cited while the conglomerate of proponents and opponents of FRT utilization waited for the formulation and enactment of legislation to regulate FRT, federal governmental agencies had been ordered to take a "light touch" approach to regulatory and non-regulatory developments, outside the federal government, that utilized AI, which included FRT. Congressional committee members' resources for informational support and activities regarding matters as serious as FRT were absent (Appendix A, Table 1, Narratives 10, 50; Appendix B, Table B1, Narratives 3-5, 11, 13-14, 16, 21, 24, 26-27, 32-33; Table B2, Narratives 7, 15, 17-18, 21-22, 28; Appendix C, Table C1, Narratives 7, 11, 43).

Overwhelmed by Bipartisan Consensus

Congressional committee members were positively overwhelmed with the bipartisan support for FRT policy formulation and for the cessation of activity toward a FRT policy. Wright (2019) urged collaborative federal regulations through clarity of the issues so FRT can flourish without creating unwarranted circumstances for individuals.

Zeng et al. (2019) concurred identifying and discussing the controversial and disconcerting issues regarding FRT and its benefits to society is necessary so regulation of the industry can occur. Bipartisan support on various FRT issues occurred without coaxing. Congressional committee members were awed by the ready desire of the opposite party to work together for FRT legislation (Appendix B, Table B1, Narrative 23; Appendix C, Table C1, Narratives 8-9, 33, 39, 46; Table 2, Narrative 5).

Overwhelmed With Doubt About Their Role

Congressional committee members were overwhelmed with doubt about their role in the development of standards and regulations for FRT management. The extended enumeration of governmental, corporate, and advocacy stakeholders who should be included in the policy formulation process and their specific roles became undefinable. Zeng et al. (2019) explained the controversies surrounding the technological development of FRT will continue until there is government regulation formulized with business representatives. Zeng et al. also indicated governing the development of AI was at the core of regulating FRT and mitigating controversies. Congressional committee members were speculative and inclusive about who should be around the FRT decision-making table (Appendix A, Table A1, Narratives 45, 52, 55-56, 68).

Overwhelmed With Fear to Act

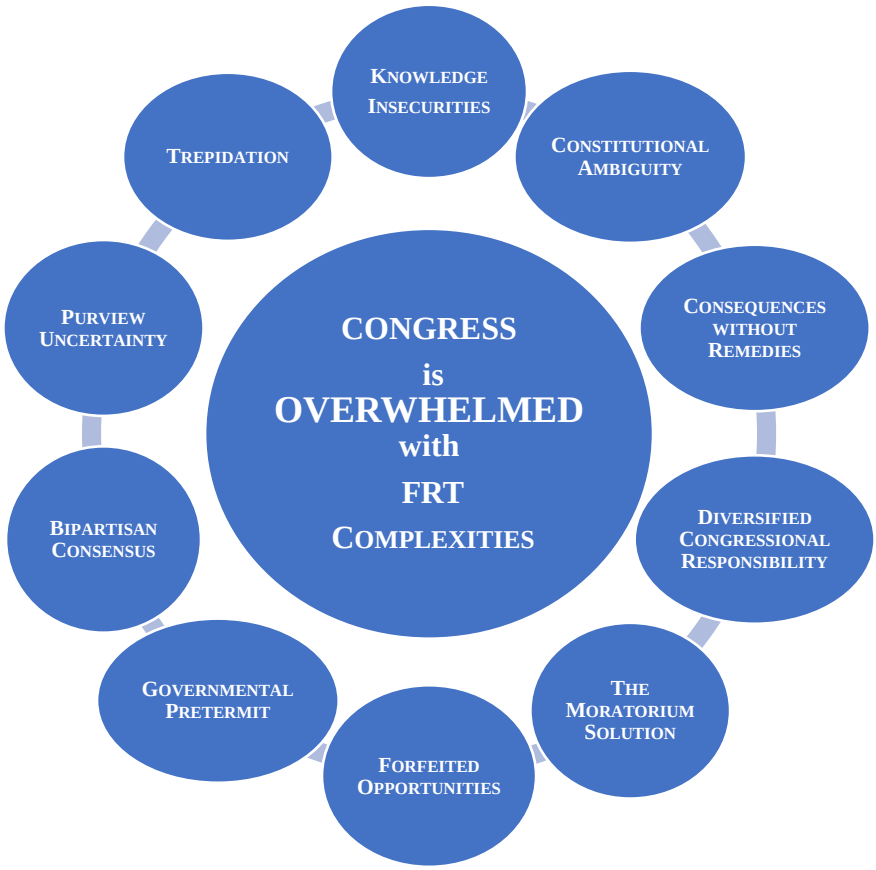
The Congressional committee members were overwhelmed by information overload and the need for more facts, the need to balance privacy protections with the public's need for security and safety, frustrations from identifying remedies to address the harms arising FRT usage in public places, facing the responsibility to make decisions

about a technology outside their bailiwick, and the desperation to call a cessation on FRT. They were overwhelmed by their inattentiveness to FRT and their missed opportunity to address its initiation, their disbelief there was no federal administrative management and oversight in place nor support to navigate them through the FRT maze, the surprise of bipartisan support for a solution, and their uncertainty about their role and the roles of others in participating in formulating and passing FRT legislation. For some Congressional committee members, these overwhelming conditions made them afraid to take action for fear of taking the *wrong* action (Appendix A, Table A1, Narratives 3, 26, 61; Appendix B, Table B1, Narrative 15).

On the basis of these findings, it appears the assignment to pass a national FRT policy is too complex to mitigate by Congress and stasis in the formulation of a national policy will continue. Figure 3 summarizes this cyclical response to the need for a national FRT policy. Regardless of these concerns, the proliferation of the development and utilization of FRT for safety, security and crime control will not ebb (Garvie et al., 2016), especially since the results of utilization are considered more beneficial than the risks to the general public with regulatory policies (IJIS Institute, 2019; Selinger & Hartzog, 2019).

Figure 3

Congress is Overwhelmed with FRT Complexities



Analysis of the Findings and the Theoretical Framework

The analysis of findings of this study aligned with the NPF process selected for this research. The hearing transcripts contained the melodramatic discourse of Congressional protagonists and antagonists' actors who pontificated their opinions on the political committee meeting stages (Blair and McCormack, 2016). By studying the narratives of the political actors, I became cognizant of purposeful communication among individuals intended to influence policy formulation (Jones & McBeth, 2020), and the

thematic factors explaining why Congress has failed to pass a national policy on FRT and how the public is affected emerged.

Limitations of the Study

In Chapter 1, a concern that Congress would pass a national FRT policy before this study was expressed. The lack of direct affiliation with members of the committee was also a concern. Neither of these possibilities were realized, and there were no limitations to the study. There were no issues of trustworthiness, and no changes to Chapter 1 are necessary.

Recommendations

Future research into why Congress has not passed a national FRT policy and how the public is affected should include a case study analysis of the most recent Congressional committee hearings regarding a national FRT policy. Since this study commenced, bills have been introduced in Congress for a moratorium on FRT use and federal agency requirements such as transparency, accuracy, and insecurity. Future research should include a comparison of this study with the results of new case study analyses to determine the validity of the thematic factors which emerged in this study.

Application of the findings could assist the Congressional committee members to realize why they have failed to pass a national FRT policy and how the public is affected by FRT use in public spaces. The thematic factors contributing to these findings require the Congressional committee members to identify with and focus specifically on their affecting conditions and implement professional and personal strategies to diminish the affecting condition. The summative assertion from the findings that the committee

members are overwhelmed must be allayed before substantive actions toward policy formulation and passage may occur. The findings, the summative assertion of being overwhelmed, and mitigation strategies may also assist both chambers of Congress to realize the pathway to passing FRT legislation. A major strategy to mitigate this national dilemma may include formalizing a federal-level unit with the combined FRT expertise to address each delaying factor identified in this study; the responsibility to pursue and define solutions; and the task to present a comprehensive product to Congress for enactment.

Implications of Positive Social Change

The factors affecting the passage of a national FRT policy are the same factors disturbing the general society concerning FRT use in public spaces. The public is also overwhelmed with an unknown technology, the potential loss of liberties, the harms to them, especially perpetual surveillance without consent and biased misidentification. Also troubling to the general society are Congressional delays due to conflicting demands, a willingness to cease a technology that has already gone too far to start over, a government which has neglected its duty to protect the public while assisting in security and public safety measures, and a hope for bipartisan compromise to allay their fears of a consequential technology. The fact that the technology affects marginalized communities and people of color more than any other race and threatens the basic liberties and freedoms of all people is disruptive in society. If members of Congress implement the mitigating strategies, they can pass a national policy that alleviate FRT disturbances to

the extent possible, and positive social change regarding FRT use in public spaces may occur.

Conclusion

This study identified factors explaining why Congress has failed to pass a national FRT policy and how the public is affected. By coding, categorizing, and theming the narratives from the Congressional committee members transcribed hearings on FRT, ten factors emerged presenting clarity to the lack of action by Congress. The findings indicated a summative assertion that the committee members were overwhelmed by FRT and all its caveats, creating stagnation in their ability to enact legislation. This indication would have to be addressed both professionally and personally by individual members of the committee and Congress as a whole. The findings also implicated the factors affecting legislative activity affect the public in similar ways. Mitigating the situation within Congress will allay the concerns within society and promote positive social change.

Analyzing the findings in the context of the NPF revealed the accuracy of the descriptive elements of this framework. The findings in the study indicated the influential operation of the narratives in the hearings as they unobtrusively directed the policy formulation process and the stagnation of that process in this study (Jones & McBeth, 2020). Through this type of discourse, political agendas are expounded, and policies are either formulated to become law or "upstaged" and rejected (Blair & McCormack, 2016).

FRT continues to be developed and proliferate in this country and the public and advocacy groups continue to be appalled at the consequences of its use in public spaces. Although "the problem that has occurred it is kind of like the horse that have already

gotten out the gate and now we are trying to catch up with it," (Alexander, 2019, p.19), FRT is not going away but expanding and not regulating it in some beneficial manner for both users and individuals will not make it better.

References

ACLU. (2019). The FBI is tracking our faces in secret. We're suing. https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing/

Agüera y Arcas, B., Mitchell, M., & Todorov, A. (2017). Physiognomy's new clothes. *Medium.* https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a

Alalouff, R. (2020). Surveillance technology. Why AI and facial recognition software is under scrutiny for racial and gender bias. *IFSEC Global.* https://www.ifsecglobal.com/video-surveillance/why-ai-and-facial-recognition-software-is-under-scrutiny-for-racial-and-gender-bias/

Alexander, C. (2019). Hearing Before the Committee on Oversight and Reform, House of Representatives. http://www.docs.house.gov

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association: JMLA*, *107*(1), 1–5. https://doi.org/10.5195/jmla.2019.615

Anderson, S. (2019). Why Was the Homeland Security Department Created? *Forbes.* https://www.forbes.com/sites/stuartanderson/2019/04/12/why-was-the-homeland-security-department-created/?sh=6da4f9dfad4b

Andrejevic, M., & Neil, N. (2019). Facial recognition technology in schools: Critical questions and concerns. *Journal of Learning, Media, and Technology*, *45*(2), 115–128. https://doi.org/10.1080/17439884.2020.1686014

Anghel, D. (2020). Facebook to pay Illinois $550 million to settle privacy lawsuit. *The Daily Illini.* https://dailyillini.com/news/2020/02/20/facebook-pay-illinois-550-million/

Antilla, L. (2005). Climate of skepticism: US newspaper coverage of the science of climate change. *Global Environmental Change. 15*(4), 338–352. https://doi.org/10.1016/j.gloenvcha.2005.08.003

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open, Elsevier Ltd, 2,* 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Bennett, K. (2001). Can facial recognition technology be used to fight the new way to against terrorism: Examining the constitutionality of facial recognition surveillance systems. *North Carolina Journal of Law and Technology, 3*(1), 151–174. https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1018&context=ncjolt

Birnbaum, E. (2020). Supreme Court declines to hear Facebook facial recognition case. *The Hill.* https://thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case

Blair, B., & McCormack, L. (2016). Applying the narrative policy framework to the issues surrounding hydraulic fracturing within the news media: A research note. *Research and Politics, 1*(3). https://doi.org/10.1177/2053168016628334

Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., & Guest, R. (2018). Biometrics: Accessibility challenge or opportunity? *PLoS ONE, 13*(3). https://doi.org/10.1371/journal.pone.0194111

Bowyer, K. (2004). Face recognition technology: Security versus Privacy. *IEEE Technology and Society Magazine.* https://www3.nd.edu/~kwb/Bowyer_Tech_Soc_2004.pdf

Bradford, B., Yesberg, J., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology, 60*(6), 1502–1522. https://doi.org/10.1093/bjc/azaa032

Bradford, L. (2020). A history of CCTV technology: how video surveillance technology has evolved. *SURVEILLANCE-VIDEO*. https://www.surveillance-video.com/blog/a-history-of-cctv-technology-how-video-surveillance-technology-has-evolved.html/

Brown, K. (2014). Anonymity, faceprints, and the constitution. *George Mason Law Review, 409(21)*2. http://www.georgemasonlawreview.org/wp-content/uploads/2014/03/Brown-Website.pdf

Buolamwini, J., & Timnit Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research 81*, 1–15. Conference on Fairness, Accountability, and Transparency. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Carter, A. (2018). Facing reality: The benefits and challenges of facial recognition for the NYPD. *Naval Postgraduate School*. Monterey, California. www.hsdl.org

Celentino, J. (2016). Face-to-face with facial recognition evidence: Admissibility under the post-Crawford confrontation clause, *MICH. L. REV., 114*, 1317. https://repository.law.umich.edu/mlr/vol114/iss7/3

Chikowore, A. (2018). Advocacy coalition framework as an actor-centered approach to policy formulation and implementation. https://www.ippapublicpolicy.org/file/paper/5b1e8454029ff.pdf

Cleland J. A. (2017). The qualitative orientation in medical education research. Korean journal of medical education, 29(2), 61–71. https://doi.org/10.3946/kjme.2017.53

Coburn, T. (2015). A Review of the Department of Homeland Security's Missions and Performance. A Report by Senator Tom Coburn Ranking Member Committee on Homeland Security and Governmental Affairs. U.S. Senate 113th Congress January 2015. https://www.hsgac.senate.gov/imo/media/doc/Senator%20Coburn%20DHS%20Report%20FINAL.pdf

Collins, T. (2019). Facial recognition: Do you really control how your face is being used? *USA Today.* https://www.usatoday.com/story/tech/2019/11/19/police-technology-and-surveillance-politics-of-facial-recognition/4203720002/

Commonwealth of Massachusetts. (2019). An Act establishing a moratorium on face recognition and other remote biometric surveillance systems. Bill S.1385. *191st General Court.* https://malegislature.gov/Bills/191/s1385

Conger, K., Fausset, R., & Kovaleski, S. (2019). San Francisco bans use of facial recognition technology. *The New York Times.* https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Congress.Gov. (2019). S.847 - Commercial facial recognition privacy act of 2019. 116th Congress (2019-2020). https://www.congress.gov/bill/116th-congress/senate-bill/847

Congress.Gov. (2019) S.2878 - Facial Recognition Technology Warrant Act of 2019. *116th Congress (2019-2020)***.** https://www.congress.gov/bill/116th-congress/senate-bill/2878

Congress.Gov. (2020). Legislation: Facial recognition technology search. https://www.congress.gov/search?q={%22source%22:%22legislation%22,%22search%22:%22facial+recognition+technology%22}&pageSize=100&page=2&searchResultViewType=expanded

Congress.Gov. (2020). H.R.3619 - Coast Guard Authorization Act of 2010. *111th Congress (2009-2010).* https://www.congress.gov/bill/111th-congress/house-bill/3619?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=77

Congress.Gov. (2020). H.R.3875 - To prohibit Federal funding from being used for the purchase or use of facial recognition technology, and for other purposes. *116th Congress (2019-2020).* https://www.congress.gov/bill/116th-congress/house-

bill/3875?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=1

Congress.Gov. (2020). H.R.4760 - Securing America's Future Act of 2018. *115th Congress (2017-2018).* https://www.congress.gov/bill/115th-congress/house-bill/4760?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=45

Congress.Gov. (2020). H.R.6381 - DHS Reform and Improvement Act. *114th Congress (2015-2016).* https://www.congress.gov/bill/114th-congress/house-bill/6381?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=61

Congress.Gov. (2020). H.R.6929 - Advancing Facial Recognition Act. *116th Congress (2019-2020).* https://www.congress.gov/bill/116th-congress/house-bill/6929?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=3

Congress.Gov. (2020). H.R.7156 - Federal Police Camera and Accountability Act of 2018. *115th Congress (2017-2018).* https://www.congress.gov/bill/115th-congress/house-bill/7156?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=42

Congress.Gov. (2020). H.R.7356 - Facial Recognition and Biometric Technology Moratorium Act of 2020. *116th Congress (2019-2020).* https://www.congress.gov/bill/116th-congress/house-bill/7356/text

Congress.Gov. (2020). S.744 - Passport Identity Verification Act. *112th Congress (2011-2012).* https://www.congress.gov/bill/112th-congress/senate-bill/744?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=65

Congress.Gov. (2020). S.1261 - PASS ID Act. *111th Congress (2009-2010).* https://www.congress.gov/bill/111th-congress/senate-bill/1261?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&r=75&s=2

Congress.Gov. (2020). S.3284 - Ethical Use of Facial Recognition Act. *116th Congress (2019-2020).* https://www.congress.gov/bill/116th-congress/senate-bill/3284

Congress.Gov. (2020). S.3771 - FUTURE of Artificial Intelligence Act of 2020. *116th Congress (2019-2020).* https://www.congress.gov/bill/116th-congress/senate-bill/3771?q=%7B%22search%22%3A%5B%22facial+recognition+technology%22%5D%7D&s=2&r=16

Corrigan, J. (2019). White House unveils a national artificial intelligence initiative. *Nextgov.* https://www.nextgov.com/emerging-tech/2019/02/white-house-unveils-national-artificial-intelligence-initiative/154795/

Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. *Nature.* https://www.nature.com/articles/d41586-019-02514-7

Crow, D., Lawhon, L., Berggren, J., Huda, J., Koebele, E., & Kroepech, A. (2017). A narrative policy framework analysis of wildfire policy discussions in two Colorado communities. *Politics & Policy, 45*(4), 626-

656. 10.1111/polp.12207. Wiley Periodicals Inc. http://www.learningfromdisasters.org/publications/2017.02.pdf

DARPA. (2018). Defense advanced research projects agency, 1958-2018. https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf

Das, A., Degeling, M., Wang, X., Wang, J., Sadeh, N., & Satyanarayanan, M. (2017) Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. *In Proceedings of the 30th IEEE Computer Vision and Pattern Recognition Workshops (CVPRW)*, 1387–1396. http://ieeexplore.ieee.org/document/8014915/ https://www.ftc.gov/system/files/documents/public_events/1223263/privacycon_worldofcameras_das2_0.pdf

Davis, J. (1979). The plain view doctrine (conclusion). FBI Law Enforcement Bulletin. Federal Bureau of Investigation, Washington, D. C. https://www.ncjrs.gov/pdffiles1/Digitization/63104NCJRS.pdf

Dharaiya, D. (2020). History of facial recognition technology and its bright future. *Readwrite.* https://readwrite.com/2020/03/12/history-of-facial-recognition-technology-and-its-bright-future/

Del Greco, K. (2019). Facial Recognition Technology: Ensuring Transparency in Government Use. https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use

Department of Justice (DOJ). (2020). The USA PATRIOT Act: Preserving life and liberty. https://www.justice.gov/archive/ll/highlights.htm

Electronic Privacy Information Center (EPIC), 2020. Facial recognition. https://epic.org/privacy/facerecognition/

Engle, J. (2020). Should facial recognition technology be used in schools? *The New York Times.* https://www.nytimes.com/2020/02/07/learning/should-facial-recognition-technology-be-used-in-schools.html

Etikan, I., Musa, S., & Alkassim, R. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4.

FBI.gov. (2020). Terrorist screening center. https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc

Future of Privacy Forum. (2018). Privacy principles for facial recognition technology in commercial applications. https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf

Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up. *Georgetown Law Center on Privacy & Technology.* https://www.perpetuallineup.org/

Gates, K. (2006). Identifying the 9/11 ‘faces of terror’- the promise and problem of facial recognition technology. *Journal of Cultural Studies, 20*(4-5), 417 – 444. https://www.tandfonline.com/doi/abs/10.1080/09502380600708820

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. *Artificial Intelligence in Healthcare,* 295–336. https://doi.org/10.1016/B978-0-12-818438-7.00012-5

Givens, A., Busch, N., & Bersin, A. (2018). Going Global: The International Dimensions of U.S. Homeland Security Policy. *Journal of Strategic Security 11*(3), 1-34. DOI: https://doi.org/10.5038/1944-0472.11.3.1689.

Gorbonosov, G. (2019). Patel v. Facebook: Ninth Circuit Grants Facebook's Motion to Stay in Facial Recognition Lawsuit. Edited by Jonathan Blake. https://jolt.law.harvard.edu/digest/patel-v-facebook-ninth-circuit-grants-facebooks-motion-to-stay-in-facial-recognition-lawsuit

Govinfo. (2020). Congressional Record (Bound Edition). *U.S. Government Publishing Office.* https://www.govinfo.gov/app/collection/crecb.

Hamann, K., & Smith, R. (2019). Facial recognition technology: Where will it take us? *American Bar Association*. https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/

Hanko, H. (n.d.). The Framework hypothesis & Genesis 1. http://www.prca.org/pamphlets/pamphlet_83.html

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case Study Research: Foundations and Methodological Orientations [34 paragraphs]. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 18*(1), Art. 19, http://nbn-resolving.de/urn:nbn:de:0114-fqs1701195

Harwell, D. (2019). ACLU sues FBI, DOJ over facial recognition technology over facial recognition technology – criticizing unprecedented surveillance secrecy. *The Washington Post.* https://www.washingtonpost.com/technology/2019/10/31/aclu-

sues-fbi-doj-over-facial-recognition-technology-criticizing-unprecedented-surveillance-secrecy/

Hirose, M. (2017). Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology. *Connecticut Law Review, 49*(5). https://opencommons.uconn.edu/cgi/viewcontent.cgi?article=1376&context=law_review

Hochreutiner, C. (2019). The history of facial recognition technologies: How image recognition got so advanced. AnyConnect Academy. https://anyconnect.com/blog/the-history-of-facial-recognition-technologies

Horton, J. (2018). Privacy under pressure: A survey of privacy expectations in the modern age. https://jewlscholar.mtsu.edu/bitstream/handle/mtsu/5695/Horton_mtsu_0170N_10980.pdf?sequence=1

IJIS Institute. (2019). Law enforcement facial recognition use case catalog. *IJIS Institute and IACP Law Enforcement Imaging Technology Task Force.* https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf

Introna, L., & Nissenbaum, H. (2009) Facial recognition technology. A survey of policy and implementation issues. *The Center for Catastrophe Preparedness and Response*. New York University.

https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy_and_Implementation_Issues

Jackson, K. (2019). Challenging facial recognition software in criminal court. *National Association of Criminal Defense Lawyers, Inc.* https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf

Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G., …& Choi, T. (2019). A facial recognition mobile app for patient safety and Biometric identification: Design, development, and validation. *JMIR Mhealth Uhealth, 7*(4), e11472. http://mhealth.jmir.org

Johnson, D. (2019). Are federal facial recognition programs supported by existing law? *FCW. The Business of Federal Technology.* https://fcw.com/articles/2019/06/04/facial-recog-house-ogr-hearing.aspx

Jones, M., & McBeth, M. (2010). A narrative policy framework: clear enough to be wrong? *Policy Studies Journal 38*(2), 329–353

Jones, M., & McBeth, M. (2020). Narrative in the tie of Trump: Is the narrative policy framework good enough to be relevant? *Administrative Theory and Praxis, 42*(2), 91-110, DOI: 10.1080/10841806.2020.1750211

Justia. (2019). Patel v. Facebook, Inc., No. 18-15982 (9th Cir. 2019). https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html

Kabigting, Edwin-Kikko R. (2018). Conceptual Foreknowings: Integrative Review of Feeling Overwhelmed. *Nursing Science Quarterly 2019*, 32(1) 54-60, sagepub.com/journals-permissions, DOI: 10.1177/0894318418807931. journals.sagepub.com/home/nsq

Kline, C. (2017). Eigenface for face detection. Georgia College, Department of Mathematics. https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/kline.pdf

Kloppenburg, S., & Van der Ploeg, I. (2018). Securing identities: Biometric technologies and the enactment of human bodily differences. *Journal of Science as Culture, 29*(1), 57-76, DOI: 10.1080/09505431.2018.1519534

Kolker, A. (2020). Biometric Entry-Exit System: Legislative History and Status. *In Focus.* Congressional Research Service. https://fas.org/sgp/crs/misc/IF11634.pdf

Kortli, Y., Jridi, M., Falou, A., & Atri, M. (2020). Face Recognition Systems: A Survey. *Sensors (Basel, Switzerland), 20*(2), 342. https://doi.org/10.3390/s20020342

Krithika L., Venkatesh K., Rathore, S., & Harish, K. (2017). Facial recognition in education system. *IOP Conf. Series: Materials Science and Engineering, 263*. doi:10.1088/1757-899X/263/4/042021

Laperruque, J., & Janovsky, D. (2018). These Police Drones are Watching You. *POGO.* https://www.pogo.org/analysis/2018/09/these-police-drones-are-watching-you/

Latman, N., & Herb, E. (2013). A field study of the accuracy and reliability of a biometric iris recognition system. *Journal of Sci Justice. 53*(2), 98-102. doi: 10.1016/j.scijus.2012.03.008

Laureate Education (Producer). (2014-a). *Research methods and design II – part 1* [Video file]. Baltimore, MD: Author.

Learned-Miller, E. (2020). Researchers Call for New Federal Authority to Regulate Facial Recognition Tech. Experts cite profiling, breach of privacy and surveillance as potential societal risks. *News & Media Relations.* University of Massachusetts Amherst. https://www.umass.edu/newsoffice/article/researchers-call-new-federal-authority

Leavens, A. (2015). The Fourth Amendment and surveillance in the digital world. J. *C.R. & Econ. Dev*., *27*(709). https://digitalcommons.law.wne.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1273&context=facschol

Litt, R. (2016). The Fourth Amendment in the information age. *The Yale Law Journal, 126.* https://www.yalelawjournal.org/forum/fourth-amendment-information-age

Lohr, S. (2018). Facial recognition is accurate, if you're a white guy. *The New York Times.* https://www2.cs.duke.edu/courses/spring20/compsci342/netid/readings/facialrecnytimes.pdf

Lunter J. (2020). Beating the bias in facial recognition technology. *Biometric Technology Today*, *2020*(9), 5–7. https://doi.org/10.1016/S0969-4765(20)30122-3

Main, D. (2017). Who are millennials? *LiveScience.* https://www.livescience.com/38061-millennials-generation-y.html

Maranzani, B. (2019). How U.S. intelligence misjudged the growing threat behind 9/11. *History.* https://www.history.com/news/9-11-attacks-america-missed-warning-signs

Martinez-Martin, N. (2019). What are important s implications of using facial recognition technology in health care? *AMA Journal of Ethics.* https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2019-02

Mayhew, S. (2018). History of biometrics. *Biometric update.com.* https://www.biometricupdate.com/201802/history-of-biometrics-2

McCabe, R., & Chaffey, T. (2011). What's Wrong with the Framework Hypothesis? https:/answersingenesis.org/creationish/old-earth/whats-wrong-with-the-framework-hypothesis/

McClellan, E. (2020). Facial Recognition Technology: Balancing the Benefits and Concerns. Journal of Business & Technology Law *15*(2). https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1322&context=jbtl

Mesnik, B. (2016). The history of video surveillance. *KINTONICS.* https://kintronics.com/the-history-of-video-surveillance/

Mileva, M., & Burton, A. (2019). Face search in CCTV surveillance. *Cogn. Research 4***(**37). https://doi.org/10.1186/s41235-019-0193-0

Moraes, T., Almeida, E., & de Pereira, J. (2020). Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. *AI Ethics*. https://doi.org/10.1007/s43681-020-00014-3

Moyer, R. (2019). The cognition of controversy: Examining policy elites' narrative cognition and communication around hydraulic fracturing practices in the U.S. https://scholarworks.uark.edu/etd/3531

Murphy, J. (2018). Chilling: The constitutional implications of body-worn cameras and facial recognition technology at public protests. *Washington. & Lee Law Review Online, 75*(1/1). https://scholarlycommons.law.wlu.edu/wlulr-online/vol75/iss1/1

Nakar, S., & Greenbaum, D. (2017). Now you see me. now you still do: Facial recognition technology and the growing lack of privacy. http://www.bu.edu/jostl/files/2017/04/Greenbaum-Online.pdf

National Institute of Justice (NIJ). (2020). History of NIJ Support for Face Recognition Technology. https://nij.ojp.gov/topics/articles/history-nij-support-face-recognition-technology

Norval, A., & Prasopoulou, E. (2017). Public faces? A critical exploration of the diffusion of facial recognition technologies in online social networks. *New Media & Society, 19*(4), 637 –654. SAGE. DOI: 10.1177/1461444816688896

Nwosu, K. (2016). Mobile facial recognition system for patient identification in medical emergencies for developing economies. *Journal for the Advancement of Developing Economies, 10.* https://digitalcommons.unl.edu/jade/10

Ologunde, R. (2015). Plastic surgery and the biometric e-passport: Implications for facial recognition. *Journal of Plastic Surgery and Hand Surgery, 45*(2). https://www.tandfonline.com/doi/abs/10.3109/2000656X.2014.951052?journalCode=iphs20

Omoviola, B. (2018). Overview of biometric and facial recognition techniques article. *ResearchGate.* DOI: 10.9790/0661-2004010105

Pierce, J., Hicks, K., Peterson, H., & Giordono. L. (2017). Common approaches for studying the advocacy coalition framework: Review of methods and exemplary practices. *European Consortium for Political Research General Conference.* Oslo, Norway. https://ecpr.eu/Filestore/PaperProposal/b0e4eb57-d311-4b73-9a45-56a8f46374f2.pdf

Policy Studies Journal. (2018). Special issue: Advances in narrative policy framework. *PSJ, 46*(4). Danvers, MA.

Qualitative Practice. (n.d.). An invitation to qualitative research, Chapter 1. https://www.sagepub.com/sites/default/files/upm-binaries/34087_Chapter1.pdf

Raudins, S. (2020). Facial recognition, thermal imaging part of the new normal. *Government Technology. The Columbus Dispatch.* https://www.govtech.com/products/Facial-Recognition-Thermal-Imaging-Part-of-the-New-Normal.html

Robertson, D., Kramer, R., & Burton, M. (2015). Face averages enhance user recognition for smartphone security. *PLoS One, 10*(3), e0119460. doi: 10.1371/journal.pone.0119460.

Ropek, L. (2019). Facial recognition software on the rise in U. S. *Government Technology (gt).* https://www.govtech.com/products/Facial-Recognition-Software-on-the-Rise-in-US-Schools.html

Roussi, A. (2020). Resisting the rise of facial recognition. *Nature.* https://www.nature.com/articles/d41586-020-03188-2

Rudestam, K., & Newton, R. (2015). Surviving your dissertation: A comprehensive guide to content and process (4th ed.). Thousand Oaks, CA: Sage. ISBN: 978-1-4522-6097-6

Saldana, J. (2016). The Coding Manual for Qualitative Researchers. *SAGE Publications, Inc.*

Samsel, H. (2019). California becomes third state to ban facial recognition software in police body cameras. *Security Today.* https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx

Schaffhauser, D. (2020). Study recommends total ban on facial recognition in schools. *The Journal.* https://thejournal.com/articles/2020/08/12/study-recommends-total-ban-on-facial-recognition-in-schools.aspx

Schoonenboom, J., & Johnson, R. (2017). How to construct a mixed methods research design. *Kolner Zeitschrift fur Soziologie und Sozialpsychologie*, *69*(Suppl 2), 107–131. https://doi.org/10.1007/s11577-017-0454-1

Segovia, S. (2015). Privacy: An issue of priority. *Hastings Business Law Journal (11)*1/8. https://repository.uchastings.edu/hastings_business_law_journal/vol11/iss1/8

Selinger, E., & Hartzog, W. (2019). What happens when employees can read your facial expressions? *Berkman Klein Center for Internet Society at Harvard University*. https://cyber.harvard.edu/story/2019-10/what-happens-when-employers-can-read-your-facial-expressions

Selinger, E., & Hartzog, W. (2019). What happens when employees can read your facial expressions? *The New York Times*. https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html

Senate RPC. (2019). Facial recognition: Potential and risks. Senate Policy Papers. *U. S. Senate. Senate Republican Party Committee.* https://www.rpc.senate.gov/policy-papers/facial-recognition-potential-and-risk

Shanahan, E., McBeth, M., Hathaway, P., & et al. (2008). Conduit or contributor? The role of media in policy change theory. *Policy Sciences 41*(2), 115–138

Shanahan, E., Jones, M., & McBeth, M. (2011). Policy Narratives and Policy Processes. *Policy Studies Journal. 39*(3), 535-561

Shanahan, E., McBeth, M. & Hathaway, P. (2011). Narrative policy framework: the influence of media policy narratives on public opinion. *Politics and Policy 39*(3), 373–400

Shanahan, E., Jones, M., & McBeth, M. (2017). How to conduct a Narrative Policy Framework Study. *The Social Science Journal*. https://doi.org/10.1016/j.soscij.2017.12.002

Shanahan, E., Jones, M., McBeth, M., & Radaelli, C. (2018); The narrative policy framework. In Weible, C., & Sabatier, P. (Eds). *Theories of the Policy Process, 4*, 173 -213. Westview Press

Simonite, T. (2020). A bill in Congress would limit uses of facial recognition. *Wired.* https://www.wired.com/story/bill-congress-limit-uses-facial-recognition/

Singer, N., & Isaac, M. (2020). Facebook to pay $550 million to settle facial recognition suit. *The New York Times.* https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html

Singh, S. (2018). Techniques and challenges of facial recognition: A critical review. *Science Direct.* Elsevier. https://www.sciencedirect.com/science/article/pii/S1877050918321252

Soliman, H., Saleh, A., & Fathi, E. (2013). Face recognition in mobile devices. *International Journal of Computer Applications (0975 -8887), 73*(2). https://research.ijcaonline.org/volume73/number2/pxc3889525.pdf

Spencer, S. (2015). Data aggregation and the Fourth Amendment. *Journal of Internet Law*. Walden University Database.

Steinbock, D. (2006). Designating the Dangerous: From Blacklists to Watch Lists. *Seattle University Law Review 30*(65).

https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1883&context=sulr

Stimson, C., & Habeck, M. (2016). Reforming intelligence: A proposal for reorganizing the intelligence community and improving analysis. *The Heritage Foundation.* https://www.heritage.org/defense/report/reforming-intelligence-proposal-reorganizing-the-intelligence-community-and

Sutton, J., & Austin, Z. (2015). Qualitative Research: Data Collection, Analysis, and Management. *The Canadian journal of hospital pharmacy*, *68*(3), 226–231. https://doi.org/10.4212/cjhp.v68i3.1456

Thales Group. (2019). DHS's automated biometric identification system IDENT – the heart of biometric visitor identification in the USA. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system

Trump, D. (2019). Executive Order on maintaining American leadership in artificial intelligence. *Executive Order 13859.* The White House. https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

Turk, M., & Pentland, A. (1991). Face recognition using Eigenfaces. *IEEE.* Massachusetts Institute of Technology. https://sites.cs.ucsb.edu/~mturk/Papers/mturk-CVPR91.pdf

United States Congress. (1968). Omnibus crime control and safe streets. Crime control. Public Health Law 90-351; 82 STAT. 197. http://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf

U. S. Custom & Border Protection (CBP). (2020). CBP Introduces Biometric Facial Comparison at Progreso Port of Entry to Secure and Streamline Travel. https://www.cbp.gov/newsroom/local-media-release/cbp-introduces-biometric-facial-comparison-progreso-port-entry-secure

U. S. Custom & Border Protection (CBP). (2020). CBP to Introduce Biometric Facial Comparison to Secure and Streamline Travel at Cross Border Xpress and Tecate. https://www.cbp.gov/newsroom/national-media-release/cbp-introduce-biometric-facial-comparison-secure-and-streamline#

United States Government Accountability Office (GAO). (2020). Facial recognition technology. Privacy and accuracy issues related to commercial uses. Report to Congressional Requesters. https://www.gao.gov/assets/710/708045.pdf

United States House of Representatives. (2019). Facial Recognition Technology: Part I Its Impact on our Civil Rights and Liberties. Hearing Transcript. http://www.docs.house.gov

United States House of Representatives. (2019). Facial Recognition Technology: Part II Ensuring Transparency in Government Use. Hearing Transcript. http://www.docs.house.gov

United States House of Representatives. (2019). Facial Recognition Technology: Part III Ensuring Commercial Transparency and Accuracy. Hearing Transcript. http://www.docs.house.gov

Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., … & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, *7*(1), lsaa038, https://doi.org/10.1093/jlb/lsaa038

Vincent, B. (2020). White House proposes "light-touch regulatory approach" for artificial intelligence. *Nextgov.* https://www.nextgov.com/emerging-tech/2020/01/white-house-proposes-light-touch-regulatory-approach-artificial-intelligence/162276/

Vought, R. (2019). Guidance for Regulation of Artificial Intelligence Applications. https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

Walden University. (2016). Trustworthiness. Research Theory, Design, and Methods. *Laureate Education Inc.*

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220. http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Weible, C., & Sabatier, P. (Eds). (2018). *Theories of the Policy Process, 4*. Westview Press

Wessler, N. (2019). The federal court sounds the alarm on the harms of facial recognition technology. *ACLU.* https://www.aclu.org/blog/privacy-technology/surveillance-technologies/federal-court-sounds-alarm-privacy-harms-face

West, J. (2017). The history of face recognition. *FACEFIRST*. https://www.facefirst.com/blog/brief-history-of-face-recognition-software/#

Wiltz, T. (2019). Facial recognition software prompts privacy, racism concerns in cities and states. *PEW*. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/08/09/facial-recognition-software-prompts-privacy-racism-concerns-in-cities-and-states

Wright, E. (2019). The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector. *Fordham Intell. Prop. Media & Ent. L.J., 29*(611). https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6

Wynn, E. (2015). Privacy in the face of surveillance: Fourth amendment considerations for facial recognition technology. *Naval Postgraduate School*: Monterey, California. https://calhoun.nps.edu/bitstream/handle/10945/45279/15Mar_Wynn_Eric.pdf?sequence=1&isAllowed=y

Yeung, D. (2018). Social Media as a Catalyst for Policy Action and Social Change for Health and Well-Being: Viewpoint. *J Med Internet Res 20*(3), e94. DOI: 10.2196/jmir.8508

Yeung, D., Balebako, R., Gutierrez, C., & Chaykowsky, M. (2020). Face recognition technologies: Designing systems that protect privacy and prevent bias. *Homeland Security Operational Analysis Center* operated by the RAND Corporation. https://www.rand.org/pubs/research_reports/RR4226.html

Zaeri, N., Baker, F., & Dib, R. (2015). Thermal face recognition using moments invariants. *Researchgate. International Journal of Signal Processing Systems 3*(2), 94-99. https://www.researchgate.net/publication/270284797_Thermal_Face_Recognition_using_Moments_Invariants

Zeng, Y., Lu, E., Sun, Y., & Tian, S. (2019). Responsible facial recognition and beyond. https://arxiv.org/ftp/arxiv/papers/1909/1909.12935.pdf

Appendix A: Hearing Transcript Part I

Figure A1

Hearing Transcript Part 1: Facial Recognition Technology - Its Impact on our Civil Rights and Liberties

FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES

HEARING

BEFORE THE

COMMITTEE ON

OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MAY 22, 2019

Serial No. 116–27

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
http://www.oversight.house.gov
http://www.docs.house.gov

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
KATIE HILL, California
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

JIM JORDAN, Ohio, Ranking Minority Member
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
JAMES COMER, Kentucky
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
RALPH NORMAN, South Carolina
CLAY HIGGINS, Louisiana
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

DAVID RAPALLO, *Staff Director*
YVETTE BADU-NIMAKO, *Legislative Director/Counsel*
GINA KIM, *Counsel*
LAURA RUSH, *Deputy Chief Clerk/Security Manager*
CHRISTOPHER HIXON, *Minority Staff Director*
CONTACT NUMBER: 202-225-5051

C O N T E N T S

Page
Hearing held on May 22, 2019 1

WITNESSES

Ms. Joy Buolamwini, Founder, Algorithmic Justice League
Oral Statement 4
Mr. Andrew G. Ferguson, Professor of Law, David A. Clarke School of Law, University of the District of Columbia
Oral Statement 5
Ms. Clare Garvie, Senior Associate, Center on Privacy & Technology, Georgetown University Law Center
Oral Statement 7
Ms. Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties *Union*
Oral Statement *9*
Dr. Cedric Alexander, Former President, National Organization of Black Law Enforcement Executives
Oral Statement *11*
Written statements for the witnesses are available on the U.S. House of Representatives Document Repository at: https://docs.house.gov.

INDEX OF DOCUMENTS

The documents entered into the record during this hearing are listed below, and are available at: https://docs.house.gov.
* Letter from the Information Technology and Innovation Foundation; submitted by Mr. Connolly and Ms. Miller.
* News article from May 17, 2019, ″Researchers alarmed by Detroit's pervasive, expanding facial-recognition surveillance program;″ submitted by Ms. Tlaib.
* Massachusetts Senate Resolution No. 1385 and House Resolution 1538; submitted by Mr. Lynch.
* Washington Post article from 10-23-18, ″Amazon met with ICE officials over facial-recognition system that could identify immigrants;″ submitted by Ms. Ocasio-Cortez.
* Letter dated 5-21-19 from EPIC; submitted by Mr. Cummings.
* Letter dated 5-17-19 from POGO; submitted by Mr. Cummings.
* Article on Geofeedia Case Study regarding Baltimore County; submitted by Mr. Cummings.

Table A1

Part I: Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces

Pathway To Answering the Research Question: Dimensions Of Purpose Record			
FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES Hearing Transcript			
Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces			
	Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**
1	We need to do more to safeguard the rights of free speech and assembly under the First Amendment, the right to privacy under the Fourth Amendment, and the right of equal protection under the law under the Fourteenth Amendment. (p. 2)	Need safeguards	Protection Under the law
2	Our goal with this review is to identify sensible and concrete recommendations, legislative or otherwise, that recognize the benefits of this technology to protect against this abuse (p. 3)	Benefits versus abuse	Protection from harm
3	…the potential for mischief when you think about folks exercising their First Amendment liberties at some kind of political rally, whether it is on the right or the left, as the chairman talked about, I think is scary. We learned in that hearing also that the IRS was actually involved in using this technology—the same IRS that a few years ago targeted people for their political beliefs. We found that—we found that very scary. Stop and think then, not just the cell phone now but actually facial recognition in real-time video, as the chairman talked about, that is a scary thought. That is 1984 George Orwell kind of scenario that I think troubles us all. (p. 3)	Scary	
4	You have already heard facial recognition and related technologies have some flaws. (p. 4)	Flaws in FRT technology	Harm to the public
5	Mistaken identity is more than an inconvenience and can lead to grave consequences. (p. 4)	Flaws in FRT technology	Harm to the public
6	At a minimum, Congress should pass a moratorium on the police use of facial recognition as the capacity for abuse, lack of oversight, and technical immaturity poses too great a risk, especially for marginalized communities. (p. 4)	Stop Using FRT	
7	One NIST data set was 75 percent male and 80 percent lighter skin, or what I like to call a pale male data set. (p. 5)	Flaws in FRT technology	Harm to the public
8	We cannot adequately evaluate facial analysis technologies without addressing this critical issue. Moving forward, the demographic and phenotypic composition of NIST benchmarks must be made public and updated to better inform decisionmakers about the maturity of facial analysis technology. (p. 5)	Need facts	
9	The harvesting of face data also requires guidelines and oversight. (p. 5)	Guidelines and oversight needed	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
10	Our faces may well be the final frontier of privacy. Congress must act now to uphold American freedoms and rights. At a minimum, Congress should require all Federal agencies and organizations using Federal funding to disclose current use of face-based technologies. We cannot afford to operate in the dark. (p. 5)	Disclosure of FRT use by federal agencies	Transparency
11	Congress must act—must act now to regulate facial recognition technologies because the case-by-case slow process of Fourth Amendment litigation is inadequate to address the rapidly changing world of mass surveillance. (p. 6)	Fourth Amendment litigation	
12	First, the Fourth Amendment will not save us from the privacy threat posed by facial recognition technology. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of these new technologies. (p. 6)	Fourth Amendment litigation	
13	**But they are chasing an accelerating train and will not catch up.** Only legislation can respond to the real-time threats of real-time Technology. (p. 6)	Too late	
14	Second, the Fourth Amendment was never meant to be the sole source of government regulation. Instead, our entire constitutional system is premised upon Congress taking a leading role guided by and only in a rare instance overruled by our founding Constitution. (p. 6)	Fourth Amendment regulation. Congress taking a leading role	
15	Third, the few steps the Supreme Court has made on the subject of locational tracking technologies offer guidance about how to avoid drafting a law that could get struck down on Fourth Amendment grounds (p. 6)	SCOTUS guidance on drafting a law	Court Guidance
16	Fourth, as Congress builds the scaffolding off that constitutional floor, we need to think about the technology not just through the lens of today but with an eye toward the expansion of surveillance technologies that will combine, aggregate, link, and share data … reshape the existing power dynamics of government and the people. (p. 6)	FRT expansion for surveillance Will reshape dynamics of country	
17	Legislation must future approve privacy protections with an eye toward the growing scope, scale, and sophistication of these systems of surveillance. (p. 6)	Protections toward expansion for surveillance.	
18	Finally, these Fourth Amendment questions must be coupled with a focus on First Amendment freedoms, civil rights, and fundamental fairness when it comes to public safety protections. (p. 6)	Fourth and First Amendments. Public safety protections	
19	The burden of surveillance technology has never been equally shared across socioeconomic or racial groups. Surveillance is both a civil rights issue and a civil liberties issue, and Congress needs to regulate with racial justice in mind. (p. 7)	Surveillance needs racial justice	Bias neutral applications
20	But face recognition is too powerful, too pervasive, too susceptible to abuse to continue unchecked. (p. 9)	FRT too powerful	Scary
21	It is time to hit the pause button. Congress must intervene to stop the use and expansion of this dangerous technology until we can fully debate what if any uses should be permitted by law enforcement. (p. 9)	Stop using FRT	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
22	As we debate this issue, we must do so with complete facts. Thus, I urge the committee to investigate two things. One, how is ICE, the FBI, and other Federal agencies using this technology? (p. 10)	Need facts	
23	Two, the committee should look at companies that are aggressively marketing this technology to the government, including how accurate their technologies are and what responsibility they take to prevent abuse. (p. 10)	Need facts	
24	But I think, you know, one of the important things of this hearing is to ask the questions and have the debate, and until we do that, we just shouldn't be using that technology for all of the concerns it raises. I mean, the advice I would have is to not use the technology until there has been a legislative process and clear standards and rules. (p. 14)	Stop using FRT	
25	I must say **we are already a little bit pregnant,** and I agree with the ranking member, **and we have got these cameras everywhere. We are a little late** in saying, well, you really shouldn't be surveilling people when there is nowhere that we don't surveille people. (p. 17)	Too late	
26	I think we are already doing what we are already afraid of and that we ought to look very closely at regulation. Watch out because you will be regulating stuff that is already done by law enforcement and that nobody—and that we have given a pass to. (p. 18)	Scary Too late	
27	This idea that we don't like arbitrary police powers or permanent police powers all speaks to the fact that the Supreme Court, if faced with the right case, might see this as a Fourth Amendment violation. (p. 18) Unfortunately, these cases take a long time to get there. Unfortunately, that it would be, you know, relying on the Fourth Amendment may not be the place we want to be …. (p. 18)	Fourth Amendment violation	
28	Chairman CUMMINGS. But an hour ago you said that you were not anxious to see a moratorium and it sounds like you may have changed that a little bit. Mr. ALEXANDER. Well, I mean—I mean, I am not because, you know, one thing I support, Chairman, I support technology. But I support good technology and I support technology that has rules with it, and it has oversight with it and there is policies written around it. I, certainly, would rather not see a moratorium. However, if the issues have been articulated here today are as serious as we believe them to be, then we have to go back and ask ourselves that question. We have to be cautious if we are going to put a moratorium on this technology, I also want to hear … the benefits, if any—if any. What have been the benefits and how do we utilize some of those benefits in some type of constructive way until we work out the bigger problems around the issues that we have discussed here today. I just don't want to throw the baby out with the bathwater if there is some way in which this technology, which I am going to make a reasonable assumption and based on my own experience in some ways it has been useful through this process of learning more and putting legislation around it. (pp. 56-57)	Stop and Assess harms and benefits	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
29	There are opportunities for that. The problem that has occurred it is kind of like **the horse that have already gotten out the gate and now we are trying to catch up with it**, because if you think about the vast utilization of facial recognition that is going on and the questions that we are posing today are going to come with a great deal of challenges. (p. 19)	Too late Challenges	
30	These software companies need to not just pass this technology to me; I need to be sure that my folks are trained. There is ethics. There is morals that goes along with it. There is policy. There is standards. There is good practices that we know, and we feel good about. (p. 20)	Valuable technology recognition	
31	But I am not certain if a total moratorium in light of the fact that we still live in an environment where we are under a great deal of threat, we still can utilize this technology. But it has to be in a way right now how do we do that while work trying to develop some standards. (p. 20)	Valuable Technology recognition Standards Needed	Benefits of FRT
32	But I think this hearing and the hearings that are going to follow, and maybe even some smaller sessions particularly with our Federal law enforcement, i.e., FBI, who utilizes this technology to fight off potential threats on a much larger scale, I think when you start talking about local policing in and of itself I think to have an opportunity to talk to some of the chiefs across the country in terms of how they are using this technology and how they think it could best benefit them if we can develop some limited framework in which they can operate from and maybe not as vast that it is now because it certainly is a serious issue and concern and problem that we have. (p. 20)	Need facts	
33	It is not as transparent as it should be, and it certainly is going to create a great deal of angst and anger among Americans in this country and particularly people who are—who are—their First and Fourth Amendments are violated. (pp. 20-21)	Transparency concern creates Anger among Americans	
34	But I am not sure if a total moratorium on this is going to be the answer to us because we still have a homeland we have to protect and there is still some value in facial recognition. (p. 21)	Valuable technology recognition	
35	So, in the EU where GDPR was passed because there is a provision for biometric data consent, they actually have an option where you have to opt in. Right now, we don't have that in the U.S. and that is something we could immediately require today. (p. 21)	No opt-in option	Informed consent
36	No elected officials are weighing in on this so that is sort of the list. But then I also think there is this chilling impact, this intimidation concept that is out there, …. (p. 28)	FRT intimidating	
37	Let us get the information out there, understand the dangers, understand whether this technology is really the helpful—the way people say it is and then let legislatures like this decide. (p. 22)	Need facts	
38	It would fundamentally undermine the First Amendment and the right of free expression and our freedom of association. I think it is chilling and a problem and needs to be Banned. (p. 52)	First Amendment offense Stop using FRT	Harm to public

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
39	The problem is here is that we are trying to keep the communities safe, at the same time trying not to violate people's First and Fourth Amendment rights. (p. 27)	Conflicting tasks – community safety without violating First and Fourth Amendment	Dual Responsibility
40	The problem is, is that the technology is developed by a software company. It is sold to a police department without proper training, without proper understanding by that department the utilization of it, and the unintended consequences. That becomes a real problem. We have to be able to train. We have to be able to understand the technology. (p. 27)	Congress and Users need facts	
41	One, there are going to be uses of this technology where we are going to want a flat-out ban, right—real-time tracking, use in protests, use in sensitive areas. And two, I think to determine what, if any, uses are permissible, we need the facts. You know, we referenced a U.K. study where there was a 95 percent inaccuracy rate. To me, that is a very relevant question as to whether we want this type of technology being used by law enforcement at all. So, until we have those facts, I think it is hard to answer all the questions. (p. 26)	Need facts	
42	They will rub up against each other and we somehow have to figure this out. But I don't think you can do one—just throw one out and just get—**you can't throw the baby out with the bathwater** is what I am trying to say. (p. 27)	Too Late - You can't throw the baby out with the bath water	
43	Does this—does this technology— we see that there are mistakes. Is there a greater propensity for mistakes with the current technology than previous technologies, whether it is artist's renderings or photographs in general? (p. 27)	Flaws in FRT technology	
44	And so, we have to address, I think, those fundamental threats before we can sort of talk about what are or aren't good uses. (p. 27)	Conflicting Tasks -address threats before talking about good uses	Dual Responsibility
45	Should states and localities be able to enact their own facial recognition technology laws? I think the Federal Government should set the floor and I think that states and local governments can raise that floor and create more protections. (p. 27)	Who should enact FRT legislation	
46	So, to me, this is a moment for us in a bipartisan way to say stop. (p. 49)	Stop using FRT	
47	But if it is going to continue to harm the American people, then it is certainly something in which we need to consider putting some pause to, if you will, in being able continue to investigate what is the good part of this technology, if possible, we still can utilize as we go. (p. 57)	Stop and Assess harms and benefits	
48	If I can pick up sort of on where we just were, Ms. Guliani. The ubiquity of this technology strikes me. Maybe we have already kind of mostly lost this battle. (p. 49)	Too late	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
49	So, we need to change the way in which we evaluate facial analysis technology, so we truly understand who it works for and who it fails on. (p. 32)	Need facts	
50	You know, oftentimes when there is a technology, as you pointed out, it will be used. However, the users see it to advance whatever their cause is, without any public input or any public limitations. And you have been doing the hard work while Congress has really not been paying much attention. (p. 29)	Congress has not paid attention	
51	So regardless of the bias or how well the technology works, there should be a choice. But second, we need to know how well the technology works and what my research has shown is that the standards from the National Institute for Standards and Technology aren't even reflective of the American people. So, we have to start there to make sure that we even have a base line for what is going on, and then there is continuous oversight because regardless of the accuracy, regardless of if there is consent, these systems, as the fellow panelists have mentioned, can be abused in all kinds of ways. (p. 30)	Need facts	
52	…as we talk about having legislation, who do you think should be at the table? Of course, we should be at the table but who else should be at the table? Because we are not the experts, so as we come up with rules and regulations. I fundamentally believe it is up to communities to decide to take a close look at how this technology is being used, what its capabilities and limitations are and decide whether the risks outweigh the benefits. That may be an appropriate use for this technology. But fundamentally, that needs to be a decision made by legislatures, not by law enforcement agencies. Mr. ALEXANDER. Yes, ma'am. Yes, ma'am. I certainly do think a couple of things. One here is that certainly you need to be at the table. The technology developer of that software needs to be at the table. Public safety needs to be at that table. (pp. 32-33)	Who should be at the table?	Leadership unknown
53	For me, and I am quite sure for many of my colleagues across the country, this technology that we are referring to can be very valuable in terms of keeping our communities and keeping our country safe. (p. 19)	Valuable technology recognition for safety	Benefits of FRT
54	Clare Garvie, witness: For all these reasons, a moratorium on the use of face recognition by police is both appropriate and necessary. It may be that we can establish common sense rules that distinguish between appropriate and inappropriate uses, uses that promote public safety and uses that threaten our civil rights and liberties. (p. 9)	Stop using FRT Need rules of use	
55	That is a serious problem and that is why you have to—for me, here again, these companies that develop this technology they too have to be held responsible and those police departments that acquired that technology from these companies have to be held accountable as well, too. (p. 54)	Supplier Responsibility	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
56	ACLU needs to be at that table, and other legal persons as well, too, so that if we are going to utilize this technology in public safety, in law enforcement, I think one thing needs to be made clear to these software manufacturers is that if you are going to develop this technology it is going to have to meet a standard that you hear being articulated at these—at this table by the scientists and those in the legal communities that are here. It needs to meet that standard. If it can't meet that standard, then there is no place for it in our society. Police need to be at the table so they can clearly understand if you decide—your jurisdiction decide to pay for and acquire this technology, you are going to be held to a standard as well, too. (pp. 32-33)	Who should be at the table?	Leadership unknown
57	Because this is a huge—this is a huge, very complicated convoluted piece of technology that may have some benefits that you have just heard but they also have a significant amount of challenges attached to them. We are going to—getting to a point where, you know, virtually everybody is in a face recognition data base, which gives the government enormous power. And so, I think we need to think about those concerns before moving forward with this technology. (p. 42)	Challenges	
58	I do expect that we are going to be able to get some legislation out on this. I talked to the ranking member. There is a lot of agreement. The question is do you have an all-out moratorium and at the same time try to see how this process can be perfected. But clearly, you are absolutely right. There is a lot of agreement here, …. (p. 44)	Agreement among members. Stop and perfect the process	
59	And I believe that—after reading this that our focus today just on facial recognition and just on law enforcement's use of this information and just, you know, public surveillance is far too narrow. (p. 46)	Surveillance focus too narrow	
60	So, we are also talking about voice recognition. We are talking about gait analysis—anything that is remote sensing. Do we need to be talking beyond facial analysis technologies? Absolutely as well, so let us look at self-driving cars. There is a study that came out of Georgia Tech showing that for pedestrian tracking self-driving cars were less accurate for darker skinned individuals than lighter-skinned individuals. So, when we are talking about this realm of human-centric computer vision, it is not just face recognition that should be concerning. (p. 47)	What other AI should be included?	
61	If this type of technology is not utilized in an ethical moral constitutional type of way, it continues to do exactly what it did to you out there, Congressman, and other people. It separates the community from its public safety. There is a lack of trust. There is a lack of legitimacy. There is this whole fear of you being a watchdog over me in a warrior sense as opposed to be a guardian of their community. (p. 54)	Ethical issues Fear	
62	Well, you know, a lot of this is still—in many ways, it is very early stages. But I still think it goes back to the entire privacy issues. (p.56)	Privacy issues	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
63	So, I really think, Mr. Chairman, and I am so encouraged by what I have heard in a bipartisan way today that we need to stop—that it has gone down too far. We are not starting at a metric where we are just beginning the deployment of this. It has already been deployed. And to Mr. Lynch's comments, it is being deployed not just for facial recognition but for everything we do. And there are benefits for that and we can see that, but we need a time out societally, as Europe has led us on, to say no. (p. 48)	Stop using FRT	
64	There is no court of appeals that has directly addressed the constitutionality of, let us say, real-time face recognition or matching against a driver's license data base. And I think that one of the big reasons for that is for defendants to raise that challenge they have to be notified, and people aren't being notified. (p. 55). I think that that is insulating this technology from the judicial review that is very sorely needed. … obviously, other bodies of case law—the Carpenter decision and others—which are relevant and could apply to uses of face recognition. But what we need is notice so that these cases can come before the court. Without that, it becomes very difficult to have developed case law. (p. 55)	Court cases are relevant to FRT	Constitutionality of FRT
65	So, in the case of Amazon, they were pushing some of the most concerning uses—face recognition, body-worn cameras, right—opening up the possibility of a near-surveillance state. And so, I think that there—they are not passive actors in the system, and they should be forced to take responsibility, and that responsibility should include questions about how accurate their technology is, are they disclosing the problems and the real risks, and are they saying no when they should say no. (p. 49)	Suppliers' responsibility	
66	The question becomes and the current concern now is that this has been very much unregulated without any oversight whatsoever and in light of the fact that we are looking at a piece of technology that is very questionable and is raising concern as we continue here this afternoon in this hearing. So, I think that that is part of what has to be assessed and further questions that have to be asked from both the Federal, state, and local level in the sharing of this information that is very sensitive and very questionable when it comes around to our constitutional liberties. (p. 51)	Need facts	
67	I mean, when it comes to FBI use, we should be concerned. I mean, these are systems that have been in place for years, and as your question rightfully pointed out, the FBI is not even acknowledging a responsibility to fully test the accuracy of systems that it is using and relying on. (p. 51)	FBI will not test systems	FBI noncompliant
68	So does all the panel agree that the Federal Government needs to set the floor before states and localities create their own rules and regulations with respect to this? Is that a consensus among everyone on the panel? Yes or no. (p. 28)	Who should enact FRT legislation	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
69	We have to resolve the fundamental questions and problems. How are we going to prevent this technology from having a disparate impact either because of accuracy or because of existing biases in the criminal justice system? How are we going to prevent the buildup of a surveillance state, right, where there is a camera on every street corner and people don't feel like they can walk around anonymously? How are we going to safeguard our First Amendment liberties and make sure that no one says to themselves, I can't go to this protest because I am afraid my face is going to be scanned? I think before—we can't move forward with this technology until we can answer and resolve those fundamental questions. (p. 57)	Need facts Fear	Unanswered questions

Table A2

Part I: How the Public Is Affected

Pathway To Answering the Research Question: Dimensions Of Purpose Record			
FACIAL RECOGNITION TECHNOLOGY: PART I ITS IMPACT ON OUR CIVIL RIGHTS AND LIBERTIES Hearing Transcript			
How the Public is Affected			
	Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**
1	Both the conservatives and liberals alike have real questions about when they are being monitored, why they are being monitored, who is monitoring them, and what happens to this information after it is collected. (p. 1)		Informed consent
2	At the local levels, cities like Detroit and Chicago are rapidly expanding the use of facial recognition technology to track its citizens in real time. (pp. 1-2)	Tracking citizens	Unwarranted surveillance; privacy protection
3	More than half of American adults are part of facial recognition databases, and they may not even know it. (p. 2)	Public does not know about inclusion in a database	Informed consent
4	We also heard testimony that facial recognition technology misidentifies women and minorities at a much higher rate than white males, increasing the risk of racial and gender bias. (p. 2)	Misidentification of women and people of color	Racial and gender bias
5	Later we learned that the police used facial recognition technology to find and arrest protestors. It is likely that I and other members of our community who were simply exercising our rights under the Constitution were scanned, identified, and monitored by using this technology. (p. 2)	Not free to protest without FRT monitoring	First Amendment right violation
6	In all of these cases the government can monitor you without your knowledge and enter your face into a data base that could be used in virtually unrestricted ways. (p. 2)	Public does not know they are monitored and placed in a database	Informed consent Control of image Privacy protection
7	The potential for mischief … is scary. (p. 3)	Possible abuse and misuse of FRT	Data security
8	There are many ways for this technology to fail. Among the most pressing are misidentifications that can lead to false arrest and accusations. Mistaken identity is more than an inconvenience and can lead to grave consequences. (p. 4)	Misidentification can lead to problems for the individual	Data inaccuracies
9	The technology repeatedly fails on the most, namely, people with nonwhite skin, women, and youth. (p. 4)	Equipment failure on people of color/women	Racial and gender bias
10	Tenants in Brooklyn are protesting the installation of an unnecessary face recognition entry system. New research is showing bias in the use of facial analysis technology for health care purposes and facial recognition is being sold to schools, subjecting children to face surveillance. (p. 5)	FRT used in health facilities, schools, and housing areas	Unwarranted surveillance Privacy protection
11	Unregulated facial recognition technology…is too powerful, too chilling, too under mining to principles of privacy, liberty, and security. (p. 7)	Unregulated FRT is contrary to privacy, liberty, and security principles	Privacy protection Standards or regulations

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
12	Face recognition presents unique threats to our civil rights and Liberties. (p. 7)	Threats to liberties	FRT harmful
13	First, face recognition gives law enforcement a power that they have never had before, and this power raises questions about our Fourth and First Amendment protections. (p. 7)	FRT powerful tool for law enforcement	Misuse can threaten protections
14	Police can't secretly fingerprint a crowd of people from across the street. They also can't walk through that crowd demanding that everybody produce their driver's license. But they can scan their faces remotely and in secret and identify each person thanks to face recognition technology. (p. 8)	FRT beneficial to laws enforcement	Secrecy
15	Second, face recognition makes mistakes, and its consequences will be borne disproportionately by African Americans. One, communities of color are disproportionately the targets of police surveillance, face recognition being no exception. (p. 8) Two, people of color are disproportionately enrolled in police face recognition systems, thanks to being over represented in mug shot data bases that the system is run on. (p. 8)	Mistakes in FRT unfair and unequal	Consequences
16	And three, studies continue to show that the accuracy of Face Recognition varies depending on the race of the person being searched. Face recognition makes mistakes and risks making more mistakes, more misidentifications of African Americans. A mistake could mean you are accused of a crime you didn't commit. (p. 8)	Mistakes in FRT unfair and unequal	FRT accuracy is questionable
17	Third, left unchecked, current police face recognition practices threaten our due process rights. My research has uncovered the fact that police submit what can only be described as garbage data into face recognition systems, expecting valuable leads in return. (p. 8)	FRT garbage in, garbage out	Threats to due process
18	The U.S. has over 50 million surveillance cameras. This, combined with face recognition, threatens to create a near constant surveillance state. Even more, right now police are often exploiting large-scale databases like driver's license repositories for face matching. This impacts the rights of everyone in these data bases, and we don't have the option of simply leaving our face at home to avoid being surveilled. (p. 9)	Cameras are everywhere; can't leave our faces at home	Surveillance impacts the rights of everyone
19	Three, this technology is not being used consistent with the Constitution. Face recognition is potentially even more invasive than the warrantless tracking that the Supreme Court found unconstitutional in the Carpenter case. Yet, it is being used without a warrant and without other protections. (p. 10)	FRT is used without a warrant	FRT is invasive
20	To be clear, police officers may have used facial recognition technology on citizens' personal photos from social media to identify and arrest them while they were exercising their First Amendment right to assemble. (p. 54)	Social media photos used by law enforcement for arrest	First Amendment violation
21	But we got to be very aware that we are not stumbling into the future blind and at that same time giving up some liberties and protections that we have all cherished not only for decades but for Generations. (p. 58)	Cannot stumble into the future	Need to know

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
22	On May 16, the Washington Post report that some agencies use altered photos, forensic artist sketches, and even celebrity look alikes for fake facial recognition searches. Using artificial intelligence to confer on a highly subjective visual impression a halo of digital certainty is neither fact-based nor just. But it is not illegal, for the simple reason that no Federal laws govern the use of facial recognition. At this point, law enforcement use of facial recognition is not only unregulated by law, but it also operates even without any consensus on best practices. Artificial intelligence systems do not invent results from thin air. They operate from data bases of identified faces in an attempt—an attempt to match one of those identified faces with the face of a suspect or subject of interest. (p. 11)	FRT is unregulated and without consensus	
23	An artificial intelligence system is only as good as its data bases. Yet, there is currently no standard governing the content of any agency's facial images data base. (p. 11)	Data bases lack standards	No standards
24	Until there is sufficient scientific evidence that shows these technologies have reached maturity, because with what we know with human-centric computer vision systems, as they are based on statistical methods, there is no way the technology will be 100 percent flawless and there are tradeoffs that need to be made. Yet the academic research just doesn't yet exist to say this is what it looks like for it to meet meaningful thresholds. (p. 17)	FRT not flawless	More research needed
25	Imagine you are arrested or convicted, or you are pulled over by police and you are—they say, we identified you as this person, you don't even have the information to say, look, you are wrong—the algorithm got it wrong, and that is really the nightmare scenario…are worried about and why we think that, you know, the prudent thing to do would be to hit the pause button. (p. 22)	Algorithms are dangerous to public	Algorithm flaws
26	Yes. I mean, certainly it could be exculpatory evidence to know, for example, that an algorithm has a reliability problem or that an algorithm returned, you know, similar photos with—indicating they can be the person. That could support a defense to say, look, I have been misidentified—there were other people who were similarly tagged by the system. (p. 24)	Tagged by the system incorrectly	Algorithm flaws
27	I think there is nothing more American than the freedom of expression and the freedom of association, and I think what we have seen is that this kind of technology can chill both of those—the ability to go out and protest in Baltimore or anywhere else, the ability to support an incumbent—you know, a political candidate who wants to go against—I mean, an upstart political candidate who wants to go against the incumbent. It is going to chill speech. It is going to chill association, and we are not going to be able to act in ways that we used to be able to act with anonymity. (p. 28)	FRT threat to free speech	The chilling effect

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
28	But one of the biggest things I find, Chairman, from my experience is that when new technology is developed and we take that technology and we introduce it into our communities across the country, we never tell our communities what it is, why it is being utilized, and how it would help benefit public safety. (p. 56) So, what ends up happening is people draw their own conclusions around it, already sometimes in suspicion of the work that police are doing because oftentimes they operate in a very clandestine type of sense. (p. 56)	Suspicious of law enforcement	They work in secrecy
29	You have new research coming out from the University of Toronto that shows even for health care-based systems of facial analysis technology you are starting to see biases. So, you get a bias when it comes to accuracy when you are looking at age or somebody has dementia versus not. So, I am hopeful that research can continue to explore potential uses. But until we have shown that it actually meets the promise, it should not be used. (p. 31)	FRT for health care usage biased	Biased results for health care
30	And right now, companies, governments, agencies can steal or use your biometric data from you without your consent and this is outrageous, right, because this is America, and we have a right to privacy. (p. 35)	Biometric data stolen	No informed consent
31	So, we have the pale male data sets being used as something that is universal when that isn't actually the case when it comes to representing the full sepia of humanity. (p. 37)	Narrow data set for testing	Demographic information inadequate for testing
32	And then if you have a case where we are thinking of putting let us say facial recognition technology on police body cams in a situation where you already have racial bias that can be used to confirm, right, the presumption of guilt even if that hasn't necessarily been proven because you have these algorithms that we already have sufficient information showing fail more on communities of color. (p. 37)	FRT on policy body cams biased	Algorithms flawed
33	Back in 2011 when the technology was really getting moving, a face recognition working group including the FBI said—and they said exactly that face recognition could be used as a form of social control, causing people to alter their behavior in public, leading to self-censorship and inhibition. So, this is something police departments themselves have recognized. (p. 39)	FRT used for social control	The chilling effect
34	I mean, one, because you are violating somebody's civil liberties in the most fundamental way, and two, you are leaving the real criminal suspect or the real criminal out there at large because you have chosen the wrong person. (p. 53)	May choose the wrong person with FRT	Violation of civil liberties
35	The Washington County Sheriff's Office gave an example where a person—a person with a 70 percent confidence was the person they ended up charging, even though the algorithm thought somebody else was at a 90 percent confidence (p. 24). The algorithm was playing witness, saying that I am 90 percent confident it is this other guy, and yet the person who I am 70 percent confident is the guy was the one who was charged. (p. 24)	Tagged by the system incorrectly	Algorithm flaws

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
36	The Supreme Court recognized recently that a person does not surrender all Fourth Amendment protection by venturing into the public sphere. Face recognition surveillance threatens to shatter the expectation Americans have that the government cannot monitor and track our movements without individualized suspicion and a warrant. (p. 41)	Going into public space does not render the Fourth Amendment void	Expectation of privacy
37	The witnesses have described a technology of potential totalitarian surveillance and social control. (p. 51)	Totalitarian threat	Social control
38	But companies have been pushing this technology on police departments, despite knowing that it works only 30 percent of the time. This puts many people, including women and people of color and young people, at grave risk of harm and underscores the need for congressional oversight. (p. 39)	Companies pushing technology on police departments	People are at risk of harm

Appendix B: Hearing Transcript Part II

Figure B1

Hearing Transcript Part II: Facial Recognition Technology – Ensuring Transparency in Government Use

FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE

HEARING

BEFORE THE

COMMITTEE ON

OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JUNE 4, 2019

Serial No. 116–031

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
http://www.oversight.house.gov
http://www.docs.house.gov

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
KATIE HILL, California
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

JIM JORDAN, Ohio, Ranking Minority Member
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
JAMES COMER, Kentucky
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
RALPH NORMAN, South Carolina
CLAY HIGGINS, Louisiana
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida

DAVID RAPALLO, *Staff Director*
YVETTE BADU-NIMAKO, *Legislative Director/Counsel*
GINA KIM, *Counsel*
LAURA RUSH, *Deputy Clerk*
CHRISTOPHER HIXON, *Minority Staff Director*
CONTACT NUMBER: 202-225-5051

C O N T E N T S

Page

Hearing held on June 4, 2019 1

WITNESSES

Ms. Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services, Federal Bureau of Investigation
Oral Statement 3
Dr. Gretta L. Goodwin, Director, Justice and Law Enforcement Issues, Homeland Security and Justice Team, U.S. Government Accountability Office
Oral Statement 5
Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology
Oral Statement 6
Mr. Austin Gould, Assistant Administrator, Requirements and Capabilities Analysis, Transportation Security Administration
Oral Statement 8

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: https://docs.house.gov.

INDEX OF DOCUMENTS

The documents entered into the record during this hearing are listed below, and are available at: https://docs.house.gov.

* Document from the Association for Cybersecurity Providers, submitted by Mr. Higgins.
* Letter to Chairman Cummings from the Consumer Technology Association, submitted by Mr. Jordan.
* Forbes Article by Thomas Brewster, ″We Broke Into a Bunch of Android Phones With a 3-D Printed Head,″ submitted by Mr. Massie.
* Article by Joseph Cox of Vice News, ″SocioSpyder: The Tool Bought by the FBI to Monitor Social Media,″ submitted by Mr. Hice.
* Archived copy of SocioSpyder web domain, submitted by Mr. Hice.
* Purchase of Order logs of FBI and agreement purchased by Allied Associates, International, submitted by Mr. Hice.
* Article, ″Face Recognition Performance: Role of Demographic Information″ dated 12-6-2012, submitted by Mr. Cummings.
* Face Off - White Paper by the Electronic Frontier Foundation, submitted by Mr. Cummings.
* GAO Priority Open Recommendations, letter to Attorney General Barr, submitted by Mr. Cummings.
* Coalition letter calling for a Federal moratorium on face recognition, submitted by Mr. Cummings.
* Three NIST reports on facial recognition, submitted by Mr. Cummings.
* Questions for the Record addressed to Ms. Del Greco, Mr. Gould, and Dr. Romine.
* Rep. Connolly’s Unanimous Consent Statement for the Record.

Table B1

Part II: Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces

Pathway to Answering the Research Question: Dimensions of Purpose Record			
FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE Hearing Transcript			
Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces			
	Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**
1	I appreciate the Chairman's willingness to have a second hearing and willingness to work together in a bipartisan fashion to figure out what we can do to safeguard American citizens' First Amendment and Fourth Amendment and due process rights as we go forward. (p. 3)	Agreement Protection	
2	The FBI's use of facial recognition for law enforcement purposes. It is crucial that authorized members of law enforcement and national security communities have access to today's biometric technologies to investigate, identify, apprehend, and prosecute terrorists and criminals. The FBI's Next-Generation Identification, or NGI system, which includes facial recognition, aids in our ability to solve crimes across the country. Facial recognition is an investigative tool that can greatly enhance law enforcement capabilities and protect public safety. (p. 4)	Valuable Technology Recognition	
3	Over the past few decades, this technology has advanced rather quickly, and it now has wide-ranging usage, from accessing a smart phone to social media, and to helping law enforcement in criminal investigations. However, questions exist regarding the accuracy of the technology, the transparency in its usage, and the protection of privacy and civil liberties when that technology is used to identify people based on certain characteristics. Today I will discuss the extent to which the FBI has assured adherence to laws and policies related to privacy and transparency regarding its use of face recognition technology, as well as whether the FBI has ensured its face recognition capabilities are sufficiently accurate. (p. 5)	FBI's role	
4	We also reported on accuracy concerns about FBI's face recognition capabilities. Specifically, we found that the FBI conducted limited assessments of the accuracy of the face recognition searches before they accepted and deployed the technology. For example, the face recognition system generates a list of the requested number of photos. The FBI only assessed accuracy when users requested a list of 50 possible matches. It did not test smaller list sizes, which might have yielded different results. Additionally, these tests did not specify how often incorrect matches were returned. Knowing all of this, the FBI still deployed the technology. (pp. 5-6)	FBI limited assessment of FRT	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
5	The FBI often uses face recognition systems operated by 21 state and two Federal external partners to enhance its criminal investigations. We reported that the FBI had not assessed the accuracy of these external systems. As a result, they cannot know how accurate these systems are, yet the FBI keeps using them. Moreover, we found that the FBI did not conduct regular reviews to determine whether the searches were meeting users' needs. We made recommendations to address all of these accuracy concerns. DOJ has yet to implement these regs. As you are aware, in April of this year we issued our annual Priority Recommendations Report which provided an overall status of DOJ's open recommendations and outlined those that GAO believes should be given high priority. This report included six recommendations related to face recognition. As of today, five of those six remain open. (p. 6)	FBI noncompliant	
6	Chairman CUMMINGS. Well, you just said state authority allows you to do this. One question that our Ranking Member has been asking over and over again is do you know whether in these states, do any elected officials have anything to do with these decisions? In other words, where is that authority coming from? We are trying to figure out, with something affecting so many citizens, whether elected officials have anything to do with it. Do you know? (p. 10)	Authority source for use of searchable database unknown	
7	Recognizing the need to positively identify passengers in an era where fraudulent means of identification are becoming more sophisticated and prevalent, TSA has consistently sought new processes and technologies to improve performance while protecting passengers' privacy. To that end, TSA's 2018 Biometrics Roadmap identifies the steps that the agency is taking to test and potentially expand biometric identification capability at TSA checkpoints, which we believe can both enhance security and improve passenger experience. (p. 8)	TSA's role	
8	The Roadmap has four major goals: partner with Customs and Border Protection on biometrics for international travelers; operationalize biometrics for TSA pre-check passengers; potentially expand biometrics for additional domestic travelers; and develop the infrastructure to support these biometric efforts. Consistent with the Biometrics Roadmap, TSA has conducted pilots that use facial biometrics to verify identity at certain airports. The pilots to date have been executed in conjunction with Customs and Border Protection. Each pilot has been supported by a privacy impact assessment, and passengers always have the opportunity to not participate. In these cases, standard manual identification process is used. (p. 8)	TSA expansion use of FRT	
9	I very much appreciate everyone's testimony today. This is an emerging technology. Mr. Chairman, Mr. Ranking Member, we should watch this technology closely and protect the rights of American citizens. We should also recognize this can be a very valuable tool for law enforcement and to fight crime in our country, …. (p. 31)	Conflicting tasks – protect citizens and recognize value of FRT to law enforcement	Dual Responsibility

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
10	Chairman CUMMINGS. Well, do individuals who consent to having their faces in the non-criminal data bases also consent to having their faces searched by the FBI for criminal investigations? For example, when applying for a driver's license, does someone consent at the DMV to being in a data base searchable by the FBI? Ms. DEL GRECO. The FBI worked diligently with the state representatives in each of the states that we have MOUs. We did so under the state's authority to allow photos to be used for criminal investigations. We also abided by the Federal Driver's License Privacy Protection Act, and we consider that a very important process for us to access those photos to assist the state and local law enforcement and our federal agencies. (p. 10)	No Consent to be in FBI searchable databases	
11	I think you have to understand the framework. I mean, you talked about strict standards in place. There were strict standards in place, at least people from our side of the aisle view it this way, strict standards in place on how people go to the FISA court and get information and put information in front of the FISA court. The Attorney General of the United States has tapped U.S. Attorney John Durham to look at potential spying done by the FBI of one Presidential campaign. So this is the context and the framework that many on our side see this happening, and it is happening when GAO—not Jim Jordan, not Republicans—GAO—Dr. Goodwin said that when you guys started this, started using this, you didn't follow the E-Government law, you didn't do privacy impact assessments like you are supposed to, you didn't provide timely notice, didn't conduct proper testing, and didn't check the accuracy of the state systems that you were going to interact with. (pp. 51-52)	FBI noncompliant	
12	These are technologies that exist that we all have. Everyone here wants to protect Fourth Amendment rights and privacy rights of American citizens. None of us want our constitutional protections violated. But the fact is this emerging technology of facial recognition is coming, and it is reflecting just the advancement of our digital technologies that we have already employed across the country and deployed in public areas, including airports. (p. 15)	FRT technology already here Too late	Proliferation of FRT
13	To me it is extremely important that we know whether the use of this technology leads to any benefits for society, especially in determining whether there is a crime that this is helping to solve, or are we just weighing in on constitutional rights of people and creating constitutional risk? We cannot know this unless there is a sufficient data base for law enforcement that uses this. So, my question is what are the current reporting requirements regarding the FBI's use of facial recognition technology? Is there any oversight reporting requirements on the use of this technology? (p. 21)	FBI Reporting requirements and oversight Not present	
14	Do you have a data base that tracks whether or not this is actually working, is it helping law enforcement arrest people, is it arresting innocent people, is it keeping information on innocent people? Do you have a data base that tells us what this program is doing and what the benefits or penalties are to our society? (p. 22)	FBI Assessment of FRT usage benefits and penalties not present	
15	Ms. TLAIB. Thank you, Mr. Chairman. I have to tell you—and through the Chairman, I hope this is okay—this stuff freaks me out. I am a little freaked out by facial recognition, Mr. Chairman. I hope that is okay, I can say that. Chairman CUMMINGS. Yes, that is okay. (p. 46)	Scared	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
16	And, Dr. Romine, what would be the most effective way for TSA to measure how accurate its facial recognition systems are when testing the identity of American citizens? Mr. ROMINE. We are not expert in testing full systems. We test algorithms. We evaluate those algorithms for accuracy of matching. The entire system is something that is a little bit outside my purview. (p. 29)	NIST Test Algorithms Not systems	
17	Ms. HILL. Okay. I personally understand Mr. ROMINE. We are not experts in testing full systems. We test algorithms. We evaluate those algorithms for accuracy of matching. The entire system is something a little bit outside my purview. Ms. HILL. Okay. I personally understand the value of this technology, but I think we really need to have some clear regulations and guidance that are essential to prevent the abuse of data collected and to protect our privacy. While I appreciate the GAO's recommendations, I think we are going to need some more teeth to ensure that those are implemented. (p. 29)	Regulations and guidance needed	
18	In the history of this country, we have always had this debate and this goal of trying to balance security with liberty. But in the era of facial recognition, I feel we are stumbling into the future without really understanding how much liberty we are giving up for how much security. And it is really with that understanding we have to set up guidelines that dictate the use of this technology. So that is where my approach comes from. (p. 42)	Conflicting tasks-balance security with liberty	
19	With the government's use of facial recognition increasing, it is important this nascent technology is not rushed to market and all communities are treated equally and fairly. (p. 35)	Do rush to market. Equal and fair treatment	
20	The objective [of the NIST] is to ensure complete transparency with regard to the performance of the algorithms we evaluate to see if we can use rigorous statistical analysis to demonstrate the presence or absence of demographic effects. That statistical analysis has not been completed yet. We have preliminary data suggesting demographic effects such as difference in age, sex, and race can affect or can have differences in terms of the performance of the algorithms. However, the increased performance across the board for the best-performing algorithms is, we expect, diminishing that effect overall. (p. 35)	Algorithm effects on demographic differences	
21	So here is what I would recommend, Mr. Gould, is this. I am all about making sure that we have screening, but I can promise you I have gone through screening more than most Americans, and there are inefficiencies in TSA that have nothing to do with facial recognition. And until you get that right, I would suggest that you put this pilot program on hold, because I don't know of any appropriations that specifically allowed you to have this pilot program. Are you aware of any? Because you keep referring back to a 2001 law, and I am not aware of any appropriations that have given you the right to do this pilot program. (p. 38)	Authority for TSA pilot program unknown	
22	Chairman CUMMINGS. I too want to thank the witnesses for being here for almost three hours. We really do appreciate your testimony. Of all the issues that we have been dealing with, this will receive the most intense scrutiny of them all. The Ranking Member referred to the fact that we are bringing you all back, but we also have two subcommittees that are also looking into this because we want to get it right. It is just that important, and so I thank you. (p. 52)	More meetings needed Very important Subject	Need info

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
23	So, Mr. Meadows, in the spirit of efficiency and effectiveness, I think has made a very reasonable request that Ms. Del Greco [FBI] and Dr. Goodwin [GAO] get together so that we can get some of these items resolved. So, I am going to call you all back in about two months. I will figure it out. Because I am worried that this is going to go on and on, and in the meantime, I am sure that we will be able to come up with some bipartisan solutions. But the American citizens are, I think, being placed in jeopardy as a result of a system that is not ready for prime time. (p. 39)	Government agencies need to work together Bipartisan solution needed Americans in jeopardy FRT not ready for prime time	Need Improvements
24	Mrs. LAWRENCE. To ''carry out,'' that is the word that you are saying. As this is evolving and we are looking at the challenges, do you have enough funding for the R&D and for the checks and balances for you to be the standard bearer of the facial recognition industry? Nothing frustrates me more than for you to come before Congress and say I have everything I need, and then when you don't do the job, ''Well, we didn't have the funding.'' So, I am asking this question, and I need you to be very honest with me. (p. 40)	Challenges Don't blame Funding if not requested Standard bearer needed	
25	Accuracy and transparency are key and vital to when we are talking about this technology, as well as just making certain we are protecting privacy rights. (p. 42)	Accuracy Transparency Privacy Protection	
26	Mrs. MILLER. Okay. And, Dr. Goodwin, to your knowledge, has the FBI been adhering to these regulations? Ms. GOODWIN. We are working very closely with the FBI. If I could go back to something Ms. Del Greco said earlier, the testing they are currently doing, the new information they are providing, until we see that, we won't be closing our recommendations. We need to make certain they are meeting the recommendations as we have put forward to them. (p. 42)	FBI unresponsive to GAO	
27	Mr. GOMEZ. That is not what I am asking. I am asking when you run the program, is it set to a high level that it needs to be accurate, to a 95 percent confidence level that the computer recognizes this individual is 95 percent likely to be this person, or is it 80 percent? Like Amazon sells their program at 80 percent default. What do you guys run your program at? Ms. DEL GRECO. Because we don't conduct an identification match, we don't look at that, sir. We have an accuracy rate we rely on, and we are currently implementing the new NIST Vendor Recognition Test results at 99.12 percent at a Rank 1, and it is 99.72 at a Rank 50. Those are the new—that is the new algorithm. But because it is not a true identification, we don't print that. (pp. 42-43)	Level of testing for algorithm accuracy not performed by NIST	
28	The recommendations that we made, those three recommendations that we made related to accuracy, we feel like this would go a long way to helping DOJ better ensure that the data that they are collecting, the way they are using the information, that that is accurate. As of yet, as you have heard, DOJ has yet to close those recommendations, and we will work very closely with them to get those closed because the issues around privacy and accuracy are very important, and they are vitally important when you are talking about using this technology. (p. 48)	Privacy and accuracy important	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
29	So that is the backdrop, that is the framework. So, when Republicans talk about, we are concerned and working with Democrats—and I really do appreciate the Chairman's focus on two hearings, and now a third hearing, and looking at legislation that we may attempt to pass here. This is the framework. So, I hope you will tell the folks back at the FBI, we appreciate the great work that FBI agents do every single day protecting our country and stopping bad things from happening and finding bad people who did bad things, but the framework and the context is very serious, and that is why we come at it with the intensity that I think you have seen both two weeks ago in that hearing and in today's hearing. So again, Mr. Chairman, thank you for your leadership on this. (p. 52)	This is the framework Republicans and Democrats concerned Tell FBI this is serious	FBI negligent
30	Mr. GOMEZ. Okay. The FBI publishes that it trains third parties in a manner consistent with the guideline and recommendations outlined by the Facial Identification Scientific Working Group. The Facial Identification Scientific Working Group does not endorse a standard certified body of facial comparison. To compare, the ten-print certification exists for personnel that analyze fingerprints. These programs require hours of training before a person can be certified. Since there is no formal certification process that the Working Group endorses, what standards does the FBI require of personnel that conduct facial analysis? (p. 43)	What Standards are required by FBI for users	Transparency FBI Responsibilities
31	Much of my line of questioning has already been asked, but I do just want to pick up on a couple of things in the space of consent because I wanted to just get some accuracy questions and just better understand for the purposes of the record here. Mr. Gould, do you keep data on how many people opt out of use for the facial recognition technology? Mr. GOULD. Ma'am, I am not aware we are actually collecting data on people who choose not to participate. I don't think we are collecting it. No, ma'am. Ms. PRESSLEY. Okay. You have no idea how many people have opted out of previous TSA facial recognition pilot programs? Mr. GOULD. No, ma'am. Ms. PRESSLEY. Okay. Do you know how many passengers were notified of TSA's use of facial recognition technology? (pp.44-45)	Data on opt out and TSA notification to passengers that FRT in use	Informed consent
32	And if I could just kind of circle back to Congresswoman Pressley's comment about consent, there is the Senate bill that will look at consent, but it only looks at consent from the standpoint of commercial usage, not Federal usage. So, we have those ongoing jobs. And then GAO does have a request in to look at face recognition technology across the rest of law enforcement. (p. 45)	Consent for FRT Federal usage not present GAO request to expand	
33	The American people deserve government accountability, and I actually agree with the questioning of the minority party leadership on this, that you don't have answers on how it is working, how it was set up, what is coming out of it, whether it is hurting people, helping people. You don't even have information on whether it is aiding law enforcement in their goal for hunting down terrorists. So, we need more accountability…. (p. 22)	Government accountability not evident	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
34	Mr. GOULD. Ma'am, the notification at the airport consists of signage and also verbal instructions from the officers. So, if … a lane where facial recognition technology is being piloted, I would say that 100 percent of the people are being made aware it is being used. And they … assume a suitable pose to actually have the camera capture their image. Ms. PRESSLEY. So again, if this is based on signage, which in many ways can be arbitrary, how are folks even aware of the option to opt out, other than signage? And then ... opt out? Mr. GOULD. It is signage. It is announced. ''If you would like to have your picture taken for your identification, please stand right here. Otherwise, let us see your credential, your hand-carried identification.'' Ms. PRESSLEY. Okay. And is that communicated in multiple languages? Mr. GOULD. For the purposes of the pilot, ma'am, it has not been communicated in multiple languages. (pp. 44-45)	Data on opt out and TSA notification to passengers that FRT in use	Informed consent
35	Mr. ROMINE. Sure. The data that we obtain is from multiple sources. The largest amount of data that we get—first I need to make a distinction between data that we are releasing as part of the ability for vendors to determine whether they are able to submit their algorithms to our system, to our evaluation process. So, we provide them with data for that. The rest of our data, the vast majority of it, is sequestered. It is not made public. It is solely for the purposes of evaluation. Most of that data is FBI image data that we sequester and protect from release. There is some other image data related to Creative Commons, to images that we have received with full institutional review that involves permissions, and then also deceased datasets. In all cases, if you look at the full suite of data, it is true that it is not representative of the population as a whole. However, we have a large enough dataset that our evaluation capabilities can be statistically analyzed to determine demographic effects of race, age, or sex. And we are in the process of doing that now and will release that report in the fall. Mr. SARBANES. So, I gather that since the last hearing you have been testing for differential error rates on the facial recognition systems between races and genders. Can you talk a little bit more about the error rates of the algorithms that you tested between different races and genders? Mr. ROMINE. Sure. I can say a little of preliminary information, but I want to stress that the full statistical analysis, the rigorous analysis, is not completed yet. The report will be released in the fall that outlines the full conclusions that we have with regard to effects, demographic effects, broadly speaking. We can say that there are still remaining differences even with the extraordinary advances in the algorithms over the last five years. There are still differences remaining that we can detect. We don't yet know whether those differences—whether it is with regard to race, sex, or age—are significant. We don't know yet until we have completed that analysis. (pp. 50-51)	Algorithm testing not set for demographic effects NIST has preliminary information Don't know yet	Accuracy issues

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
36	There are at least two levels of analysis that are of concern here today. One is the threshold question of whether we like or don't like this technology given the general threat that it can pose to civil liberties. The second theme is whether recognizing that the technology is barreling ahead anyhow and is being adopted and applied increasingly across many different platforms, let's say, and uses, whether it is being developed in a way that ensures that when it is used, it is not being used in a discriminatory fashion, it is not being applied unfairly, et cetera. And that depends on the algorithms being developed in a way that is respectful of accurate data, and we are not there yet, as I understand it. So, it just increases the anxiety level. So, we are going to be paying a lot of attention. I am glad the Chairman is going to have you all come back, because I think he is right that this is a moving target here. We are going to be paying a lot of attention to how the data gets digested and how the algorithms that flow from that data are being applied, whether they are accurate and so forth. So, we appreciate your testimony, but obviously this is not the end of the inquiry. (p. 51)	FRT is a moving target Conflicting tasks – expand FRT and ensure algorithm accuracy	
37	The Department of Commerce's National Institute of Standards and Technology… NIST's role in standards and testing for facial recognition technologies. In the area of biometrics, NIST has been working with the public and private sectors since the 1960's. NIST's work improves the accuracy, quality, usability, interoperability, and consistency of identity management systems and ensures that United States interests are represented in the international arena. (pp. 6-7)	NIST's role	

Table B2

Part II: How the Public Is Affected

Pathway To Answering the Research Question: Dimensions Of Purpose Record			
FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE			
How the Public is Affected			
	Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**
1	The stark conclusion after our last hearing was that this technology is evolving extremely rapidly without any real safeguards. Whether we are talking about commercial use or government use, there are real concerns about the risks that this technology poses to our civil rights and liberties and our right to privacy. (p. 1)	FRT evolving rapidly	Threat to civil rights
2	Two weeks ago, we learned some important things. Facial recognition technology, there are all kinds of mistakes made when it is implemented. Those mistakes disproportionately impact African Americans. There are First Amendment and Fourth Amendment concerns when it is used by the FBI and the Federal Government. There are due process concerns when it is used by the FBI and the Federal Government. (p. 2)	FRT makes mistakes	Racial bias
3	We learned that over … 20 states, have given their Bureau of Motor Vehicles the driver's license data base. They have just given access to that to the FBI. No individual signed off on that when they renewed their driver's license or got their driver's license. They didn't sign any waiver saying, oh, it is okay to turn my information, my photo over to the FBI. No elected officials voted to allow that to happen, no state assemblies, no general assemblies, no bills, no Governor signing something, passing a bill saying it is okay for the FBI to have this information. (pp. 2-3)	Sharing of data by FBI	Authority unknown
4	And now we learn that when GAO did their investigation and study in how the FBI implemented this, there were all kinds of mistakes the FBI made in how it was implemented. I think five recommendations that the GAO said you are supposed to follow the FBI didn't follow. (p. 3)	GAO and FBI not working together	FBI noncompliant
5	And all this happens, all this happens in a country with 50 million surveillance cameras. (p. 3)	Surveillance cameras everywhere	
6	However, questions exist regarding the accuracy of the technology, the transparency in its usage, and the protection of privacy and civil liberties when that technology is used to identify people based on certain characteristics. (p. 5)	Accuracy, transparency, and privacy protection concerns	
7	The use of face recognition technology raises potential concerns about both the effectiveness of the technology in aiding law enforcement and the protection of privacy and individual civil liberties. This technology is not going away, and it is only going to grow. So, it will be important that DOJ take steps to ensure the transparency of the systems so that the public is kept informed about how personal information is being used and protected; that the implementation of the technology protects individuals' privacy; and that the technology and systems used are accurate and are being used appropriately. (p. 6)	DOJ should ensure transparency of technology to protect civil liberties	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
8	The Federal Driver's License Privacy Protection Act, it allows the state to disclose personal information, including a photo or an image obtained in connection with a motor vehicle record, to law enforcement to carry out its official function. (p. 11)	Authorizing law to share images	
9	…with all areas, for face recognition, rigorous testing and Standards development can increase productivity and efficiency in government and industry, expand innovation and competition, broaden opportunities for international trade, conserve resources, provide consumer benefit and choice, improve the environment, and promote health and safety. (p. 8)	Benefits of testing and standards	
10	TSA is committed to addressing accuracy, privacy, and cybersecurity concerns associated with biometrics capture and matching. (p. 9)	TSA commitment	
11	…TSA is in the process of a systematic assessment of the applicability of biometric identification at our checkpoints. This identification process will enhance aviation security while also increasing passenger throughput and making air travel a more enjoyable experience. TSA's system will be used for passenger identification and to determine the appropriate level of screening only. It will not be used for law enforcement purposes. And as always, passengers will have the opportunity to not participate. (p. 9)	TSA biometric ID stations offers opt-out to passengers	
12	Ms. KELLY. And then what are you doing to make sure that no categories of people are suffering from lower rates of accuracy? Mr. ROMINE. The best we can do in that is to ensure Transparency and public access to data about the level of the demographic effects. We have no regulatory authority to do anything about that other than to just make the data available for policy makers to make appropriate decisions. (p. 36)	Ensure transparency	No regulatory authority
13	It is true that the algorithms, depending on the way that they have been developed, can have biases associated with them. In many cases the improvement that we see in the performance of these algorithms, the dramatic improvement, comes from a transition that the vendor community and participant community have made to deep-learning algorithms, these machine-learning algorithms that are what has made the difference…. And the training of those algorithms determines the level of bias that may exist within the algorithms themselves. (p. 13)	Algorithms can be biased. Training of algorithms determine level of bias	Training for developer of algorithms needed to combat bias
14	So now you are saying that you are going to do these pilot programs and you are just going to herd people—now, you are saying voluntarily, but I could imagine, like you have done with pre-check, you can either agree to surrender your right to anonymity and wait in the long line, or you can give up your Fourth Amendment rights and go in the quick line. Is that the dynamic that is going on here? (p. 14)	TSA piloting programs may mean surrender rights	
15	… We had a problem with OPM where we had 20 million individuals, their personal information, Social Security numbers, everything that they submitted on Federal documents to OPM was stolen by, we think, the Chinese. I am just curious and concerned that we don't have a great history here in protecting people's personal information. (p. 14)	OPM has data security issues	Data security
16	We haven't done an analysis of accuracy rates for the transgender community. I am not sure how we would obtain the relevant data that we would use to do that, but I am aware of—I have been made aware of concerns in the transgender community about the potential for problematic use here. (p. 42)	Accuracy rates for transgender community	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
17	Mr. AMASH. Under what statutory authority does TSA use face recognition technology on American citizens? Mr. GOULD. We use the authority of the Aviation Transportation Security Act, which requires us to positively identify passengers who are boarding aircraft and proceeding through the checkpoint. (p. 26) Mr. AMASH. And can you tell me what statutory authority TSA uses for face recognition technology on domestic travelers generally? Mr. GOULD. Sir, I would say it was the same authority, the Aviation Transportation Security Act. Mr. AMASH. And does TSA have any plans for real-time face recognition technology in airports? Mr. GOULD. Sir, if you mean real-time as facial capture and matching at the checkpoint, then yes, that is what we are pursuing. Mr. AMASH. And has TSA considered the privacy implications of real-time face recognition technology? Mr. GOULD. Yes, sir, absolutely. We have done privacy impact assessments associated with this. There is signage at the airports that clearly identifies that we are using facial recognition technology in a pilot manner to identify passengers, and we don't store any photographs on the camera. (pp. 26-27)	TSA authority for FRT unknown	
18	Mr. MEADOWS. No, I understand. I just came back—I came through JFK. I didn't see any of the signs that you are talking about, all right? So, I guess what I am saying is what statutory authority gives you the ability to do that? You keep referring to 2001. I actually am on the Transportation Committee, and I can tell you we never envisioned any of this. I am looking at the very statute myself here. How can you look and suggest that the statute gives you the ability to invade the privacy of American citizens? (p. 27)	TSA FRT usage authority questioned	No transparency
19	The Washington Post further stated that around 25,000 Passengers traveled through Atlanta's airport pilot program terminal each week. According to the article, ''only about two percent of travelers opt out.'' Even assuming that the systems used by TSA are 99 percent accurate, which they are not, the high volume of passenger traffic would still mean that at least hundreds of passengers are inaccurately identified each week. (p. 29)	Many people are misidentified by TSA	Accuracy is a problem
20	The recommendations that we made, those three recommendations that we made related to accuracy, we feel like this would go a long way to helping DOJ better ensure … data that they are collecting, the way they are using the information, that that is accurate. As of yet, as you have heard, DOJ has yet to close those recommendations, and we will work very closely with them to get those closed because the issues around privacy and accuracy are very important, and they are vitally important when you are talking about using this technology. (pp. 47-48)	Recommendations for transparency for large database	
21	Ms. GOODWIN. So, if you think about the face services system and then all of the searchable repositories, that is over 640 million photos, and the FBI really only searches for criminal. They are looking for the criminal photos. They are looking through all of this for their criminal investigations. But across all the repositories, we are talking over 600 million. (pp. 34-35)	FBI database is large but did not comply with GAO	No transparency or consent

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
22	When we had our hearing on May 22 in this committee, there was an MIT researcher, Joy Buolamwini, who was testifying about datasets that NIST uses, … not adequately test for the full range of diversity present in the U.S. population. She said, ''In evaluating benchmark datasets from organizations like NIST, I found some surprising imbalances. One prominent NIST dataset was 75 percent male and 80 percent lighter skinned, what I like to call a 'pale male' dataset." (p. 50)	Data set for testing too narrow	
23	With the government's use of facial recognition increasing, it is important that this nascent technology is not rushed to market and that all communities are treated equally and fairly. (p. 35)	Don't rush to market	Fairness and equally are necessary
24	Mr. ROMINE. The scientific data verifies that facial recognition accuracy is highly dependent on image quality and on the presence of injuries. Both of those things can affect the ability to have accurate— Ms. TLAIB. So, is there any viable solution to improving the real time capabilities? Mr. ROMINE. I can't predict how accurate the systems will be in the future as they continue to develop. Currently, systems that use facial images that are not in profile or that are not straight on, like mug shot images, or facial images that are indistinct or blurred, have a much lower ability to match. (p. 48)	Database accuracy vital	
25	I have a lot of concerns regarding the false-positive rate of the technology, racial bias in the technology, gender bias, and even during—this is Pride Month, June is Pride Month. I think about the transgender and non-binary communities, and we have seen reports that show that Black women are more likely to be misidentified than any other group. So, when you layer on top of that the transgender person, non-binary, Black individual, what happens to those results? (p. 42)	Concerns about false positives	Color and gender biases
26	These are technologies that exist that we all have. Everyone here wants to protect Fourth Amendment rights and privacy rights of American citizens. None of us want our constitutional protections violated. But the fact is this emerging technology of facial recognition is coming, and it is reflecting just the advancement of our digital technologies that we have already employed across the country and deployed in public areas, including airports. Ms. Del Greco, like any technology, there is a chance for abuse. (p. 15)	FRT use must protect constitutional rights	Potential abuse
27	But in regard to, right now, the use of facial recognition accuracy, you all had six recommendations about transparency and so forth, but I was just talking to some of my colleagues, and how do you fix something … when you dump so many innocent people into a data base? I mean, the numbers are 411 million. I think I heard from you 600 million people are now in this data base that is being used for criminal justice purposes, which I am not sure what is the definition of that. (p. 47)	Recommendations for transparency for large database	Innocent people in database is harmful

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
28	What number of photos does the FBI have access to in just their data base? Ms. GOODWIN. In just their data base, a little over 20-plus, 36 million (p. 34). Mr. JORDAN. Thirty-six million. And then in the data bases that they can then send information to and that are screened and used and there is interface and interaction with at the state level, what is the total number of photos in all those data bases? Ms. GOODWIN. So, access to photos across all the repositories, about 640 million. Mr. JORDAN. Six-hundred and forty million photos. There are only 330 million people in the country. Wow. The FBI has access to 640 million photos, and this is the FBI that didn't comply with the five things they were supposed to comply with when they set up the system, and they are still not in compliance with. . (pp. 34-35)	FBI database is large but did not comply with GAO	No transparency or consent

Appendix C: Hearing Transcript Part III

Figure C1

Hearing Transcript Part III: Facial Recognition Technology – Ensuring Commercial Transparency and Accuracy

FACIAL RECOGNITION TECHNOLOGY (PART III): ENSURING COMMERCIAL TRANSPARENCY AND ACCURACY

HEARING

BEFORE THE

COMMITTEE ON

OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JANUARY 15, 2020

Serial No. 116–82

Printed for the use of the Committee on Oversight and Reform

Available on: *http://www.govinfo.gov*
oversight.house.gov or
docs.house.gov

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan
KATIE PORTER, California
DEB HAALAND, New Mexico

JIM JORDAN, Ohio, Ranking Minority Member
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
JAMES COMER, Kentucky
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida
FRED KELLER, Pennsylvania

DAVID RAPALLO, *Staff Director*
YVETTE BADU-NIMAKO, *Senior Counsel*
COURTNEY FRENCH, *Senior Counsel*
GINA KIM, *Counsel*
ALEX KILES, *Counsel*
AMY STRATTON, *Deputy Chief Clerk*
CHRISTOPHER HIXON, *Minority Staff Director*
CONTACT NUMBER: 202-225-5051

C O N T E N T S

Hearing held on January 15, 2020 1

WITNESSES

* *Opening statements, and prepared statements for the witnesses are available at: docs.house.gov.*

Brenda Leong, Senior Counsel and Director of AI and Ethics Future of Privacy Forum
Oral Statement 6
Dr. Charles Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology
Oral Statement 7
Meredith Whittaker, Co-Founder and Co-Director, AI Now Institute, New York University
Oral Statement 9
Daniel Castro, Vice President and Director of Center for Data Innovation, Information Technology and Innovation Foundation
Oral Statement 11
Jake Parker, Senior Director of Government Relations, Security Industry Association (SIA)
Oral Statement 13

INDEX OF DOCUMENTS

The documents listed below may be found at: docs.house.gov.
* Report from the American Civil Liberties Union; submitted by Chairwoman Maloney.
* Study from the National Institute of Science and Technology; submitted by Chairwoman Maloney.
* Statement of Chief James Craig, Detroit Police Department; submitted by Rep. Higgins.
* Letter from the BTU; submitted by Rep. Pressley.
* Letter from the National Association for the Advancement of Colored People; submitted by Rep. Pressley.
* Letter from the American Federation of Teachers, Massachusetts; submitted by Rep. Pressley.
* Letter from the Massachusetts Teachers Association; submitted by Rep. Pressley.
* Letter from the American Civil Liberties Union; submitted by Rep. Pressley.
* Report from the Detroit Community Technology Projects; submitted by Rep. Tlaib.
* Report from the American Civil Liberties Union, ″Amazon's Face Recognition Software Falsely Matched 28 Members of Congress with Mugshots,″ submitted by Rep. Gomez.

Table C1

Part III: Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces

Pathway To Answering the Research Question: Dimensions Of Purpose Record			
FACIAL RECOGNITION TECHNOLOGY: PART III ENSURING COMMERCIAL TRANSPARENCY AND ACCURACY Hearing Transcript			
Factors That Explain Why Congress Has Not Passed Legislation for FRT Usage in Public Spaces			
	Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**
1	It is clear that despite the private sector's expanded use of technology, it is just not ready for primetime. (p. 1)	FRT not ready for primetime	Need more research
2	We have a responsibility to not only encourage innovation, but to protect the privacy and safety of American consumers. That means educating our fellow members and the American people on the different uses of the technology and distinguishing between local, subjective, identification, and surveillance uses. That also means exploring what protections are currently in place to protect civil rights, consumer privacy, and data security and prevent misidentifications, as well as providing recommendations for future legislation and regulation. (p. 2)	Protection Recommend for future legislation and regulations	Need policy
3	I would like to announce today that our committee is committed to introducing and marking up common sense facial recognition legislation in the very near future. And our hope is that we can do that in a truly bipartisan way. (p. 2)	Committed to FRT legislation Hope for bipartisan way	
4	And while this hearing is about commercial uses of facial recognition, I want to be very clear. I have no intention of unnecessarily hampering technological advancement in the private sector. (p. 2)	Not interested in hampering the private sector usage	Benefits to others
5	The urgent issue, the urgent issue we must tackle is reining in the Government's unchecked use of this technology when it impairs our freedoms and our liberties. (p. 3)	Urgent to rein in unchecked Government use	
6	This issue transcends politics.... It is imperative that Congress understands the effects of this technology on our constitutional liberties. Facial recognition presents novel questions that are best answered by congressional policymaking, which can establish a national consensus. (p. 3)	Effects of FRT on liberties. Congressional policy making is best	
7	The unique Government-wide focus of this committee allows us to consider legislation to address facial recognition technology here at the Federal level. We know that a number of Federal Government agencies possess facial recognition technology and use it without guidance from Congress, despite its serious implications on our First and Fourth Amendment rights. At the bare minimum, we must understand how and when Federal agencies are using this technology and for what purpose. Currently, we do not know even this basic information. (p. 3)	Need info on federal use of FRT	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
8	Because our committee has jurisdiction over the entire Federal Government's use of emerging technology, we must start by pursuing policy solutions to address this fundamental information. It is our intention as well to introduce legislation. We are trying to work with both sides here, trying to work together. That will provide transparency and accountability with respect to the Federal Government's purchase and use of this technology and this software. I am pleased to be working with my colleagues across the aisle on the bill that would address these questions. (p. 3)	Policy solutions necessary Working with both sides Transparency and accountability important at Federal level	
9	So, we will start having these important discussions in a bipartisan way to figure out how and what can the Federal Government do. What can Congress do? What is our responsibility? (p. 4)	Bipartisan discussions to define roles	Consensus important
10	To focus only on the false positives, I think is a major problem for us, though, because I can tell you, technology is moving so fast that the false positives will be eliminated within months. So, I am here to say that if we only focus on the fact that they are not getting it right with facial recognition, we have missed the whole argument because technology is moving at warp speeds, and what we will find is, is not only will they properly—my concern is not that they improperly identify Mr. Gomez, my concern is that they will properly identify Mr. Gomez and use it in the wrong manner. (p. 5)	Technology moving at warp speed Flaws in FRT technology	
11	…how can we put a safeguard on to make sure that this is not a fishing expedition at the cost of our civil liberties because that is essentially what we are talking about. We are talking about scanning everybody's facial features, and even if they got it 100 percent right, how should that be used? How should we ultimately allow our government to be involved in that? (p. 6)	Federal government's role in FRT	
12	The ethical considerations of where and how to use facial recognition systems exceed traditional privacy considerations, and the regulatory challenges are complex. Even relatively straightforward legal liability questions prove difficult when many parties bear some share of responsibility. (p. 7)	FR systems exceed privacy issues and complex regulatory challenges exist	
13	Most facial recognition systems in use are developed by private companies, who license them to governments and businesses. The commercial nature of these systems prevents meaningful oversight and accountability, hiding them behind legal claims of trade secrecy. This means that researchers, lawmakers, and the public struggle to answer critical questions about where, how, and with what consequences this technology is being used. This is especially troubling since facial recognition is usually deployed by those who already have power—say, employers, landlords, or the police—to surveil, control, and in some cases oppress those who don't. (p. 10)	The commercial nature of systems hides them in trade secrets Deployed by those already have power	
14	Facial recognition is not ready for primetime. Congress has a window to act, and the time is now. (p. 11)	FRT not ready for primetime	
15	So, rather than imposing bans or moratoriums, Congress should support positive uses of the technology while limiting the potential misuse and abuse. (p. 12)	Conflicting tasks-support positives and limit misuse and abuse	
16	We support sensible safeguards that promote transparency and accountability as the most effective way to ensure the responsible use of the technology without unreasonably restricting tools that have become essential to public safety. Additionally, SIA does not support moratoriums or blanket bans on the use of this important technology. (p. 14)	Support transparency and accountability but not ban	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
17	As we think about regulation, we believe that any effort specific to commercial use makes sense in the context of the National Data Privacy Policy. Many legislative efforts in this area include biometric information, and was said earlier, we think this needs to be tech neutral. This is the right approach to include. (p. 14)	Biometric information needs to be tech neutral	Remove bias
18	We support sensible safeguards that promote transparency and accountability as the most effective way to ensure the responsible use of the technology without unreasonably restricting tools that have become essential to public safety. Additionally, SIA does not support moratoriums or blanket bans on the use of this important technology. (p. 14)	Support transparency and accountability but not ban	
19	As we think about regulation, we believe that any effort specific to commercial use makes sense in the context of the National Data Privacy Policy. Many legislative efforts in this area include biometric information, and was said earlier, we think this needs to be tech neutral. This is the right approach to include. (p. 14)	Biometric information needs to be tech neutral	Remove bias
20	We have not done the research that is needed to affirmatively answer that, yes, we can protect people's privacy, their liberty when these technologies are deployed at wide scale in a complex geopolitical context. I think we need more of that research, and we need clear regulations that ensure that these are safe. (p. 21)	More research and clear regulations are needed	
21	Could you speak potentially to the—how do we get this right from our perspective of where we sit? Because sometimes, you know, in advancements in technology or anything else, sometimes we step in as the Federal Government to fix a problem and actually end up creating an environment that prohibits the technological advancements or the natural market things that work to make us get to that solution. Sometimes we actually make us take a step back. So, what is the right approach here? (p. 23)	Sometimes federal government intervention makes things worse	
22	I was hoping you could clarify the statement that policymakers and the public should not think of facial recognition as either always accurate or always error prone. In my opinion, as policymakers, we should be pushing to have these technologies get as close to always accurate as possible. Why should we not strive to think of this technology as always accurate, and how long will we have to wait for this technology to reach close to always accurate for all demographic groups. (pp. 23-24)	Policymakers should think of FRT as always accurate	
23	We test mathematical algorithms at NIST. We don't have the capacity and we don't test systems that are deployed in the field. And those have implications as well. (p. 24)	NIST test algorithms, not systems	
24	Mr. ROMINE. From our perspective, whether it's policymakers or Government entities or private sector entities that want to use face recognition, the most important thing to do is to understand—to have the accurate data—accurate, unbiased data that we can provide, so that appropriate decisions are made with regard to whether to regulate or not, what kinds of regulations might be needed, in what context. If you are in a procurement situation, procuring a system, you want to know the performance of that system and the algorithms that it depends on. So, those are the things that we think are appropriate. From an auditing capability or an auditing perspective, we don't view the testing that we do as an audit, so much as providing policymakers and Government and the private sector with actionable information. (p. 24)	Important to understand and have accurate data NIST just provide actionable information	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
25	One of the regulatory options is to have requirements that say Government use or purchase of systems have to be NIST evaluated or have to be, have been ranked by some external objective tester that has clear transparency into what the standards were and how it was measured and what was done. (p. 25)	Need NIST evaluation of any system purchased by government	
26	And part of the source of confusion, I think, in some areas is that there's many different types of systems that are out there. So, some are just doing facial analysis. For example, in the digital signage industry, if you walk by an advertising sign—— Mr. HICE. Without consent? Mr. CASTRO. Without consent. (p. 26)	Digital signage use FRT without consent	Acceptance
27	And so, when we talk about why we are nervous about this, context is critical. And the context that is most critical and most concerning to, I think, Republicans and Democrats on this committee and, frankly, all kinds of people around the country who have taken some time to look into this a little bit is how the Government will use it and potentially violate their most basic liberties. And that is what we are out to get. (p. 29)	Concerned about government Use and violation of basic liberties	
28	Mr. GOMEZ. First, every time I listen to a discussion on facial recognition, more and more questions emerge. It is amazing. I would like to thank my colleagues on both sides of the aisle. I know folks think that Democrats don't care about liberties or freedoms, but we do. But we also care about not only the public space, but also in the bedroom and over one's body, right? That is the way I kind of approach this issue, from a very personal perspective. (p. 30)	More questions about use from a personal perspective	
29	But we will react, and we will start putting some limitations on it. I know that it is tough, but there are a lot of questions. One of the things that I have been trying to figure out, what agencies— like what companies, what agencies, what Federal authorities are using it? How are they using it? Who sold it to them? And if there is a third-party validator, like NIST, who has evaluated its accuracy. Because when this technology does make a mistake, the consequences can be severe. (p. 30)	Need facts	
30	I think it's important to emphasize, as Mr. Jordan did, that accurate facial recognition can also be harmful. So, bias is one set of problems, but this goes beyond that. I think any place where facial recognition is being used with social consequences, we will see harm from these racially and gender biased disparate impact. (p. 32)	FRT used with social consequences is harmful	
31	Mr. ARMSTRONG. Thank you, Madam Chair. I think there are a couple things that we should talk about for a second because I think they are important. And one of them—I am going to go to the Fourth Amendment and criminal context and how this could be deployed there. And this isn't the first time we have seen the crisis in Fourth Amendment. It happened with telephoto lenses. It happened with distance microphones, GPS trackers, drones, and now we are at facial recognition. And to be fair, the Fourth Amendment has survived over time pretty well, but biometric information has a different connotation, which I will get to in a second. (p. 36)	Biometric information and Fourth Amendment concerns	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
32	But the Carpenter case is a pretty good example of how at least the U.S. Supreme Court is willing to change how they view privacy in the digital age. So, part of our job as Congress is to ensure that we write a law and write regulations that ensure that we can maintain those types of privacy standards. (p. 36)	Legislation must have privacy standards	Standards needed
33	So, as we are continuing to carve through these, one thing I think we have to absolutely understand is in these types of cases, we need to apply a statutory exclusionary rule. Otherwise, any regulations we pass don't really, truly matter in a courtroom. And two, we have to figure out a way for meaningful human review in these cases. (p. 36)	Legislation needs an exclusionary rule and human review in cases	
34	The only comment I have from the NIST perspective is that the algorithm testing that we do is to provide information to people who will make determinations of what is and is not an appropriate use. That includes this—you know, this committee, any potential regulation or lack of regulation, and any deployment that's made in the private sector or otherwise is outside the purview of NIST. (p. 39)	Regulations are not a part of NIST responsibility	
35	Mr. COMER. I think there is bipartisan concern here today for facial recognition technology as we move forward. My first question is for Dr. Romine, with respect to the National Institute for standards testing. What is NIST's role in establishing Government-wide policy? Mr. ROMINE. The only role that we have with respect to Government-wide policy is providing the scientific underpinning to make sound decisions. And so, as a neutral, unbiased, and expert body, we are able to conduct the testing and provide the scientific data that can be used by policymakers to make sound policy. (p. 40)	Bipartisan concern NIST does not make policy	
36	Mr. COMER. Well, how does a NIST technical standard differ from a policy standard? Mr. ROMINE. Well, certainly technical standards can be used by policymakers. So, in this case, a determination of a policy that was predicated on identification of algorithms that are based on their performance characteristics is—would be one example of that. But from a policy perspective of what to do or what not to do with face recognition technology, that's something we would support with scientific data, but not with policy proclamations. (p. 41)	NIST difference between technical standards and policy standards	
37	Mr. COMER. Let me ask you this. Is NIST the right agency to develop Government-wide policy? Mr. ROMINE. I don't think so, sir. I don't think that's a NIST role. (p. 40)	NIST's role is not policy making	
38	Mr. PARKER. So, I think that the debate going on right now about establishing a national framework for data privacy is a really important one. And I think that how to set rules for use of the technology in the commercial setting, it's within that framework. And so, I know we've had the GDPR in Europe, but also in the United States, we have some states that are establishing their own frameworks. And that could be a real problem for our economy if we don't establish standardized rules. (p. 41)	National framework for data privacy and standards needed	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
39	Mr. CONNOLLY. Well, it just seems to me, Madam Chairman, that this being the third hearing where we all have expressed concern about the zone of privacy and, frankly, informed consent about citizens or noncitizens whose data—in this case, their face—may be used and how it may be used and transferred to a third party, we have got some work to do in figuring out the rules of engagement here and how we protect fundamental privacy rights of citizens. Unless we want to go down the road of expanding and transferring excuse me, transforming the whole definition of the zone of privacy. And that is a very different debate. But it seems to me that we can't only concede the technology will drive the terms of reference for privacy. (p. 42)	Concern about the zone of privacy transformed by FRT	
40	I am talking again largely what Government is doing, what the Federal Government is doing. So, the first thing we would like to ask for is we just want to know which agencies are using this? How they are using it? To what extent is it happening? And as I think several of you testified, but certainly Ms. Whittaker, we just don't know that. We don't know to what extent is the FBI using it. To what extent are other agencies using it, IRS, any other agency? (p. 49)	Federal government's use of FRT, specifically FBI use	
41	So, first part of what we hope will be legislation that we can have broad support on, that the chairman and both Republicans and Democrats can support, is tell us what is going on now. (p. 49)	Republican and Democrat support wanted	
42	And then, second, while we are trying to figure that out, while the studying and we are getting an accountability and what is all happening, let's not expand it. Let's just start there. Tell us what you are doing and don't do anything while we are trying to figure out what you are doing. And then once we get that information, then we can move from there. (p. 49)	Need facts	
43	Our job is to get it right. Our job is to ensure that we have responsible regulation that protects the privacy of all Americans. But part of doing that is recognizing that it is here, and in some way, shape, or form, it is going to continue to be here. And there are a tremendous amount of positive applications that can be used. (p. 50)	FRT is here Responsible regulation and privacy protection needed	
44	I don't want any false positives. And I don't want any false positives based on race, age, or gender. But my number-one concern is not only those false positives, it is the actual positives—where they are doing it, how they are doing it, why they are doing it. And we have to understand that while this technology has a tremendous benefit to a lot of people, it poses really significant and unique dangers to fundamental, basic First Amendment rights, Fourth Amendment rights. And we have to continue to work forward. (p. 50)	There are benefits and dangers to basic rights with FRT usage	FRT dangerous

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
45	I should also say this isn't the first time the Government has been behind the eight ball on these issues. We are so far behind on online piracy. We are so far behind on data collection, data sharing, and those types of issues. And one of the dangers we run into with that is by the time we get around to dealing with some of these issues, society has come to accept them. And how the next generation views privacy in a public setting is completely different than how my generation and generations above us viewed privacy in a public setting. And the world is evolving with technology, and this is going to be a part of it going forward. (p. 50)	Government behind the eight ball Technology is going forward	
46	But I do want to say that one of the things that came out of the hearing is that it really is not ready for primetime, and it can be used in many positive ways. (p. 51)	FRT is not ready for primetime Has value	
47	I think this hearing showed that this is a wide-scale use. We don't even have a sense of how widely it is being used, yet there is very little transparency of how or why it is being used and what security measures are put in place to protect the American people from that use and their own privacy concerns. (p. 53)	Wide-scale issue No transparency Security needed to protect the public	
48	And we also have the dual challenge not only of encouraging and promoting innovation, but also protecting the privacy and safety of the American consumer. I was very much interested in the passion on both sides of the aisle to work on this and get some account ability and reason to it. And I believe that legislation should be bipartisan. I firmly believe the best legislation is always bipartisan. And I hope to work in a very committed way with my colleagues on this side of the aisle and the other side of the aisle to coming up with common sense facial recognition legislation. (p. 53)	Bipartisan work Conflicting tasks – promote innovation and protect privacy and safety	
49	So, it is not one or the other because I do believe that this will get better and better and better. And we have to put the parameters on it on that use of that technology, but there is still a lot of questions that we have to do. (p. 53)	Need facts	
50	When I started looking into this issue, I did run into that brick wall of national security claims, plus the corporate sector saying that we have, you know, it is proprietary, this information, when it comes to our technology, and we are not going to tell you what it says, how accurate it is, who we are selling it to, who is using it. (pp. 53-54)	Brick wall for information from government and corporate sector about technology	No transparency and cooperation
51	That wall must come down. And that is what I think that we share across the political spectrum. How do we make sure that that wall comes down in a responsible way that keeps innovation going, keeps people safe, but respects their liberties and their freedom? (p. 54)	Conflicting tasks – keep innovation going responsibility and respect people's liberties	

Table C2

Part III: How the Public Is Affected

Pathway To Answering the Research Question: Dimensions Of Purpose Record			
FACIAL RECOGNITION TECHNOLOGY: PART III ENSURING COMMERCIAL TRANSPARENCY AND ACCURACY Hearing Transcript			
How the Public is Affected			
	Narratives (Excerpts from Hearing including page numbers)	**1st Cycle Coding**	**2nd Cycle Coding**
1	Increasingly, local, state, and Federal Government entities are utilizing facial recognition technology under the guise of law enforcement and public welfare, but with little to no accountability. With this technology, the Government can capture faces in public places, identify individuals, which allows the tracking of our movements, patterns, and behavior. All of this is currently happening without legislation to balance legitimate Government functions with American civil liberties. That must change. And while this hearing is about commercial uses. (p. 2)	Government function versus civil liberties	Balance needed
2	This issue transcends politics. It doesn't matter if it is a President Trump rally or a Bernie Sanders rally, the idea of American citizens being tracked and catalogued for merely showing their faces in public is deeply troubling. It is imperative that Congress understands the effects of this technology on our constitutional liberties. (p. 3)	FRT usage effects liberties	
3	I found out that it is being used in so many different ways. Not only in law enforcement—at the Federal level, at the local level—but it is also being used when it comes to apartment buildings, when it comes to doorbells, when it comes to shoppers, when it comes to a variety of things, right? But at the same time, this technology is fundamentally flawed. (p. 4)	FRT used in private living spaces	FRT flawed
4	For somebody who gets pulled over by the police, in certain areas, it is not a big deal. In other areas, it could mean life or death if the people think you, are a violent felon. So, we need to start taking this seriously. (p. 4)	ID mistake could be a matter of life or death	Algorithm flaws
5	So, this is something that we need to raise the alarm. And that is what these hearings are doing in a bipartisan way. To make sure that the American public doesn't stumble into the dark, and suddenly, our freedoms are a little bit less, our liberties are a little bit less. (p. 4)	Bipartisan way to assure freedoms	
6	This issue probably doesn't rank in the top three issues of any American out in the United States, but as it continues to be used and it continues to have issues, there will be more and more people who are misidentified and more and more people who are questioning if their liberties and their freedoms are starting to be impacted for no fault of their own, just some algorithm misidentified them as somebody who committed a crime in the past. (p. 4)	Issue not important unless affected	Algorithm Mistakes harmful

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
7	Because I think if we start focusing again on just the accuracy, then they are going to make sure that it is accurate, but what standards should we have the accuracy there? Should it be 100 per cent? Should it be 95 percent? You know, I think when Mr. Gomez was actually identified, the threshold was brought down to 80 percent. Well, you are going to get a lot of false positives when that happens, but we need to help set the standards and make sure that our government is not using this in an improper fashion. (p. 5)	Accuracy is important	
8	However, the real harms arising from inaccurate recognition and characterization systems cannot be ignored. (p. 7)	Inaccuracy is the real danger	
9	New uses are being imagined all the time, but the potential harms are real. In addition to inaccuracy, concerns about real-time surveillance societies have led individuals and policy makers to express significant reservations. The decision by some municipalities to legislatively ban all use of facial recognition systems by government agencies reflects these heightened concerns. (p. 7)	Real-time surveillance a concern	Unwanted surveillance
10	While FPF prefers a comprehensive privacy bill to protect all sensitive data, including biometric data, we recognize that Congress may choose to consider technology-specific bills. If so, our facial recognition privacy principles provide a useful model, particularly in requiring the default for commercial identification or verification systems to be opt-in—that is, express affirmative consent prior to enrollment. Exceptions should be few, narrow, and clearly defined, and further restrictions should be tiered and based on the scope and severity of potential harms. (p. 7)	Structure of a FRT bill	Legislation needed
11	Facial recognition poses serious dangers to our rights, liberties, and values, whether it's used by the state or private actors. The technology does not work as advertised. Research shows what tech companies won't tell you, that facial recognition is often inaccurate, biased, and error prone. And there's no disclaimer to warn us that the populations already facing societal discrimination bear the brunt of facial recognition's failures. (p. 9)	FRT error-prone and dangerous to rights	Company don't warn users
12	Facial recognition and analysis are also being used to make judgments about people's personality, their feelings, and their worth based on the appearance of their face. This set of capabilities raises urgent concerns, especially since the claim that you can automatically detect interior character based on facial expression is not supported by scientific consensus and recalls discredited pseudoscience of the past. (p. 10)	FRT used to judge more than faces	No scientific consensus for use
13	To address the harms of this technology, many have turned to standards for assessment and auditing. These are a wonderful step in the right direction, but they are not enough to ensure that facial recognition is safe. Using narrow or weak standards as deployment criteria risks allowing companies to assert that their technology is safe and fair without accounting for how it will be used or the concerns of the communities who will live with it. If such standards are positioned as the sole check on these systems, they could function to mask harm instead of preventing it. (p. 10)	Standards developed for some to address harms	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
14	From aviation to healthcare, it is difficult to think of an industry where we permit companies to treat the public as experimental subjects, deploying untested, unverified, and faulty technology that has been proven to violate civil rights and to amplify bias and discrimination. Facial recognition poses an existential threat to democracy and liberty and fundamentally shifts the balance of power between these using it and the populations on whom it's applied. Congress is abdicating its responsibility if it continues to allow this technology to go unregulated. And as a first step, lawmakers must act rapidly to halt the use of facial recognition in sensitive domains by both government and commercial actors. (p. 10)	FRT threatens democracy and liberty	
15	If you care about the over-policing of communities of color or gender equity or the constitutional right to due process and free association, then the secretive, unchecked deployment of flawed facial recognition systems is an issue you cannot ignore. (pp. 10-11)	Over-policing	Secretive unchecked deployment
16	I think there is probably a greater danger that they will get facial recognition right. You know, it is not the misses that I am concerned about right now, although that has to stop. It is what happens when they have all this data out there, whether it is law enforcement for private firms. (p. 20)	Greater danger if FRT is right	
17	We had a massive data breach by Suprema, which is a big biometrics collector, 100 million people, I think. No, I am sorry, 27 million people in that breach. And then Customs and Border Patrol, 100,000 people that they identified, along with license plates, that was breached. So, the concern is once this information is collected, it is not secure. And that is a major problem for all of us. (pp. 20-21)	FRT databases are unsecured	
18	I think auditing is absolutely important, but we need to understand how we're measuring these systems. In my written testimony, I gave an example of one of the most famous facial recognition measurement systems. It was a dataset that we measure these systems against, and it's called Labeled Faces in the Wild. And in short, it features photos of mainly men and mainly white people. So, the way that the industry assessed accuracy was to be able to recognize white men, and that gives us a sense of why we're seeing these pervasive racial and demographic biases across these systems. (p. 24)	FRT has demographic biases	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
19	So, the standards we choose to measure ourselves by matter greatly. And if those standards don't ask questions about what the data that will be used in these systems in a deployment environment will be, how these systems will be used. If they don't ask questions like what the Atlanta Plaza tenants were concerned about, will they be abused? (p. 25)	What should the standards for accuracy of data look like	Data accuracy. Standards for development.
20	There is no question this technology of facial recognition is extremely important and viable for our Government, I think, most notably, places like border patrol and law enforcement. At the same time, there is also no question that this technology allows for any individual to be identified in public spaces, be it through private sector or Government entities, and therein lies a potential problem and grave concern for many people. Both, whether we are dealing in private sector or Government, should bear the responsibility of individual privacy and data security. (p. 25)	Technology is a threat to individual privacy	Privacy protection
21	I mean, it is one thing to have policies, to have things written down. It is another thing to implement these things to protect the public, protect individuals who are not—have not consented to this type of technology. So, how will these facial recognition products, as they develop, inform individuals that they are being exposed, potentially without their knowledge? (p. 26)	Widespread Surveillance	Unwanted surveillance
22	I would also recommend that the communities on whom this is going to be used have a say in where it's halted and where it may be deployed. Are the people who are the subjects of its use comfortable with its use? Do they have the information they need to assess the potential harm to themselves and their communities? And is this something that—have they been given the information they need to do that. (p. 29)	Americans catalogued in a database for showing their faces	Informed consent. Affirmative consent.
23	So, there's two levels of obscurity. There is law enforcement exemption, military exemption, where we don't get the information about the use of these technologies by government, and then there is corporate secrecy. And these interlock to create total obscurity for the people who are bearing the costs of these violating technologies. (p. 30)	Obscurity in FRT deployment	Transparency needed
24	I think it's important to emphasize, as Mr. Jordan did, that accurate facial recognition can also be harmful. So, bias is one set of problems, but this goes beyond that. I think any place where facial recognition is being used with social consequences, we will see harm from these racially and gender biased disparate impact. (p. 32)	Accurate FRT harmful	Harm for gender and racial bias
25	So, we're seeing high stakes that really compromise life and liberty here from the use of these biased algorithms. (p. 32)	Biometric or algorithms bias	

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
26	And you know, in response to the question of where they are being used, which algorithms are being used here, we don't have public documentation of that information. We don't have a way to audit that, and we don't have a way to audit whether they are— whether NIST's results in the laboratory represent the performance in different contexts, like amusement parks or stadiums or wherever else. So, there's a big gap in the auditing standards, although the audits we have right now have shown extremely concerning results. (p. 32)	Standards and regulations are needed	
27	The use of facial recognition technology continues to grow at a breathtaking pace and is now seeped into nearly every aspect of our daily lives. Many families are unaware that their faces are being mined as they walk through the mall, the aisles of the grocery store, as they enter their homes or apartment complexes, and even as they drop their children off at school. (p. 34)	Technology not rushed to marketing	Public unaware
28	We know that the logical end of surveillance is often over-policing and the criminalization of vulnerable and marginalized communities. (p. 34)	Surveillance is biased	
29	Well, this technology is clearly biased, inaccurate, and even more dangerous when used in schools, where Black and brown students are disproportionately already over policed and disciplined at higher rates than their white peers for the same minor infractions. In my district, the Massachusetts Seventh alone, Black girls are six times more likely to be suspended from school and three times more likely to be referred to law enforcement, again, for the same infractions as their white peers. Our students don't need facial recognition technology that can misidentify them and lead them to the school-to-confinement pathway. (p. 35)	Communities are not treated equally and fairly	Biometric or algorithms bias
30	In Detroit, for example, the city's Public Housing Authority recently installed security cameras on these public housing units that we believe is going to be something that encroaches onto people's privacy and their civil liberties. You know, these are people's homes. And so, I don't think being poor or being working class means somehow that you deserve less civil liberties or less privacy. And so, Ms. Leong, what are the privacy concerns associated in enabling facial recognition software to monitor public housing units? If you live in a low-income community, is your civil liberties or your privacy lessened? (p. 38)	Communities are not treated equally and fairly	Biometric or algorithms bias
31	They are for-profit technology that are coming into communities like mine that is overwhelmingly majority Black and testing these products, this technology, onto people's homes, the parks, the clinics. It is not stopping. Now I hear my good colleague from Massachusetts talk about them installing it in schools. They are using this, and I have a police chief that says, oh, this is magically going to disappear crime, but if you look, my residents don't feel less safe. They actually don't like this green light that is flashing outside of their homes, the apartment building, because for some reason he is telling everybody it is unsafe here. You know, it takes away people's kind of human dignity when you are being policed and surveillanced in that way (p. 38)	Communities are not treated equally and fairly	Community equality needed

	Narratives (Excerpts from Hearing including page numbers)	1st Cycle Coding	2nd Cycle Coding
32	And that demonstrates that we need to focus on what the things are that we are protected, which has been discussed so clearly here today in terms of our values, freedoms, and liberties. And then how we don't let the technology because it's here, because it can do certain things, or because it's even convenient that it does certain things, impinge on those in ways that we don't think through carefully and not ready to accept those compromises. (p. 52)	No one wants constitutional protections violated	Privacy protection