January 2015

Reconceptualizing Privacy: An Examination Of The Developing Regulatory Regime For Facial Recognition Technology

David James Potter

RECONCEPTUALIZING PRIVACY: AN EXAMINATION OF THE DEVELOPING REGULATORY REGIME FOR FACIAL RECOGNITION TECHNOLOGY

by

David James Potter
Bachelor of Science, University of Nebraska, 2008
Master of Public Administration, University Nebraska Omaha, 2010

A Dissertation

Submitted to the Graduate Faculty

of the

University of North Dakota

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Grand Forks, North Dakota
August
2015

This dissertation, submitted by David J. Potter in partial fulfillment of the requirements for the Degree of Doctor of Philosophy from the University of North Dakota, has been read by the Faculty Advisory Committee under whom the work has been done and is hereby approved.

Slavka Antonova

Kyle Conway

Richard Fiordo

Lana Rakow

James Mochoruk

This dissertation is being submitted by the appointed advisory committee as having met all of the requirements of the School of Graduate Studies at the University of North Dakota and is hereby approved.

Wayne Swisher
Dean of the School of Graduate Studies

July 27, 2015
Date

PERMISSION

Title	Reconceptualizing Privacy: An Examination of the Developing Regulatory Regime for Facial Recognition Technology
Department	Communication and Public Discourse
Degree	Doctor of Philosophy

In presenting this dissertation in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my dissertation work, or in his absence, by the Chairperson of the department or the dean of the School of Graduate Studies. It is understood that any copying or publication or other use of this dissertation or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and the University of North Dakota in any scholarly use which may be made of any material in my dissertation.

David Potter

David J. Potter

7/20/15

Date

TABLE OF CONTENTS

LIST OF FIGURES xi

ACKNOWLEDGMENTS xii

ABSTRACT..... xiii

CHAPTER

1. INTRODUCTION 1

1.1 Chapter Descriptions.....7

2. UNDERSTANDING THE CONTEXTUAL DEVELOPMENTS FOR THE FACIAL RECOGNITION TECHNOLOGY MEETINGS.....11

2.1. Key Parameters of the Facial Recognition Debate Case 15

2.1.1. Venue 16

2.1.2. Participant Groups 17

2.1.3. Meeting Phases 20

3. FACIAL RECOGNITION TECHNOLOGY 24

3.1. Biometric Data.....24

3.2. Modalities of Facial Recognition.....26

3.3. History and Development 29

3.4. Techniques for the Acquisition of Face Data 32

3.4.1. Intensity Images.....32

3.4.2. Video Sequences.....34

3.4.3. 3D and Infrared.....35

3.5. Facial Recognition Technology Uses 35
3.6. Public Debate 38
4. THEORETICAL FRAMEWORK 40
4.1. Historical Conceptions of Privacy 41
4.2. Contemporary Conceptions of Privacy 46
4.3. Private Organizations' Need for Privacy 54
4.4. Legal Conceptions of Privacy 56
4.5. Information Privacy 59
4.6. What Privacy Is Not 63
4.7. Discussion on Privacy 65
4.8. Modes of Resistance to Facial Recognition Technology 67
4.9. Communication Technology Regulation Studies 68
4.9.1. Theories of Regulation 71
4.9.2. Soft Versus Hard Regulation 71
4.9.3. Regulation of Technology 75
4.10. Discussion on the Application of Regulation Theories 77
4.11. Multistakeholder Collaborative Process 78
4.11.1 Multistakeholder Processes and Shared Power 84
4.11.2. Multistakeholder Outcomes 85
4.11.3. Learning 85
4.11.4. Concensus 87
4.11.5. Capacity Building 88
4.12. Discussion on Multistakeholder Theories Application 88

4.13. Summary 89

5. METHODS 91

5.1. Philosphical Underpinnings 91

5.2. Research Design 94

5.3. Stages of Research 96

5.3.1. Data Collection 96

5.3.2. Participant Observation 97

5.3.3. Semi-Structured Interviews 98

5.4. Data Analysis 99

5.5. Research Questions 105

6. EVOLUTION OF DATA PROTECTION REGULATION 107

6.1. History and Development of Data Protection 107

6.2. Safe Harbor 110

6.3. U.S. Data Protection 114

6.4. Photography, the First Amendment, and Copyright 118

6.4.1. Photography and the First Amendment 118

6.4.2. Photography and Copyright 119

7. HOW IS THE REGULATORY REGIME OF FRT EMERGING IN THE U.S 122

7.1. Stakeholders 122

7.1.1. Non-Governmental Organizations 122

7.1.2. Academics 123

7.1.3. Businesses 123

7.1.4. Government....124

7.2. Historical Results Impacting the Multistakeholder Process for Facial Recognition Technology....124

7.2.1. Inefficiencies....125

7.2.2. Participation....128

7.2.3. Business Resistance....130

7.2.4. Trust....131

7.2.5. Expectations....133

7.2.6. Moderator....134

7.3. Previous Processes Regarding Facial Recognition Technology....135

7.4. The Current Multistakeholder Process on Facial Recognition Technology....136

7.4.1. Perceived Benefits From the Multistakeholder Process....137

7.4.2. Criticism of the Multistakeholder Process....139

7.4.3. Convener....140

7.4.4. Scope....144

7.4.5. Moderator....148

7.4.6. Participation....150

7.4.7. Expectations....153

7.5. New Strategies Adopted to Encourage Stated Outcome Success....154

7.5.1. Personal Communication Strategies....155

7.5.2. Decision Making Strategies....157

7.6. Complications With the Multistakeholder Process on Facial Recognition Technology....163

7.6.1. Disparate Opportunities to Participate in the Decision Making Process 163

7.6.2. Perceived Representation Issues 164

7.7. Towards Creating a Code of Conduct 167

7.8. Conclusion 168

8. REGULATION OF FACIAL RECOGNITION TECHNOLOGY 169

8.1. Deployment of Facial Recognition Technology 170

8.2. Stages of Facial Recognition 185

8.3. Facial Recognition Technology Data 190

8.3.1. Reverse Engineering Data 196

8.3.2. Data Security 199

8.3.3. Data Access 208

8.3.4. Data Retention 220

8.4. Notice 225

8.5. Transparency 228

8.6. Conclusion 230

9. HOW DOES FACIAL RECOGNITION TECHNOLOGY CHALLENGE CURRENT CONCEPTIONS OF PRIVACY 232

9.1. Understanding Stakeholders' Conceptions of Privacy 232

9.1.1. Big Data and Privacy 238

9.1.2. Technology and Privacy 240

9.1.3. Privacy and Control 241

9.1.4. Privacy and Business 243

9.1.5. Privacy and Anonymity 247

9.2. Anonymity and Free Speech 252

9.3. Facial Recognition Technology as a Threat to Privacy 252

9.3.1. Facial Recognition Technology Simulating Human Capabilities 253

9.3.2. Data 256

9.3.3. Data Linkage 258

9.3.4. Cognitive Intrusion 261

9.4. Reconceptualizing Privacy 262

10. CONCLUSION 266

Appendix A: Universal Declaration of Human Rights Privacy Principles 275

Appendix B: List of Interviewees 277

Appendix C: Definitions for the NTIA Multistakeholder Facial Recognition 278

Appendix D: Mission Statement of the Department of Commerce 281

Appendix E: List of Acronyms Used 282

Appendix F: Provisions of the NTIA 283

Appendix G: Interview Protocol 285

Appendix H: Table of Codes 288

REFERENCES 289

LIST OF FIGURES

Figure Page

1. Timeline for facial recognition technology entering the public debate 11

2. Timeline of 2014 multistakeholder meetings 16

3. Display of American Institute of Architects Boardroom, NTIA MSH Venue 17

4. Timeline for major stages of MSH meetings on FRT.....23

5. EU data protection timeline 114

ACKNOWLEDGMENTS

I wish to express my sincere thanks to my adviser, Dr. Slavka Antonova, whose guidance and advice made this dissertation possible. I would also like to thank the members of my advisory committee: Dr. Kyle Conway, Dr. Richard Fiordo, Dr. Lana Rakow, and Dr. James Mochoruk; their contributions to this project have helped immensely.

I would also like to thank my parents, without whom I would not be here today; their support for my education and welfare cannot be overstated. This project has only been completed thanks to their tireless support.

Finally, I would like to extend my gratitude to all of my fellow Communication and Public Discourse graduate students who supported me in all of my scholarly endeavors and shenanigans. I would especially be remiss if I did not thank Dr. Joshua Young for putting up with me through the good times and the bad times.

To my parents, Dr. Dave and Connie Potter
Thank you for your unending love and support.

ABSTRACT

The National Telecommunications and Information Administration have convened a series of meetings to create a voluntary code of conduct for the commercial use of facial recognition technology. This research asks and answers three questions related to the creation of the voluntary code of conduct: 1) How is the regulatory regime of FRT emerging in the U.S.? 2) What are the roles of the various stakeholders in shaping the commercial regulation of FRT? 3) How does FRT challenge our current conceptions of privacy? Data has been gathered to answer these questions using participant observation and semi-structured interviews. The data was analyzed via mediated discourse analysis. Findings of the research include: the highly sensitive nature of the biometric data that facial recognition technology collects, the data's ability to be linked across multiple databases, the surreptitious way the data can be collected, the potential chilling effect the technology can have on the First Amendment, and the various threats the technology poses to privacy.

Keywords: Privacy, Facial Recognition Technology, Multistakeholder, and Biometric Data

CHAPTER 1

INTRODUCTION

Privacy is currently at the center of a major U.S. controversy. On February 12, 2014, Kentucky Republican Senator Rand Paul filed a class action lawsuit against President Barack Obama, Keith Alexander, Director of the National Security Agency (NSA), James Clapper, Director of National Intelligence, and James Comey, Director of the Federal Bureau of Investigation (FBI). Paul contended that the warrantless and suspicionless data collection of American citizens, which had been performed by the government, was illegal under the Fourth Amendment (Fuller, 2014). Paul's concerns reflect a wide-spread public feeling of uneasiness with the government's access to private online data. According to the Pew Research Internet Project, 68% of Internet users believe the privacy laws do not provide enough protection and 50% are worried about the amount of their personal information available online (Rainie, Kiesler, Kang, and Madden, 2013). Other citizens cite laws such as the Patriot Act to argue that the collection of users' private data is necessary for the security of the country. Facial Recognition Technology (FRT), a relatively new form of data collection technology possesses the powerful ability to link data about individuals, further invading personal privacy and threatening the general anonymity, the ability to be anonymous in public a majority of the time that Americans currently enjoy.

The ability to scan an individual's face and recognize it, which is within the capacity of FRT, further exacerbates the public debate on Internet privacy. Joseph Atick (2011), a pioneering scientist of modern FRT, defined facial recognition as a computer's ability to recognize faces in photos and appropriately identify separate individuals. FRT is the essential hardware to record or scan an image, as well as the software to process the algorithms required for recognition or verification. In the following work, FRT is used as a blanket term to include the hardware and software necessary for face recognition, identification, and verification. The International Biometrics & Identification Association (IBIA) draws a distinction between *photographs*, which it does not view as biometric identifiers, the ability to uniquely identify a person by a distinguishing *biological feature*, and a *faceprint*, the digital code extracted from a photograph, that can be matched against other databases (Atick, 2011; Rouse, 2008). Faceprints can be thought of similarly to fingerprints, as both are unique individual identifiers.

There are three stages in the application of FRT, beginning with face detection. *Face detection* can be accomplished using memoryless systems, which do not "extract, store or utilize faceprints; they simply detect the presence of a human face" (Atick, 2011, p.1). Although unnerving in its own right, the current privacy controversy concerns the systems that store such information, rather than simply acknowledge it. The other two stages in FRT application include facial recognition identification and facial recognition verification. *Identification* is the process of comparing a singular faceprint to a database of multiple faceprints to determine who the individual is. *Verification*, on the other hand, provides process reliability by ensuring that a person is who he says he is.

Recently, the *commercial use of FRT* has gained popularity. Internet companies like Facebook and Google have made noticeable use of the technology through "tagging"[1] and Google Glass[2] respectively. Many retailers are adopting the technology to combat shoplifters. Most notably, FRT was deployed during the 2001 Super Bowl to search individuals against a mug shot database in an effort to identify wanted criminals (McCullagh, 2001).

This dissertation explores the evolution of the regulatory regime of FRT. First, the focus is the National Telecommunications and Information Administration (NTIA) multistakeholder (MSH) process for the development of a regulatory regime for FRT; this is a unique process which involves stakeholders who previously participated in an earlier MSH process convened by the NTIA. This process began February 6, 2014 and continues as of this writing (June 2015). The meetings were primarily followed via the webcast posted on the NTIA website. In all ten meetings have been recorded. Issues discussed in the meetings include but are not limited to: notice, transparency, reverse engineering of data, First Amendment rights, Fourth Amendment rights, and surveillance.

Through the discourse analysis of video transcripts and interviews conducted for the study, as well as tracking the development of the regulatory regime for FRT, this researcher demonstrates how the stakeholders view the concept of privacy and the various methods they have constructed to regulate FRT. Interviews have been conducted with members from each stakeholder group: academics, government officials, business members, and non-governmental organizations (NGOs). A discussion on the merits and

[1] Refers to a feature on Facebook where an individual can assign a name to an individual in a photograph.
[2] Eyewear that allows an individual to Google search and perform other tasks on objects in their range of sight.

the deficits of creating a voluntary code of conduct to regulate this technology has been provided. This dissertation demonstrates that the flexibility of a code of conduct allows for continued innovation of the technology. Alternatively, the voluntary nature of the code of conduct provides little protection to consumers if companies do not agree to sign on. This dissertation illustrates the positions of various stakeholder groups and their advocacy goals for outcomes to the voluntary code of conduct. The primary focus of the process is to protect United States consumers and their privacy; however, many of the businesses represented in the process are international in nature. References to international standards or laws are done for the sake of business entities involved in the process but the primary focus remains on the United States consumer.

Several assumptions have been made while conducting this research. The first assumption made is the adoption of the liberal notion of privacy. As Anita Allen (1998) notes: "The liberal conception of privacy is the idea that government ought to respect and protect interests in physical, informational, and proprietary privacy" (p. 723). The liberal notion of privacy is similar to liberal notions of property; privacy is associated with things we own such as our home, body, and affects (Allen, 1998). This notion of privacy is primarily concerned with inaccessibility to either our person or our information. Also, this notion places a premium on individual choice and autonomy over our lives. This view of privacy has been challenged by business interests represented in the multistakeholder process.

Another assumption of this research is the primacy of business or economic interests over the liberal notion of privacy and democracy. During the course of observing the meetings, business and economic interests have trumped the privacy of

individuals. It is clear that corporate power has trumped that of the individual and appears to challenge a few pillars of American democracy namely the First and Fourth Amendments.

Finally, privacy is a concept without strict agreement as to its definition or scope, nor is there uniform appreciation for privacy amongst the public. Privacy varies in importance to individuals subjectively and in the context of a given situation. As such, it is very difficult for the academic community to make statements and conceive of privacy as a static definition. Therefore, the academic community has provided narrow conceptions of privacy including: physical, informational, or cognitive; and dealt with specific facets of privacy. The dissertation demonstrates how FRT blurs the distinctions the academic community has previously made. As such, I propose that privacy needs to be reconceptualized. Privacy scholars should conceive of privacy as interference. The interference concept accounts for privacy's subjective and contextual nature while, more importantly, not adding an additional definition of privacy, which is common in academic literature. This work aims to explain why this conception works and why it will be beneficial to privacy scholars.

Several research questions have been asked and answered by this dissertation. The first question the dissertation answers is: How is the regulatory regime for FRT emerging in the U.S.? This regime is being developed via a unique MSH format to protect consumer privacy. The second question addressed by the dissertation is: What are the roles of the various stakeholders in shaping the commercial regulation of FRT? In other words, what consumer safeguards are being implemented to protect privacy from the challenges posed by FRT. Finally, this project addresses the question of: How does

FRT challenge our current conceptions of privacy? The project has concluded that privacy must be re-conceived because of the capabilities of FRT.

This dissertation employs multiple research methods to answer the above stated questions. Data has been collected by conducting interviews with participants involved in this process as well as through participant observation. Discourse analysis has been conducted on the data to determine which texts have contributed to the development of a code of conduct for FRT. Multiple research methods have been employed to enhance the reliability of the findings.

This dissertation contributes new knowledge to the fields of new media, privacy, and the regulation of communication technology. FRT is a new medium through which communication can be conducted, as such it poses new challenges as well as benefits to the way humans communicate. It is argued in this dissertation that FRT poses new and unique challenges to current conceptions of privacy; as such, new understandings of privacy are needed in light of the development of FRT. Finally, this project contributes to current understandings of the regulation of communication technology. This project argues that there is a field of technology regulation despite the term scantly appearing in the academic literature.

There are limitations to all research projects and this dissertation is no exception. Limitations include:

- The debate and creation of a voluntary code of conduct are incomplete. The original timeline for the process was to begin in February and end in June with a scheduled re-convening of the group in September, this timeline was adopted by this dissertation.

- The novelty of this technology is another limiting factor of this dissertation. There is scarce theoretical literature available about the technology.
- Not all stakeholders who were reached agreed to provide an interview. Important stakeholder voices are missing from this dissertation.
- Novelty of the evolving regulatory regime for FRT being created via a MSH process.

1.1. Chapter Descriptions

Chapter two contains a detailed case description of the evolving regulatory regime for FRT. The meetings arose out of trade complications with the European Union (EU) and the Consumer Privacy Bill of Rights (CPBR) (2012). The case is discussed in reference to relevant documents and previous processes convened dealing with FRT. While the NTIA MSH meetings represent the first regulatory regime for FRT there were other "best practices[3]" issued previously by the Federal Trade Commission (FTC). A description of the venue, participants, and proceedings of the meetings is also presented.

The third chapter is a description of how FRT actually works. FRT has multiple uses and different modalities. The chapter discusses the differences between recognition, authentication, and identification. There are several different ways to conduct a facial scan, each with their own merits and deficits. These various scanning methods are discussed, including how they are used to identify or authenticate an image. Also, in this chapter, a discussion of accuracy rates, thresholds and their uses, as well as hybrid uses of the technology are provided.

[3] The FTC has issued a staff report containing best practices for the commercial use of FRT.

Chapter four discusses the theoretical underpinnings of this research. The dissertation employs the social constructivist paradigm and shows how this case study fits under it. This research relies on three primary theoretical concepts: privacy, regulation of technology, and multistakeholder collaboration. Presented in the chapter are the historical, legal, theoretical, and varied conceptualizations of privacy. This chapter shows that the regulation of technology is a field of study, though the term is not used in the academic literature. Also presented are the historical approaches to the regulation of communication technologies as well as contemporary theories of technology. Finally, a discussion on the history and merits of the multistakeholder approach to creating regulation is provided. The discussion focuses on the advantages of collaboration as it relates to the case as well as regulating the technology.

The fifth chapter is best described as a research methods chapter. In this chapter a discussion of the case study design, its rationale for being chosen, and the strengths and weaknesses of the design are provided. This dissertation employs multiple methods for collecting data including participant observation, semi-structured interviews, and discourse analysis. Strengths of these data collection methods as well as the benefit of using multiple data collection methods to triangulate results are discussed as well.

Chapter six is a discussion and comparison of the U.S. and EU data protection laws, specifically focusing upon their differences. In many ways, this analysis is necessary because of tensions between the U.S. and the EU, primarily in terms of each country's stance on data protection. Edward Snowden's revelations concerning the NSA spying scandal strained U.S. EU commerce relations due to Safe Harbor violations. Lack

of data protection on the part of the U.S. needs to be understood in order to comprehend why the CPBR was created and what its goal is.

Chapter seven contains analysis of the first research question of the dissertation (Please see section 5.5. for a more detailed review of the research questions): How is the regulatory regime for facial recognition technology emerging in the U.S.? This MSH process was preceded by an earlier process regarding mobile application transparency. The mobile application transparency process was concerned with the notice that users receive about their data and privacy protections when downloading and using a mobile application or "app." This carryover of stakeholders is a unique situation as most stakeholders are new to each process. Furthermore, the previous process was largely described as unpleasant and unproductive. Next, a discussion of how the voluntary code of conduct is emerging for FRT is provided. Participants in the current MSH process have adopted new communicative strategies and alternative decision making methods to achieve positive outcomes. The strengths and weaknesses of these new decision making methods are discussed as well. A discussion is also provided on stakeholder relationships, participant influence on the MSH process, as well as representation in the meetings.

Chapter eight primarily concerns how the technology itself is regulated, which is an ongoing process. Here the research question: "What are the roles of the various stakeholders in shaping the commercial regulation of FRT?" is answered. A discussion is provided on data security, as it was the initial matter discussed during the MSH meetings after the group had learned about the technology. Further detail is provided about the

sensitivity of the data collected, best practices for securing said data, and the different privacy implications attached to each modality of FRT.

In chapter nine the central question of this research is answered, which is how privacy should be reconceptualized because of this technology. Initially, data on how stakeholders conceive of privacy are presented. Understanding how stakeholders conceive of privacy is important in determining the development of a voluntary code of conduct for FRT. Next, the many conceptions of privacy are briefly discussed as well as how FRT blurs the distinctions privacy scholars have previously made. An argument is provided for the merits conceptualizing privacy as interference without creating additional definitions of privacy, which would only serve to further cloud the waters of academic study.

Chapter ten acts as the final chapter of this dissertation, where a summary of the major findings from this research, limitations to the research, and areas for future inquiry are all presented. The MSH process for FRT is ongoing, and, as such, conclusions are limited as to what language will be contained in the code of conduct as well as the consumer protections to privacy may provide. An argument for further research concludes this chapter.

CHAPTER 2

UNDERSTANDING THE CONTEXTUAL DEVELOPMENTS FOR THE FACIAL RECOGNITION TECHNOLOGY MEETINGS

In the United States, facial recognition technology has been under development for decades[4], funded primarily through government agencies. One of the first times FRT entered the public debate was the December 2011 Federal Trade Commission workshop on FRT. The workshop brought together diverse participants to discuss a variety of issues surrounding the increasingly likely commercial use of FRT. The FTC in October of 2012 issued a staff report entitled *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*. The best practices included privacy consideration, the sensitivity of FR data, and security measures (Federal Trade Commission, 2014).

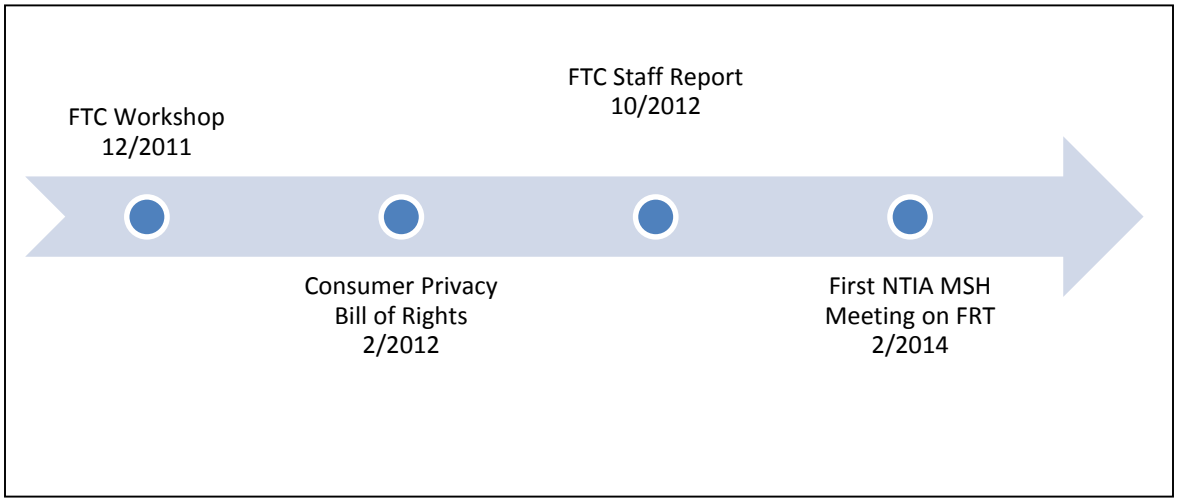

Figure 1. Timeline for facial recognition technology entering the public debate

[4] Please see section 3.3. History and Development

The National Telecommunications and Information Administration's (NTIA) The NTIA multistakeholder meetings for facial recognition technology began with the Consumer Privacy Bill of Rights (CPBR) in, February of, 2012). The White House intended the CPBR to protect consumer's privacy by describing broad privacy protecting principles that consumers should expect from companies that handle personal information. The CPBR is

> [P]art of a comprehensive blueprint to protect individual privacy rights and give users more control over how their information is handled. This initiative seeks to protect all Americans from having their information misused by giving users new legal and technical tools to safeguard their privacy. (White House, 2014)

The CPBR tasks the Department of Commerce's NTIA with convening a series of multistakeholder (MSH) meetings, including Internet companies, consumer advocates, trade associations, businesses, and governments on a variety of privacy issues (including the use of facial recognition technologies). The goal of the MSH meetings is to create enforceable codes of conduct that comply with the CPBR and that can be enforced by the FTC. The Obama Administration has also pledged to work with Congress to enact comprehensive privacy legislation. [5]

[5] The current 2013-2014 113th Congress is on track to be the least productive Congress ever, passing just 142 bills as of July (Murray, 2014). According to the Pew Research Center, have just a 28% favorable view of Congress, 69% disapprove (Pew Research Center, 2014). Additionally, just 44% of the American public approve of the President according to Pew Research Center (Tyson, 2014). The administration has pledged to work with Congress to pass the privacy principles in the CPBR but has also urged advocates and the private sector to work together to implement the principles outlined in the CPBR. Given the current political realities, it seems unlikely that the President and Congress will enact these privacy protections legislatively. Codes of conduct represent an alternative way forward toward the goal of protecting consumer privacy by developing voluntary codes of conduct that comply with the privacy principles and can be enforced by the FTC.

The Obama Administration directed the NTIA Privacy MSH Process: FRT to produce codes of conduct. This MSH framework allows interested parties to participate and work within their areas of expertise. As it is explained by the White House, "Multistakeholder processes can provide scalable, flexible means of developing codes of conduct that simplify companies' compliance obligations" (White House, 2012, p. 2). To a certain extent, business is dependent on consumer trust and confidence. It is anticipated that businesses, that chose to adopt a voluntary code of conduct, will enjoy an extra level of consumer trust. Adoption and compliance with a code of conduct, once created, could provide businesses with a competitive advantage (Bowie & Jamal, 2006, p. 339).

Another National Telecommunications and Information Administration driven process was held prior to the current one on FRT, in July of 2012, concerning Mobile Application (app) Transparency. Some stakeholders from the current FRT process described the mobile app process as frustrating, as some stakeholders were deliberately disruptive rather than working towards an agreeable end, disruptive stakeholders likely had the goal of avoiding the creation of new regulation. Not all of the stakeholders from the FRT process were involved in the mobile app process, but those who were may have approached the current situation with a skeptical view. Prior experience with a MSH process allowed the NTIA to conduct a more coherent debate of the FRT uses, stakeholders expressed opinions that the FRT process proceeded with less confrontation, which they largely attributed to the moderator, John Verdi, who skillfully facilitated the debate.[6]

[6] John Verdi was a former advocate at the Electronic Privacy Information Center (EPIC) before being hired at the NTIA. Verdi sees his role in the process as a facilitator, nothing more or less. He was very specific about his role as facilitator, so as to not influence the process but to simply facilitate it. Some stakeholders

The following key principles of the CPBR provide important context for the group's interaction and the code of conduct created (White House, 2012) *Individual control*, or consumers have a right to exercise control over what personal data companies collect from them and how they use it. *Transparency* is the right consumers have to easily understandable and accessible information about privacy and security practices. *Respect for context* concerns consumers having a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. *Security* is a right consumers have to secure and responsible handling of their personal data. *Access and accuracy* is a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate. *Collection* concerns consumers having a right to reasonable limits on the personal data that companies collect and retain. Finally, *accountability* is a principle where personal data is handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights (Whitehouse, 2012).

These privacy principles were based on the National Institute for Standards and Technology's (NIST) Fair Information Practice Principles (FIPPs), originally included in the Privacy Act of 1974 (NSTIC, 2014). The above principles were specifically designed with generalizability in mind in order to promote flexibility in company implementation. The Obama Administration hopes that the flexibility of the general principles in the CPBR will lead to innovation that creates better consumer and business outcomes.

---

have had a previous relationship with Verdi and others have not. Stakeholders have not articulated a negative opinion of John or his facilitation of this process.

2.1. Key Parameters of the Facial Recognition Debate Case

The MSH meetings on FRT that the NTIA convenes, facilitates the stakeholder debate on how to protect consumer privacy from the commercial use of the technology. The NTIA is an executive branch agency that primarily advises the President on matters of information and telecommunications policy. One of the chief concerns of the NTIA is enhancing access to broadband Internet; however, the NTIA also focuses on copyright, online privacy, online security, and the Internet economy. The NTIA handles domestic and international telecommunications activities.

The NTIA MSH meetings concerning FRT began February 6, 2014. These meetings were announced on the NTIA website in advance to encourage interested parties to join the mailing list for the process. Each of the meetings were scheduled once a month from February to December of 2014, with each meeting lasting, four hours. This dissertation was designed to follow the stated timeline and is one of the reasons this research ends ahead of the completion of a code of conduct for FRT. The meetings were open to the public (a notification was published on the NTIA website December 3, 2013 announcing the upcoming meetings) and convened at the boardroom of American Institute of Architects in Washington D.C.; they were also made available via a webcast on the NTIA website, providing interested parties the opportunity to dial in to the conference call. One business interviewee (whose anonymity has been protected) has described the process as "radically transparent." A timeline for the 2014 meetings is as follows:

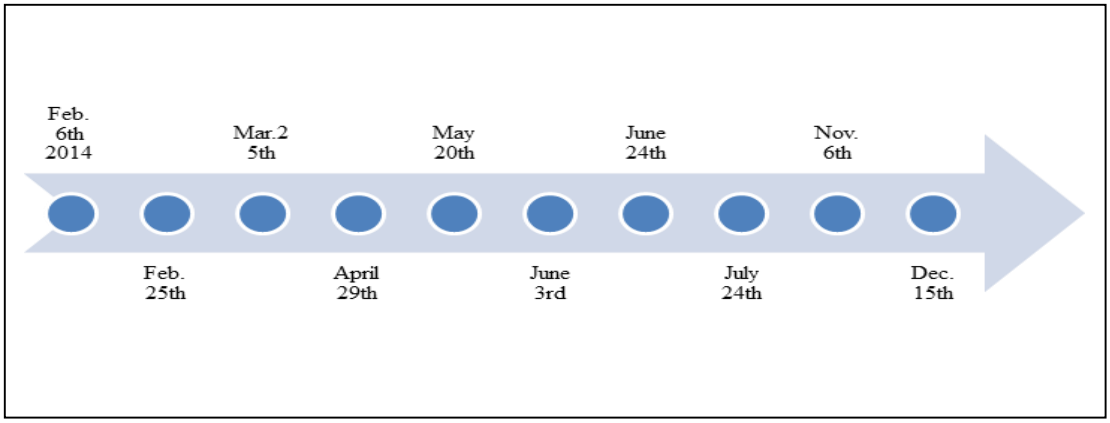

Figure 2. Timeline of 2014 multistakeholder meetings.

2.1.1. Venue

The desks in the boardroom are arranged in a two tiered horseshoe shape. The room is capable of seating around 70 individuals. The seats are all provided with microphones so that stakeholders can be heard in both the room and on the webcast (See Figure 3.)

The stakeholder collaboration is facilitated by a projector located in the center of the room so that the participants can see and work on documents collaboratively. Three cameras in the room ensure observation via the webcast and allow individuals to see the documents, as well as the speakers.

Figure 3. Display of American Institute of Architects Boardroom, NTIA MSH Venue

Adapted from "American Institute of Architects' Website" (American Institute of Architects, 2014)

Figure 3. Display of American Institute of Architects Boardroom, NTIA MSH Venue. Adapted from "American Institute of Architects' Website" (American Institute of Architects, 2014)

2.1.2. Participant Groups

Representatives from four broad groups of stakeholders were present at the meetings: academics, government, business, and non-governmental organizations (NGOs). The following provides more details on the representatives: *Academics* from varied institutions have made presentations, some institutions represented include but are not limited to: Rutgers University, Carnegie Mellon University, and UCLA. *Government* representatives include the NTIA, the FTC, some elected official representatives, and the Information and Privacy Commissioner's Office of Ontario. *Business* representatives include but are not limited to International Biometrics and Identification Association (IBIA), Interactive Marketing Researchers, Kairos, Pacaso, NetChoice, Motorola, and

others[7]. The last major stakeholder group is *NGO* participants that are comprised of advocacy groups, including the American Civil Liberties Union (ACLU), Center for Digital Democracy (CDD), Common Sense Media, Consumer Federation of America, Electronic Privacy Information Center (EPIC), Center for Democracy and Technology (CDT), and others.[8] The following is a brief description of the stakeholders who attained high visibility through participation. These descriptions are included to provide the reader an idea of the advocacy goals of the most vocal participants involved in the process.

- The American Civil Liberties Union was one of the most vocal participants throughout the process.[9] Throughout this MSH process the ACLU was concerned about protecting the privacy rights of individuals.
- Common Sense Media, an advocacy group, was primarily concerned with FRT being used to take pictures of or sell products to children. In later meetings, the group also urged the other stakeholders to include the term "facial profiling" into the definitions list.[10]

[7] Private sector participants were harder to track because not all of them have been vocal participants

[8] It is not always clear who is monitoring the meetings as stakeholders can call in to the meetings or follow along on the webcast without identifying themselves or their respective organizations. Stakeholders may have various motivations for monitoring the meetings and not participating.

[9] According to the ACLU's website, "The ACLU is our nation's guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country" (ACLU, 2014).

[10] According to the Common Sense Media website, "Common Sense is dedicated to helping kids thrive in a world of media and technology. We empower parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids' lives" (Common Sense Media, 2014).

- Consumer Federation of America is a non-profit organization protecting consumer rights, was often in opposition to the interests of commercial companies[11].
- The Center for Digital Democracy (CDD)[12] advocated for increased learning and education during the meetings when other members of the group felt they had sufficient facts. CDD protested and challenged the validity of the MSH process.
- The Center for Democracy and Technology (CDT)[13] provided technical expertise and occasionally voiced their opinion on matters they are invested in, most notably data encryption and the definition of encryption as it relates to FRT.
- NetChoice was also actively involved in the process.[14] The organization has been involved in helping draft the definitions that the group will work with and use on the code of conduct.
- The International Biometric Industry Association (IBIA) has also been an active participant in the NTIA MSH meetings on FRT.[15]

[11] "The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, nearly 300 of these groups participate in the federation and govern it through their representatives on the organization's Board of Directors" (Consumer Federation of America, 2014).
[12] "CDD has been at the forefront of research, public education, and advocacy on protecting consumers in the digital age. It has helped foster widespread debate, educating a spectrum of stakeholders, and creating a legacy of government and self-regulatory safeguards across a variety of Internet and digital media platforms" (Center for Digital Democracy, 2014).
[13] "CDT is a champion of global online civil liberties and human rights, driving policy outcomes that keep the Internet open, innovative, and free" (Center for Democracy and Technology, 2014).
[14] "NetChoice is a trade association of eCommerce businesses and online consumers all of whom share the goal of promoting convenience, choice, and commerce on the net" (NetChoice, 2014).
[15] "The International Biometrics & Identification Association (IBIA) is a trade association founded in September 1998 in Washington, DC that promotes the effective and appropriate use of technology to

- Motorola, represented by an attorney in the FTR proceedings, is a leading mobile device manufacturer. It remains unclear to this researcher exactly what Motorola was advocating for during the meetings but the organization led the risks/harms committee by way of use cases to provide actual FRT use examples. The group worked alongside the Definitions Committee but has an important role in determining what some of the ultimate uses of FRT may be via the code of conduct. Motorola also represented a potential key stakeholder as some technologists have already shown that facial recognition (FR) is possible using mobile devices and off the shelf software.

2.1.3. Meeting Phases

The FRT MSH collaborative process progressed in phases from February to December 2014. The researcher observed the following three major phases in the MSH process based on stakeholder interaction and the agenda set by the moderator.

1. February-April: was the information collection stage marked by expert presentations and stakeholder debates. This provided stakeholders with a baseline of knowledge on several different areas. With the possible exception of certain technologists, stakeholders were learning about how the technology works, how different companies use the technology, and what the technology may be able to do in the future. Initially, the Microsoft representative was a vocal contributor at the meetings. She gave a brief presentation about how their Xbox Connect technology worked, which provides a large consumer use of FRT and technologies similar to FRT. The first four meetings were reliant

---

determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments" (International Biometrics and Industry Association, 2014a).

on presentations from companies, technologists, and advocates for more fact finding. The initial stage of the process started with consensus building, where stakeholders developed a common understanding of terminology, technology capabilities, and agreement about the scope of the process. This consensus building continued throughout the process and was prominently seen again at the end when the codes of conduct were drafted and a consensus was reached in terms of appropriate actions to include in the code.

A major source of contention in the initial meetings, and a lingering point of frustration, was the scope of the code of conduct. With the National Security Agency (NSA) revelations from Edward Snowden, the stakeholders at the meeting were increasingly concerned about government's use of the technology, specifically related to surveillance, personal privacy, and freedom of speech.

2. May-July: In the case collection stage the stakeholders were utilizing their knowledge about the technology to identify potential risks/harms. The participants were also looking at examples of best practices, previous debate, and the technology being deployed in the physical environment to create a code of conduct. In the second stage, the actual work on a code of conduct began. Committees were formed to create a common language (definitions committee) and to discuss applications (risks/harms committee). This led the participants to consider which uses of the technology they were uncomfortable with, and opinions often varied. Discussing cases of the application of the FRT led the group to compile a list of use cases that became the Risks/harms

Committee. These use cases challenged the participants to create solutions or guidelines to the use of the technology in specific situations. Terminology quickly became a problem for the group which often led to misunderstandings.

The definitions committee focused on creating a common language that the stakeholders could use to avoid terminology confusion. For example, stakeholders were confused about what a "user" of FRT was. Did a user describe the person operating FRT or the person the technology was being applied to? Terminology issues such as these were identified and corrected by the Definitions Committee.

3. November-December: The drafting stage was marked by stakeholders coming together to decide on a final code of conduct. In this stage the capacity building potential of the MSH process is demonstrated as the stakeholders used their "accumulated social, intellectual, and political capital" to make decisions (Antonova, 2011, p. 433). At this final stage the participants who drafted the code of conduct expressed two varying positions. The privacy protection advocates argued for a more limited scope for the use of FRT, which was contrary to the industry advocates' perspective. Industry advocates suggested a wider scope of FRT uses. Where the code applies to the scope, use, and varied capabilities of the technology remain to be seen. The final stage proceeded based on topics of consensus within the group. The first issue that received broad consensus from the stakeholders was security. Agreement was achieved that FR data should receive strong protection in order to make

the data as secure as possible. Recent data breaches occurring at Target and Home Depot were discussed during the meetings and encouraged stakeholders to treat data security seriously. It was believed that stakeholders coming to consensus on "low hanging fruit" items, such as security, provided the group with momentum and good will so that more contentious items could be agreed upon later.

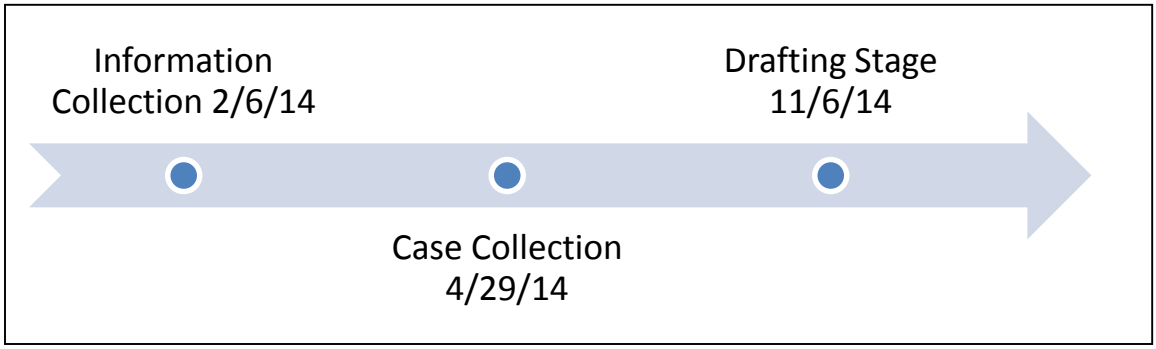

Figure 4. Timeline for major stages of MSH meetings on FRT.

CHAPTER 3

FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology applies algorithms to process photos of an individual. This evaluation can recognize the presence of a face, authenticate an individual for access to a privilege, or identify an unknown individual. Facial recognition technology collects unique biometric data that cannot be changed or replaced if exploited.

3.1. Biometric Data

Biometric data are based on personal unique biological traits such as finger prints. The term biometrics is now commonly used to describe the technology that allows for the collection and examination of biometric data. Biometric data are increasingly being used by consumers, and commercial, as well as government, uses abound (Wood, 2014). Biometrics offer the possibility of making daily transactions and interactions safer, as it is hard to copy or fake DNA or similar biological traits. Apple iPhone users, for instance, can now use their fingerprint to unlock the device or use a scan of their face. This eliminates the worry of stolen or compromised passwords which ultimately leads to unwanted access of protected data. It also facilitates convenience of use by eliminating the need to remember multiple passwords; instead a device can be accessed by simply presenting one's face or scanning one's finger.

Despite the common belief that biometrics enhance security and provide convenience to the user, some experts have expressed concerns: an individual's biometric

data are very difficult, if not impossible, to change. Should biometric data be compromised, there is no way to change the data, as one would if their password was compromised. For these reasons, biometric forms of authentication are often a secondary form of authentication, or, if used as a primary form, are typically coupled with another secondary form of authentication, like a pin number or smart card (Atick, 2014).

FRT is one mode of obtaining biometric information about a person. Other methods include iris scans, hand telemetry, fingerprints, and DNA. Facial recognition technology is unusual because it does not require the consent of the person whose picture is being taken; photography is a First Amendment protected activity (Schauer, 1981). Iris scans and hand telemetry devices would require the individual to consciously interact with the system. The faceprint, the biometric information created from an image, can be taken surreptitiously from a distance or even at night if using infrared FRT (Kong, Heo, Abidi, Paid, & Abidi, 2005). This technology mimics a human skill, recognizing faces. In contrast, humans cannot identify someone based on a casual observation of their fingerprint or the size of their hand. The other major difference is the scalability of the technology; FRT can scan and store potentially endless numbers of images, while humans are capable of remembering up to 10,000 faces, according to some estimates (Radford, 2004).

Facial recognition technology is applied to an image or a series of images of a person. The images often reveal additional information about the person besides allowing the technician to extract a face template. Many digital cameras capture what is called Extended File Information (EXIF). EXIF data contains information about the camera that took the photo, such as file name, size, date, camera make, camera model,

resolution, flash usage, focal length, and Jpeg process (Alvarez, 2004, p. 2). Apple's iPhone is also capable of embedding precise geo-coordinates with photos and videos taken with the device (Friedland & Sommer, 2010, p. 1). Also unique to FR is its ability to easily fix a person in place and time. The fact that more information can be collected about an individual from their faceprint, which can be gleaned from a photo, raises concerns about privacy expectations, particularly who is collecting the information.

3.2. Modalities of Facial Recognition

Facial recognition technology usually operates in a predictable manner, however, not all systems perform identification. The initial process is *face detection*. The system must first look through the image or video to determine whether or not there is the presence of a human face. Applications for face detection may include face counting to determine traffic in a store. During this process there is no additional information collected about the person and no comparisons are made about the individual.

Face detection is not completely innocuous, however, because the system or operator may be capable of making other determinations about the individual. The system may be able to recognize race, gender, and even an individual's age range. Operators may be able to draw conclusions about the wealth or relative health of an individual based on other factors present in the picture, such as clothing or medical devices.

Another cause for concern about face detection is whether the system is capable of recognizing the same face. During this process, the system may collect face data and store it for a period of time without identifying it. Imagine someone who is an alcoholic and frequents the local liquor store. The system may not know who the individual is, or

anything about the individual, but it may be able to determine that the same individual visits the store on a daily basis. This example seems innocuous unless their face is identified and enrolled in a separate system that can be linked to the liquor store. From there, the individual could be dropped from his/her health insurance or even denied an organ transplant. The rise of "big data,"[16] including vast consumer dossiers full of transactional, demographic, and financial data could be more easily linked thanks to FRT.

After a face has been detected, the system may or may not be capable of performing a more detailed analysis. The next step is *authentication*, sometimes used interchangeably with *verification*. During the authentication stage the (FR) system is trying to determine if the person who is presenting himself as John Doe is in fact John Doe. Payroll systems commonly deploy this type of technology. Employees often present their faces as a way to clock into and out of work. During the authentication process, the system compares the face and identity that is presented with a stored (enrolled) identified image in a database. The system extracts the face template from the individual in front of it and compares it with the identified template stored in the system.

During this process there are two types of errors that could occur. A type I error is the acceptance of a false positive. The FR system matches the individual to a stored identity incorrectly. In other words, the system believes that there is a match when in fact there is no match. The systems can be altered according to a threshold rate, which equates to how willing the operator is to experience false positives. Therefore, if a system has a false accept rate of .1 for every 1000, then there will be one false positive

[16] The ability of society to harness information in novel ways to produce useful insights or goods and services of significant value" and "…things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value (Press, 2014 par. 10).

identification per 10,000 individuals that attempt access. The rate corresponds with the size of the database. For every 100,000 there will be 10 false positives, for 1,000,000 there will be 100 and so on (Vaillant, 2014)

A type II error refers to a false reject; this occurs when an individual with correct credentials is present and the system mistakenly fails to allow the individual access. An example of this would be if an ATM machine failed to allow an individual access to their bank account.

These two types of errors impact the end user in completely different ways. When a type II error occurs, as with the ATM example, an authorized user is denied access to a system or privilege to which they should have access. Continuing the ATM example, the user becomes annoyed that they do not have access to their account, and may have to employ another authentication method, including entering a pin number or physically visiting the bank to present the appropriate credentials, in order to access their money. However, if a type I error is made, then an unauthorized user will gain access to another individual's bank account, which could lead to fraud or theft. This is why the threshold false accept rate of the system becomes critically important.

The threshold rate can be raised or lowered depending on the needs of the system. For critical access applications, such as a bank account, the threshold can be very high, which will lower, or maintain, the false accept rate. However, the two errors have an inverse relationship. As the threshold is raised, the false accept rate stays low but the false reject rate increases. In banking matters, most customers are willing to accept a higher false reject rate and deal with the annoyance rather than have an unauthorized individual gain access to personal bank accounts. Of course, the bank can collect more

images of the individual or higher quality images to improve both the accuracy of the system and the experience of the customer. In other applications where less sensitive access is on the line, the threshold can be lowered (Vaillant, 2014).

Experts suggest that the most difficult process to complete is that of identification. This is where the FR system performs a one to many match. Here the system tries to find the identity of an unknown individual by extracting their faceprint and comparing it with a database of templates. This type of application is common in law enforcement communities trying to match criminals to identified mug shots. In these systems, the threshold false reject is usually lowered. Law enforcement is willing to accept more false positives in order to find the criminal. Often a system will return multiple images that an analyst will then review in order to determine a match. Mug shots follow a standard format in terms of face orientation, distance, and lighting in order to increase the likelihood of finding a match.

3.3. History and Development

Facial recognition technology can be traced back to the 1880s when Alphonse Bertillion, a police officer working in Paris, became concerned with identifying criminals. Bertillion decided to record body images of criminals and took their mug shots under controlled lighting. Standardized images and mug shots thus became standard practice in police work until there were too many images to search effectively. Despite FRT's criminological beginnings, the technology is not associated as strongly with criminality as is fingerprinting. Eventually, innovations in computing technology led researchers to try to teach computers to read faces (Morozov, 2012), thus began the work of modern FRT.

Some of the earliest digital work on facial recognition began in the 1960s. After spending several years working on pattern recognition, Woody Bledsoe, along with Helen Chan and Charles Bisson, began developing a way for computers to recognize faces. However, much of this early work was not published, though, "Because the funding was provided by an unnamed intelligence agency that did not allow much publicity" (Ballantyne, Boyer, & Hines, 1996, p. 10). The project originally involved matching a photograph of an individual to a data set containing many images, essentially matching a photograph from a book of mug shots. The results were expressed as a ratio between the number of images the program felt were matches to the original number of images selected. However, the technology faced many challenges, namely the rotation and tilt of the head (face), lighting, angle, facial expression, and aging (Ballantyne, et al., 1996).

The technology employed by Bledsoe located several coordinates on the face used to perform accurate facial measurements. These measurements include the inside and outside corners of the eyes, the location of the pupils, the width between the eyes and pupils, and the point of widow's peak (hairline). The technology also accounted for the various angles and rotations of the images by "normalizing" these measurements. In all 20 distances were recorded and the technology was capable of processing 40 pictures per hour. The research was advanced by Peter Hart at the Stanford Research Institute, where the computer consistently outperformed human recognition on a database of 2000 images, marking one of the first successful uses of the technology (Ballantyne, et al., 1996).

In the 1970's, scientists were unable to make major progress in the development of FRT for several reasons. The quality of the images was not high enough for the systems to perform more accurate recognition. More sophisticated algorithms were also needed to process the images. Finally, computing power was either insufficient or too expensive (Morozov, 2012).

The 1980's saw the formation of a new industry. Academia and corporations came together to work on "automated person identification," which would later become the biometrics industry. In 1992, the research division of the NSA convened a meeting of a biometrics group. Intelligence and defense agencies, which funded most of the FRT projects, allowed the technology to progress significantly (Morozov, 2012).

The use of FRT garnered much public attention in 2001 when it was utilized to compare Super Bowl attendees against a mugshot database (McCullagh, 2001). Cameras were fixed at the turnstiles to surveil fans as they entered the venue, which resulted in the most public and most highly criticized use of FRT's capabilities (ACLU, 2003). Accuracy has now greatly improved as well. One industry test showed that the 2006 algorithms were ten times more accurate than those available in 2002 and more than a hundred times more accurate than those in 1995 (Morozov, 2012) and yet FRT technology is still evolving. FRT systems are now capable of skin texture analysis, where a segment of skin is converted to mathematical segments of space. Infrared scans which are capable of performance in the dark, are also often utilized and can detect vein structure under the face, another biometric identifier (Kong et al., 2005; Morozov, 2012). Face "hallucination" is another developing technique for FR where computers guess what

a low resolution face may look like from a large collection of high resolution faces (Liu, Shum, & Freeman, 2007).

3.4. Techniques for the Acquisition of Face Data

Facial recognition techniques can be broadly categorized into three areas based on the acquisition of face data: intensity (color) images, video sequences, and 3D information or infrared imagery (Jafri & Arabnia, 2009). A discussion follows on how each of these techniques work.

3.4.1. Intensity Images

Face recognition derived from intensity images fall into two main categories: feature-based and holistic. Feature-based approaches identify, extract, and measure features of the face, including, but not limited to, the eyes, mouth, nose and other fixed markings. These markings are then used to create a geometric relationship where, statistical pattern recognition techniques can match faces (Jafri & Arabnia, 2009). However, it is unfair to say the system functions automatically "In general, current algorithms for automatic feature extraction do not provide a high degree of accuracy and require considerable computational capacity" (Jafri & Arabnia, 2009, p. 43). This is to say that the process is not automatic; technicians are often needed to locate the geographic areas (widow's peak, chin, pupil spacing, etc.) that allow FR to work.

Another features-based approach is Elastic Bunch Graph Matching. This technique creates a graph from hand selected fiducial points on the face. Fiducial points are reference points on the face; for example, the pupils of the eyes are considered fiducial points. Each fiducial point then becomes part of a complete graph. The distance from the points are measured to create a series of graphs called a face bunch graph.

Graphs for new faces can be compared to the original and matches are made by determining the highest similarity value between graphs (Jafri & Arabnia, 2009).

Features-based approaches offer several advantages. Since the features are extracted before matching an image, they are resistant to inaccuracy created by position changes of the face. These approaches offer relatively compact representations of the face, which aid in the matching process and can be performed with relative speed. However, automation of feature detection has proven difficult and requires greater time for data gathering. Individuals employing these techniques make arbitrary decisions on facial features. If the selected features cannot be discriminated from, matching will prove difficult (Jafri & Arabnia, 2009). Therefore, the chosen features are important to the matching process as some features offer greater accuracy than others. Other methods focus on the entirety of the face and not simply facial features.

Holistic methods, based on the entire image of the face also fall into two main subcategories: statistical and artificial intelligence (AI). The simplest statistical approach draws data from a two dimensional representation of the color values of a face. A direct comparison can then be made between the original face and other faces. This technique has been shown to work, but its usability is rather limited by alterations in lighting, pose, and expression. Remedies to these shortcomings include infrared images and 3D images (Hiremath & Hiremath, 2013).

Unlike statistical methods, AI uses intensity images to conduct FR. AI is a complex way of conducting FR, "AI approaches utilize tools such as neural networks and machine learning techniques to recognize faces" (Jafri & Arabnia, 2009, p. 48). Neural networks mimic the way the human brain works. In the brain, there are interconnected

neurons to allow for thought processing. Neurons, which comprise neural networks, respond to input signals and allow the machine to "think" (Russell, 1991). A popular example of an AI application is Facebook's AI system "Deep Face." Deep Face uses AI technology known as deep learning to match faces. It is just slightly less accurate than humans, it correctly matches faces 97.25% of the time. whereas humans are 97.53% accurate (O'Toole, 2014).

3.4.2. Video Sequences

FRT is popularly used for security purposes, often applied to security video recordings. Video sequences are examined by the technology in stages, "A video-based face recognition system typically consists of three modules: one for detecting the face; a second one for tracking it; and a third one for recognizing it" (Jafri & Arabnia, 2009, p. 51). To offer security, FRT needs to be able to recognize faces in real time and identify them. Frames are selected from the video that offer the best chance of performing a match and then a recognition technique is applied to the intensity image. Methods for FR in video sequences vary from Difference of Gaussian filtering, "an illumination pre-treatment," to skin color modeling (Wang, Li, Wang, Jiang, Jiang, & Zhao, 2012, p. 429). Other methods employ using images, where the face has moved 180˚, allowing the system to see the front and both sides of the face. One method involves analyzing video and 3D information for accuracy (Jafri & Arabnia, 2009).

Video sequences are more difficult to match compared to static images as they often suffer from low quality, the presence of multiple faces, and background information that hinders the process. However, the abundance of data in video sequences allows the option of discarding less desirable images. Video sequences also offer the advantage of

viewing the face from multiple angles, which can eliminate other accuracy detriments, such as facial expressions and lighting.

3.4.3. 3D and Infrared

Most of the research on FR has been focused on 2D matching. However, as the technology progresses increased attention will continue to focus on alternative matching methods, such as, 3D information and infrared imagery. The 3D technique allows for the recording of complex data, including the curvature of the face, jaw line, and cheek profile. These techniques are also not easily confused by lighting and orientation variances, compared to the 2D techniques. However, the complexity of the data causes a significant increase in computing expenditures. Currently, 3D techniques employ the use of lasers, structured light systems, stereo vision systems, and reverse rendering (Jafri & Arabnia, 2009).

Infrared imaging offers yet another method for FR. Infrared techniques reveal vein and tissue structures of the face, which are unique to each individual. Infrared techniques are limited in use due to the high cost of thermal sensors, lack of data sets, sensitivity to ambient temperature conditions, and the disruption glass causes when collecting information (eyeglasses can occlude data) (Jafri & Arabnia, 2009). Nevertheless, infrared techniques allow for the collection of data in dark places, making it a unique option for FR.

3.5. Facial Recognition Technology Uses

Current uses of FRT can be broadly categorized into three sections: government, commercial, and private. These categories are often not distinct. For example, the

government can contract with commercial vendors of FRT, and, in turn, the commercial entities may use the data they gather for their own economic interests.

The original area of interest in the FRT was law enforcement. In September of 2014, the Federal Bureau of Investigation (FBI) announced that its FR system was fully operational. The system would allow law enforcement agencies, including probation and parole officers, to cross-reference photos from criminal databases. It would also allow continuous updates on reported criminal history for individuals in trust positions, such as school teachers (Volz, 2014).

In March 2014, the city of Seattle voted to allow the police department to use FRT to identify suspects caught on camera (Wagstaff, 2014). Police had reported they were already doing the process manually, but that FRT would speed it up significantly. The project was funded by a grant from the Department of Homeland Security. The measure was originally opposed by the city council until certain provisions were added, including allowing only trained officers to use the FR software, as well as limiting the use of the software to still images and individuals suspected of criminal activity (Wagstaff, 2014).

Government uses tend to revolve around security and identity. Evgeny Morozov (2012) described a situation in 2010 where Navy SEALs used FRT from satellite photos to identify a suspected terrorist. The New York Times reported that the NSA is collecting millions of photos that can be examined by FRT. This technology is also deployed in airports to verify passports and heightened assurance of positive identification on government IDs.

It appears that some commercial entities may have an edge on the government in terms of accuracy. Russell Brandom (2014) reported that Facebook's DeepFace system is better than the FBI's new Next Generation Identification system boasting 97% accuracy rate compared to the FBI's 85% accuracy, respectively. The FBI's FR database has caused some controversy because the database will include biometric identification of persons who are not suspected of criminal mischief (Electronic Privacy Information Center, 2014).

A popular private sector use of FRT includes social networking sites, particularly Facebook and Google+ which are leading developers of FRT. Facebook has spent considerable time and effort developing its FRT with the latest announcement of their DeepFace technology. The DeepFace technology is almost as accurate in identifying faces as humans are (O'Toole, 2014), and is coupled with the largest photo library in the world, thanks to Facebook users (Grandoni, 2014). Similar to Facebook's tagging feature, where Facebook asks if you would like to attach your friend's names to pictures on your profile, Google+ has a "Find My Face" feature that suggests names in photos. Unlike Facebook, Google+ has users opt-in to use the controversial feature, providing users with the opportunity to consent (Kincaid, 2011).

Payroll systems that employ FRT allow employers to eliminate possible employee fraud on time cards. If an employee claims that they worked for eight and a half hours and they should be paid for the time they put in, and liability on the employer's behalf is eliminated as well. This also prevents fellow co-workers from clocking in a late friend at work, which can cost businesses thousands in lost revenue through decreased production (Brackeen, 2014).

Although commercial and government uses of FRT are still in their infancy, experts perceive potential government uses for fraud prevention of social programs, assistance in locating missing children, passport verification, and the prevention of driver's license duplication. Commercial applications range from social networking, payroll systems, cruise ship photos, eye tracking, emotion research, facial response to stimuli, image searches, and government sponsored vendor services.

3.6. Public Debate

The public debate surrounding FRT is one that continues to shift. Given the technology's history, especially that significant funding was provided by intelligence and defense organizations, much of its earliest implementations were created for law enforcement use (Ballantyne, Boyer, & Hines, 1996; McCullagh, 2001). Members of the public, who seek police intervention to maintain law and order, grant such agencies a certain amount of discretion in performing those roles, thus are unlikely to question the need for this new surveillance technology (Gates, 2011). These views are supported by a more communitarian view of privacy advocated by Amitai Etzioni (1999). Etzioni's views require individuals to relinquish some of their privacy in order to maintain public safety and order. However, there are members of society who are more skeptical of the role of police and question their need for such technologies. The Snowden revelations have in part supported the latter's argument. Daniel Solove (2011) argued that a false dichotomy exists between privacy and security, and that both can be achieved properly utilizing technology. For further discussion on contemporary views of privacy please see section 4.2.

Retail use is another instance where FRT has garnered much attention in the public sphere. Advertisers and retailers are eager to use the technology to better serve their customers, as they say, and quickly point them in the direction of products and services they are likely to buy. Groups like Common Sense Media and Center for Digital Democracy are concerned, though, about the technology being used to "steer" customers to particular products/services or even discriminate based on race, gender, or age. Providing disparate opportunities to customers via FRT is a legitimate concern.

Helen Nissenbaum (2009) argued for privacy in context. Privacy protections and affordances should be based on the context in which they arise. There are some indications that this may be the way that FRT is treated. For instance, people may enjoy the convenience of FRT's use at airports to speed lines, limit intrusive searches, and increase security. These are likely seen as legitimate uses of the technology. FRT systems located outside of children's stores, bathrooms, or surreptitiously surveilling people from mall kiosks are generally viewed as inappropriate uses of the technology at the meetings. Furthermore, privacy is a fluid concept and a subjective value. Providing individuals with a choice or the ability to consent to being subject to FRT is being discussed as an appropriate way to deploy the technology. However, even with the flexibility of choice and transparency, (two principles outlined in the CPBR) (Please see p. 11 for full list of principles), there are participants who worry about "bad actors" who would not consent to FRT in an effort to avoid detection and potentially aid in their nefarious acts.

CHAPTER 4

THEORETICAL FRAMEWORK

For this project, the theoretical construct relied on the concepts of privacy, communication technology regulation, and the multistakeholder collaborative process. The academic community has not reached consensus on the theoretical or legal conception of privacy as it has been interpreted as a legal concept in a variety of different contexts. The framers of the U.S. constitution recognized the need for privacy as a necessary condition for freedom. Although technological advances in communication have played a substantial role in improving the public's lives as well as the democratic process, these advances have also enhanced the government's and commercial organizations' ability to intrude on one's privacy. Diverse theoretical and legal interpretations of privacy focus on the dialectic between the right to privacy and the enhanced technological power of surveillance. The theories of privacy presented here are meant to serve as a "purposive sample" to cover the central arguments in the field of privacy (Randolph, 2009, p.4).

Similarly, the presentation of theories on regulation and the multistakeholder format is not meant to be exhaustive. The theories presented were selected based on their importance to their respective fields, as well as their relevance to this research project. Furthermore, the "regulation of technology" is not a phrase used often in the academic literature, but, as will be shown, such a field exists nonetheless. Privacy is not a new

concept, so it is important to track the way that scholarship and thinking on the subject has evolved. Presented initially are some historical conceptions of privacy.

4.1. Historical Conceptions of Privacy

As early as the mid-19th century, John Stuart Mill conceived of privacy as a necessary condition for freedom. For Mill (1988), "[I]n the part which merely concerns himself, his independence is of right, absolute. Over himself, over his own body and mind, the individual is sovereign" (p. 69). Mill believed actions that do not affect society or other individuals should be permitted to the individual, based on his or her own liberty. Mill also found "The only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant" (p. 68). Of course, surveillance was already a problem in Mill's time. In fact, surveillance was an issue before Mill. During the early years of the U.S. postal system, letters would often be delivered in bulk via ship, to a central location where they sat for extended periods of time. To keep information private some individuals employed wax seals. In 1753 Benjamin Franklin, Postmaster General, required postal workers to swear an oath not to open mail (Regan, 1995). In sum, two conceptions of privacy, *the need for seclusion and the need to keep information private*, were recognized at this early time. The categorization of *physical privacy* and *information privacy* are still used in scholarship today.

In the late 19th century, Samuel Warren and Louis Brandeis were the first legal scholars to argue about the right of privacy in the context of mass media and photo cameras (Warren & Brandeis, 1890). For them, privacy was "the right to be let alone."

Warren and Brandeis penned *The Right to Privacy* in 1890, during a time when the technologies of the day, cameras and the press, enabled others to encroach on one's privacy. The response occurred after Warren read a society page piece about the lavish party he threw for his daughter after her wedding in the *Boston Saturday Evening Gazette* (Rosen, 2000). Thus, decisive steps were made to broaden the notion of privacy by considering the private agents abilities to conduct surveillance over private individuals; in doing so, privacy was codified as a legal concept and constituted 'intrusion of privacy' as a separate tort or private law.

In many ways, Warren and Brandeis created the foundation of FRT as a challenge to privacy. They were concerned about cameras operated by private agents intruding on others' privacy, much like the capabilities of FRT. Now the NTIA meetings on FRT are a continuation of the discussion started by Warren and Brandeis in the late 19th century. Other scholars would continue to develop privacy as an academic concept.

Alan Westin (1968) maintained that the origins of privacy go well beyond the 19th century, back to man's animal origins. Westin challenged Mill's conception of privacy as absolute, writing "[T]he individual's desire for privacy is never absolute, since participation in society is an equally powerful desire" (pg. 7). One must carefully consider the balance between the individual's right to privacy and the collective good. Individuals have a vested interest to keep parts of their lives private, and, in many cases, making certain beliefs, attitudes, or preferences known would be deemed offensive or inappropriate. However, the collective good of society often compels individuals to reveal personal information for the safety and benefit of the whole, as seen in the sex

offender registry, vaccination compliance, and jury duty. The balance is not easy to strike.

Government also has an impact on privacy norms (see section 4.3. for further discussion on organizations' need for privacy). For example, totalitarian governments protect their own privacy and surveil their constituents closely. Conversely, democratic forms of government are surveilled by groups and individuals while constituent privacy is highly regarded. Indeed, high importance is placed on privacy as the voter casts his/her ballot. The government requires some information from individuals and groups to function effectively, but the balance depends on social norms and values. For Westin (1968), most American claims to privacy stem from their fierce love of independence and high value on individuality. Mill (1988) supported this notion in *On Liberty*.

For Westin (1968), privacy was not primarily viewed in terms of surveillance, but he certainly was not unaware of surveillance practices. He described surveillance as necessary for social control. He further wrote that surveillance was necessary to protect society. However, surveillance can invade privacy with negative consequences. In fact, just a few short years after Westin's book *Privacy and Freedom* was published, Richard Nixon resigned the presidency following the Watergate scandal. The Democratic National Committee headquarters break-in ultimately started an investigation by authorities. The authorities soon found that Nixon had placed wiretaps on the Democratic offices in an attempt to gain insight into their political strategies (Mellinger, 2011).

FRT poses new challenges to privacy that previously did not exist. The technology can be applied to images retroactively. Many individuals have had their

pictures taken by newspapers, for yearbooks, and other events, the technology can potentially identify individuals found in these dated images. Individuals post numerous photos of themselves to social media where End User License Agreements (EULAs) dictate what happens to user's content and how long data can be retained. Individuals may have their images captured without their knowledge and used for purposes to which they did not consent. FRT has the potential to magnify the potential privacy harms faced in each of these scenarios.

The French philosopher Michel Foucault provided one of the most insightful notions on privacy and surveillance when he discussed Jeremy Bentham's Panopticon (Foucault, 1995). The Panopticon is a prison design where one guard in a central tower would have the ability to watch every single prisoner. At the same time, the prisoners would not be able to see the guard to know if he was actually present or if present who he was monitoring. Foucault (1995) stated, "Visibility is a trap" (p. 200). The individual is seen but cannot observe who is watching him. Foucault stated that this makes the individual "the object of information, never a subject in communication" (p. 200). Furthermore, this asymmetric power imbalance is particularly effective in maintaining social norms. When individuals cannot observe those who are observing them, they must assume they are being watched and conduct themselves according to the norms. The invisibility of the watcher gives him power, "This invisibility is a guarantee of order" (Foucault 1995, p. 200). "Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault 1995, p.201). The principle difference, however, is that citizens are not prisoners. Nevertheless, "[Jeremy] Bentham was surprised that panoptic

institutions could be so light: there were no more bars, no more chains, no more heavy locks" (Foucault 1995, p. 202). In many cases, the presence of cameras seems innocuous, and may make people feel safe, such as in banks and schools. However, if these cameras can all be accessed by the National Security Agency, and there are those who believe this to be the case, the panoptic power would be unnerving. Government surveillance is but one form of privacy invasion.

Private agents are a separate source of surveillance and a challenge to privacy. When in public, there is normally no expectation to privacy; there is also no immediate assumption that one's image will be recorded either. FRT has the ability to turn the assumption of relative anonymity around. As a result, citizens are beginning to take action to protect their relative anonymity in public.[17] Such behavior is an expression of internally motivated resistance.

Foucault wrote that the Panopticon assures the functioning of power. Individuals behave differently when they know they are being observed. In a world where cameras are everywhere, one must ask how this will change individual behavior. It appears that the number of cameras currently available and the limitations of FRT have already changed how people act. Indeed, organizations like Justice Caps provide consumers with hats that project infrared light to interfere with the camera and scuttle face recognizing software (Chibba, 2014). Currently, the technology is somewhat limited for real time use but future actions taken by individuals to protect their faces may be more drastic than wearing ball caps.

[17] Please see section 4.8 for further discussion on protecting relative anonymity from FRT.

In summary, the surveillance power that FRT could impose may have material effects on societal norms. Many aspects of privacy historically conceived are still relevant to life in society today. Scholarship has continued to develop theories of privacy, these are presented next.

4.2. Contemporary Conceptions of Privacy

Amitai Etzioni, former senior advisor to the Carter White House (1999), voiced a communitarian notion of privacy. He noted, as did Daniel Solove (2011), that privacy does not have to be traded for other values or interests. For Etzioni, privacy should be balanced against the good of society. Etzioni stated that privacy interests should be considered when there is a clear and documented threat to privacy, not just a hypothetical fear. Many privacy advocates fear the government and its power of surveillance, but Etzioni noted that privacy enhancing forms of technology, such as encrypted communications, also allow criminals to operate with less fear of prying eyes. This reasoning holds that the value placed on privacy in American society is inefficient for the government and some businesses because it allows negative actions, including criminals to operate, illegal immigrants to persist, and parents to not pay child support. One must consider the costs and benefits privacy provides, and Etzioni contended that privacy must not be placed on such a high pedestal; there must be compromise, especially in the application of FRT.

FRT will have to be analyzed in such a light. At the NTIA meetings members are concerned about the threats FRT poses to privacy. FRT poses significant challenges to privacy. However, FRT also presents the possibility of providing more secure

authentication methods. In the future, individuals will have to balance the potential costs and benefits of the technology when attempting to regulate its usage.

Privacy has recently been balanced against national security in light of recent terror attacks, beginning with the 9/11 attacks (terrorists flew planes into the World Trade Center Towers killing thousands) and continuing with the Boston Marathon bombings (2013) of more recent memory. The technology almost allowed the capture of Dzhokhar Tsarnaev before the bombings took place; the technology was simply not advanced enough at the time. Tsarnaev was spotted on several security cameras, but the images were not of sufficient quality to allow the application of FRT.

Etzioni's (1999) position on privacy is difficult for many who believe in individualism. Communitarians worry about excessive individualism, a value that has high regard in the U.S. However, Etzioni wrote his book before the NSA was tracking citizens, before the IRS targeted specific individuals and groups, and well before the government mandated national health coverage for all Americans all of which reveal private and personal information to the government. Under the Affordable Care Act, U.S. citizens are required to sign up for health coverage or be fined by the IRS. David Lyon (1994) noted the power of the IRS writing, "In the USA the Internal Revenue Service (IRS) is the largest civilian collector of personal data" (p.91). Signing up for this coverage includes divulging one's name, location, income, and a host of other personal information. Solove (2011) rejects an all or nothing privacy surveillance dichotomy and a variety of actions, technologies, and policy changes support his view. In the process of signing up for these services individuals must show some identification credential, such

as a driver's license or passport. Individuals are compelled to have their image captured and utilized by the government and subsequently other private organizations.

Laurence Lessig (2006) challenged how people typically view their Fourth Amendment rights in terms of privacy. Lessig wrote, "Technology enables perpetual and cheap monitoring of behavior" (p. 200). Lessig specifically noted the privacy implications of FRT, describing it as the least intrusive and fastest growing biometric technology. Lessig is more concerned with the fact that on the Internet it is hard to know what constitutes an overly burdensome search, as stated in the Fourth Amendment. It is possible for one's emails and computer to be viewed without one's knowledge, which is almost certainly a breach of privacy. However, is the search of one's computer burdensome if the individual is unaware the search occurred? Government institutions, as well as private institutions, store personal data, which sometimes includes images. Deciding whether or not a search is considered burdensome could have a profound impact on FRT regulation.

For Helen Nissenbaum (2009) privacy should be interpreted in the context in which it is examined. For example, if a person enters the hospital because of an ailment, information may be collected about the patient including weight, blood pressure, pre-existing conditions, and heart rate; information considered to be very personal. It may be critical in this setting for the information to be collected, but in other circumstances inappropriate or annoying in the case of higher insurance premiums. Nissenbaum argued that privacy is not about restricting the flow of information but rather ensuring it flows appropriately based on the context of the situation. Another point that Nissenbaum makes is that there is *information about* individuals and *information associated* with

individuals. It is entirely possible for incorrect conclusions to be reached about a person based on information associated with his or her person. It does not take an elaborate imagination to conclude that images of individuals could be associated with information that may or may not be true about them.

> If a right to privacy is a right to context appropriate flows [many forms of notice are based on context], and not to secrecy or to control over information about oneself, there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information as long as the sharing and withholding conform with the principled conditions prescribed by governing contextual norms. (Nissenbaum 2009, p. 187)

It is unclear how these governing contextual norms are created or what happens when there is unauthorized or malicious use of data. Unfortunately, there are no clear precedents set for the unauthorized or malicious use of data, as well as no definite legal recourse or policies outlining the considerations, legal or penal. For example, it is still unclear if the NSA reading private citizen's emails constitutes a search under the 4th Amendment. These kinds of policy, legal, and penal considerations all provide context which is central to Nissenbaum's argument. Without these considerations, individuals interested in protecting their privacy have a difficult time making informed decisions.

Nissenbaum's argument for contextualizing privacy is predicated on individual choice, which may not always be available. Not only can government institutions like the IRS compel citizens to reveal information, private organizations can as well. Websites like Google and Facebook are notorious for surveilling their users. Many individuals are simply unaware their data are being used and some simply do not care. In situations like

these the context matters very little because users do not have a choice in how their data are used. Many websites end user license agreements (EULAs)[18] are asymmetrical, granting all the negotiating power to the organization. Despite the appealing notion of appropriate flows of information, there are many instances in which the user has no control over how his or her information is used. In such cases, it is left to the organization's self-regulatory policies, primarily the *code of conduct*, to contextualize the provider/consumer relationship in the absence of government regulation or law. Individuals are often presented with an all or nothing proposition and the costs of not participating or utilizing a service are seen as higher than the private information they are forced to reveal.

Daniel Solove (2011) reminded individuals that privacy is not just about keeping information secret and that it is rarely an all or nothing decision. Solove examined the argument many privacy advocates hear, "I have nothing to hide." Privacy is not just about keeping bad information secret. Surveillance and intrusion on privacy can have an impact on free speech, free association, and other First Amendment protections that are a cornerstone of American democracy. Furthermore, traditional refuges of protection, like the Fourth Amendment, will not protect Google searches and personal information from the government and corporations. Solove also argued that the aggregation of seemingly innocent data in small amounts when compiled can create a detailed portrait of an individual. This is the same concern Nissenbaum (2009) articulated when she distinguished information collected about a person and information associated with a

[18] Agreement entered into between the user and the software provider.

person. Multiple captured images of an individual could potentially reveal a great deal of information.

Aggregating user data is easier thanks to the *Assumption of Risk Doctrine*, a legal tort defense. It holds that when a person tells another person a secret they no longer have an expectation that the secret will remain private (Solove, 2011). Pertaining to the Internet, the doctrine does not protect the billing and shipping information provided to businesses like Amazon under the Fourth Amendment. Additionally, all the information Amazon retains concerning past purchases and purchasing preferences is not protected either. Images shared via Facebook could end up in the hands of a third party where the expectation of privacy disappears as well.

Solove (2011) used the metaphor of an envelope to discuss Fourth Amendment protections. The envelope is the material that is protected under the Fourth Amendment from search and seizure. The information on the envelope is in plain view and therefore there is no expectation to privacy, so it is not protected under the Fourth Amendment. However, the information on the envelope is often just as valuable, as it says who the letter is from and where they would like it to be delivered. On the Internet, the envelope is the URL address. The problem is that the URL address, the address protocol for the Internet, contains a lot of information that would otherwise be held in the content of the envelope, e.g. http//www.google.com/what-is-the-formula-for-figuring-the-area-of-a-circle? Using this innocuous example, it is not only easy to see who is sending the message and where they are sending it, but what the content of the message is as well. In this case Marshall McLuhan (1994) seemed to be absolutely correct that the medium is the message (Lessig, 2006).

Lessig (2006) and Solove (2011) alerted the reader to privacy threats on the Internet in terms of the Fourth Amendment in their seminal works. Given the age of the Amendment, it is clear it needs to be updated, or there needs to be a new interpretation of it, to reflect current privacy problems. "Burdensome" searches are context dependent on the Internet. "Reasonable expectations to privacy" also must be viewed in a different light. If citizens are concerned about their privacy, and the NSA scandal suggests they should be, constantly worrying about what one searches or says on the Internet has First Amendment implications, a "chilling effect" or self-censorship similar to Foucault's panopticon effect. As Senator Samuel Ervin explained, "When people fear surveillance, whether it exists or not, when they grow afraid to speak their minds and hearts freely to their government or to anyone else, then we shall cease to be a free society" (as cited in Neier, 1975, p. 12). From the above discussion, it becomes clear that in many instances, American citizens may start considering privacy as a First Amendment issue. Furthermore, Lessig and Solove appear to have been ahead of their time. Their challenges to the Fourth Amendment, about what constitutes a burdensome search, have been substantiated in a class action lawsuit, as stated in the introduction, filed by Senator Rand Paul against the President, NSA, and FBI for collecting metadata about U.S. citizens. A delayed ruling by Judge Richard Leon in the court case *Klayman v. Obama*, ruled the collection of metadata likely unconstitutional. However, the ruling was delayed so the government could file an appeal (Robertson, 2013). The outcome of Paul's legal action or the ruling in *Klayman v. Obama* could have profound implications on surveillance and privacy depending on the wording of the decision.

Privacy is a fundamental human right according to the *Universal Declaration of Human Rights* (Necessary and Proportionate, 2014). The declaration identifies principles determining appropriate times for government to invade an individual's privacy. Of central concern are the concepts of legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communication systems, safeguards for international cooperation, and safeguards against illegitimate access (Necessary and Proportionate, 2014).[19] *Legality* is concerned with the legal authority that exists for a government entity to invade one's privacy and the legal restrictions regarding doing so. *Legitimate aim* specifies that communications can only be surveilled by certain state actors to achieve a legitimate aim. *Necessity* is the principle of gathering only the information that is necessary for the government to build their case. *Adequacy* instructs state actors to use an adequate surveillance level to achieve its goals. *Proportionality* is a check on fairness; the government presumably possesses a far greater ability to invade citizens' privacy than citizens have on investigating the affairs of the government. *Competent judicial authority* implies that impartial judicial authority must be obtained before surveilling communications. *Due process* ensures a fair, impartial, and public hearing to the individual on issues of any human right. *User notification* states that individuals should be notified about the decision to surveil their communications with exceptions only in exigent circumstances. *Transparency* is a concept that involves the government notifying citizens about when they invade citizens privacy, the extent to which they do so, and the tools they have available to them to do so. *Public oversight* ensures legitimacy and

[19] Please see Appendix A for a table detailing the principles further.

transparency. *Integrity of communications* systems ensures that the state cannot compel software or hardware providers to build in surveillance capacities in their products. *Safeguards for international cooperation* suggest that in cases where state laws may intersect with national laws, those with higher individual protections are used. Finally, *safeguards against illegitimate access* suggest that the state legislates against illegal public or private communication surveillance (Necessary and Proportionate, 2014). Notably, the *Universal Declaration of Human Rights* considers privacy in terms of interference which is the position further developed in this dissertation (see section 9.4.), "No one shall be subjected to arbitrary *interference* [emphasis added] with his [sic] privacy…" (Hurley, 2015, p.72). These ideals are included in privacy considerations in the international community.

4.3. Private Organizations' Need for Privacy

Individuals are not the only party concerned when discussing privacy. Companies must carefully guard *proprietary information* that they feel give them a competitive edge. There are many examples of elaborate security measures enacted to keep company recipes, like Coca Cola and Kentucky Fried Chicken (KFC), private. KFC famously kept their fried chicken recipe in a lock box handcuffed to a security consultant as it was moved to a newer more high-tech safe (Schreiner, 2009). This is related to companies utilizing FRT, like Facebook. Facebook would not talk to National Public Radio about its security measures, citing that, "social media companies rarely talk about their internal systems" (Kaste, 2013). The paradox is that companies like Facebook go to great lengths in order to capture their users' personal information, but keep their own proprietary information safeguarded. Fuchs (2011) stated "The use of targeted advertising and

economic surveillance is legally guaranteed by Facebook's privacy policy" (p. 149). Browser cookies, information about pages visited on the Internet, are collected from users by Facebook to sell to advertisers. Users have the ability to opt-out of the cookie tracking feature, but only by viewing the lengthy privacy policy and clicking a link to a separate webpage. A court case like *Facebook Inc. v. Power Ventures Inc*. illustrates the lengths organizations will go to in order to protect their own information, Facebook sued their third party advertiser for violating the company's privacy policy. Companies developing FRT carefully guard their proprietary systems. Certain FRT methods and algorithms work better than others, thus companies developing FRT have a vested interest in keeping these methods private. These various methods provide regulators with additional challenges ensuring that all methods and uses of FRT are equally regulated.

James Coleman (1982) described the increasingly heavy influence that corporations have when legal considerations are discussed. The law considers corporations to be "natural persons," the modern corporation, through limited liability, is treated as an "individual." Nonetheless, the individuals who run the corporations are protected from being personally held responsible for the corporation's liabilities. Coleman described the rapid growth of corporations, as compared to natural persons, and made the case that corporations have skewed the power wielded over natural persons in their favor. For instance, individuals can sue Facebook over privacy violations, but cannot hold Mark Zuckerberg personally responsible for them, nor damage him financially for any violations. Given the valuation of fines the company pays, Facebook, a company valued in the billions, is ostensibly paying a speeding ticket for its violations. Most corporations have vast resources compared to the individual person. Indeed, most

corporations are structured around CEO's or executive boards, made up of natural persons who are in charge of the corporation, who cannot be held liable for their actions on behalf of the corporation. This skewing of power leads to what Coleman called, and titled his book, *The Asymmetric Society*. Regulating companies in a meaningful way may prove challenging as regulations are often predicated on legal definitions which are hazy, at best, in the realm of privacy.

4.4. Legal Conceptions of Privacy

As it was already introduced, the first legal conception of the *right to privacy* was provided by Samuel Warren and Louis Brandeis in 1890 for the *Harvard Law Review* (Belmas and Overbeck, 2012). Through court decision in legal cases, two important privacy concepts have emerged that most U.S. states recognize either by statute or judicial decision. These concepts include that the media may publish newsworthy stories on individuals without their blessing, but a person's name or likeness may not be used for commercial purposes, usually advertising without their express consent (Belmas & Overbeck, 2012).

Most legal cases regarding invasion of privacy are tort actions or civil lawsuits. Courts have identified four distinct privacy torts, including those concerning the publication of embarrassing private facts, physical and technological intrusion, false light, and commercialization (Terilli & Splichal, 2011). Genelle Belmas and Wayne Overbeck (2012) noted that ten states have not recognized the "false light" tort of privacy invasion.

There are several landmark court cases regarding privacy, but one of the most foundational cases is *Katz v. United States* (1967). The ruling in this case considers a

"reasonable expectation to privacy" (Belmas & Overbeck, 2012). Some scholars have found the ruling in Katz troubling as it is tautological; once a court rules there is an expectation to privacy it is used regardless of whether it existed prior to the ruling (Etzioni, 1999). *Griswold v. Connecticut* (1965) is credited with establishing a constitutional right to privacy ruling that forbidding contraceptives violated marital privacy. *Eisenstadt v Baird* (1972) ruled that contraception could be distributed to unmarried couples, widening the scope of privacy. The ruling provided equal protection to both married and unmarried couples and protected the privacy of unmarried couples. *Roe v. Wade* (1973) granted women personal choice on abortion, an action previously controlled by the state. The *NAACP v. Alabama* (1958) ruled that certain organizations do not have to turn over their membership rolls to the state (Terilli & Splichal, 2011). The court ruled in *Department of Justice v. Reporters Committee for Freedom of the Press,* (1989) that public record information can be shielded from disclosure because it exists in a computer database. There seems to be varied opinions on privacy that continue to change based on the most recent rulings.

Despite many of these cases expanding the right to privacy the case that is most central to FRT is *Katz v. United States* (1967). The Katz ruling states that one must have a reasonable expectation of privacy in order for the actions to be considered private. A reasonable expectation exists if a person actually expects privacy and if society as a whole views that expectation as legitimate. In *Vega-Rodriguez v. Puerto Rico Tel. Co.* (1997) the court held that it is implausible for an employee to expect privacy, while toiling in a workplace's open and undifferentiated work area (Hatcher, 2001). Additionally, the court noted that employers have a right to efficiently operate their

business. To facilitate this efficient operation employers have the right to monitor occurrences that happen in plain view. The court also explained that since employers can hire supervisors to monitor work, the business can also use unconcealed video cameras to achieve the same purpose as long as they are not equipped with microphones (Hatcher, 2001). Similarly, in *United States v. Vazquez* (2011), the court ruled that women videotaped entering an abortion clinic had no legitimate expectation to privacy as there were persons consistently exercising their First Amendment rights on a regular basis, as well as the tapings occurring in broad daylight in the open (Hatcher, 2001). Even more controversial the *C'Debaca v. Commonwealth* (1999) case where a man's conviction for using a camera to film under a woman's skirt was reversed, stating she had no expectation of privacy while standing in public fairgrounds (Hatcher, 2001). Similarly in *Thompson v. Johnson Community College* (1997), the court held that employees had a legitimate expectation to privacy in individual locker areas but not in the surrounding locker area. In short, the reasonable expectation to privacy is controversial and without clear consensus (Hatcher, 2001).

In light of the Thompson ruling, FRT then has to reconcile with the plain view principle. According to Mark Tunick (2009), the plain view principle is defined as follows:

> Plain view principle: (1) If information about ourselves (including the fact that we are engaged in an activity or present in a certain location) is in plain view or earshot of anyone engaged in legitimate means of observation, we cannot reasonably expect privacy in that information; (2)otherwise we can. (p. 599)

This principle usually applies to police officers; they are allowed to seize contraband or pertinent evidence that is found in plain sight during an investigation. The plain view principle seems to clearly indicate that individual lives, despite any relative anonymity they may currently enjoy, may be legally monitored in the future with the rise of Closed Circuit Television (CCTV)[20] and FRT. According to Maxine Frith (2004) the average Briton is caught on camera an average of 300 times a day. It is true that Great Britain has a more comprehensive CCTV system than the U.S. but there are an increasing number of cameras in the U.S.

Early scholars of privacy were primarily concerned with invasion of personal privacy by individuals. In addition to individuals intruding on personal privacy, now one must be concerned with surveillance by both the government and corporations. In the aftermath of the terrorist attacks of 9/11, the erosion of privacy rights is now primarily occurring in the name of security. Increased government surveillance is usually couched in the need to keep citizens safe. Corporations also have a vested interest in surveilling those who have been identified as shoplifters. Other intentions of corporate surveillance include using the information to provide customers with more effective advertisements.

4.5. Information Privacy

There have been many ways that privacy has been conceived. One of the most useful categorizations of privacy has been proffered by Smith, Dinev, & Xu. (2011), making the distinction between informational and physical categorizations of privacy.

[20] "Closed Circuit Television (CCTV) is a system where the circuit in which the video is transmitted is closed and all the elements (camera, display monitors, recording devices) are directly connected. This is unlike broadcast television where any receiver that is correctly tuned can pick up and display or store the signal. Such specialized systems are not subject to regulation by the Federal Communications Commission (FCC)" (Brickhouse Security, 2015, par. 1)

Historically, privacy was largely thought of in terms of the physical, "access to an individual and/or the individual's surroundings and private space" (Smith et al., 2011, p. 990). With the ever increasing amount of data being collected about individuals, information privacy became a specific conception of privacy subsumed under the general thought of privacy. Information privacy is concerned with information that can identify a person, also known as *personally identifiable information* (PII).

Yet information privacy is much broader than information that directly identifies someone. During the NTIA FRT meetings, Alessandro Acquisti, professor at Carnegie Mellon University, showed his latest unpublished proof of concept experiment. During the experiment he had students on campus to ask if they would like to have their picture taken and fill out a three page privacy survey. Using the captured image, Acquisti was able to use FRT to find the student's Facebook profile, predict the first five numbers of their social security number, and even find their Match.com dating profile, where pseudonyms are typically used (Acquisti, 2014). Acquisti's experiment utilizes face information, which is tied to an identity that is unknown, and uses the face information to identify the individual. Other information, such as spending habits, routines, places of work, may also be combined to invade personal privacy and potentially result in a positive identification.

With an increased importance placed on informational privacy, and the rise of e-commerce, privacy has also been conceptualized as a commodity. Zizi Papacharissi (2010) contended that people tend to trade privacy for access to services such as online social networks.

> Slowly, privacy defined as the right to be left alone attains the characteristics of a luxury commodity, in that a) it becomes a good inaccessible to most b) it is disproportionately costly to the average individual's ability to acquire and retain it, and c) it becomes associated with social benefits inversely, in that the social cost of not forsaking parts of one's privacy in exchange for information good and services (e–mail account free–of–charge, online social networking) places one at a social disadvantage. (Papacharissi, 2010, par. 6)

From a business standpoint, consumers are constantly offered benefits, coupons, reward cards, and discounts in exchange for personal information. There are also perceived benefits to having more "friends" on social networks as users trade their information and privacy to the networks.

Perhaps the most troubling conception of privacy, and one currently coming to fruition, is a *cognate based conception of privacy* (Smith et al., 2011, p. 993). In a world where privacy seems to be under constant attack, the mind may be considered the last tomb for complete privacy; after all, credible telepathic individuals are hard to come by. Facial expressions, whether knowingly displayed or not, can be captured by FRT and reveal some likely thoughts. If the technology is applied to a video sequence, it can even capture "micro-expressions" which deception experts are only able to spot with limited accuracy in real time (Meyer, 2010). Infrared FRT can also measure the temperature of one's face, which may signal an increased level of interest or even deception. In fact, high-definition thermal imaging is being developed to quickly and accurately identify deception. One study showed deceptive individuals were correctly identified 75% of the

time and those being truthful were correctly categorized 90% of the time (Pavlidis, Eberhardt, & Levine, 2002). This technique was shown to be comparable to polygraph tests, but do not require skilled operators and can be conducted with greater speed. While current uses may primarily be concerned with deception, future uses may reveal other aspects of human cognition.

A popular component of information privacy is privacy conceptualized as *control over one's information*. Control is a popular way of conceptualizing information privacy because it allows privacy to be "operationalized". For instance, regulators can create rules for control such as who is authorized to review information, under what circumstances they are allowed to review information and how sensitive data should be protected. The Edward Snowden revelations have made clear that security agencies are able to learn eclectic bits of information about individuals without their consent, eliminating their ability to control the information. Data breaches at prominent retailers like Target and Home Depot also illustrate why "control" is not a sufficient way to conceptualize privacy.

Conversely, suppose an individual could have total control over his or her information, there is still no guarantee of privacy. The government mandates that one wear clothing while out in public, ensuring some physical privacy. However, there are plenty of people on the Internet who choose to share operations of themselves, record and display child birth, pose nude for art, or engage in pornography for money. Securing control through established rules does not guarantee privacy (Allen, 1999, p. 867).

Despite data breaches and individuals who voluntarily relinquish their privacy, the conceptualization of privacy as control still does not satisfy. Even when assuming

individuals are privacy protective and adequate security to prevent data breaches exists, there are a host of activities in which individuals are compelled to reveal private information. A good example is the Affordable Care Act (ACA). The ACA requires all U.S. citizens to have health insurance, a noble goal. However, because of this individuals are now mandated to reveal personal information in the form of medical history including mental health issues, sexually transmitted diseases, and prior medical procedures or face financial penalty. Beyond this, for an individual to qualify for federal subsidies, they must reveal financial data just as they would when they pay taxes. The government has a power to compel private information from the individual, as well as to compel the individual to remain private by mandating clothes be worn in public, dictating what is and is not private in search and seizures, and enacting non-disclosure agreements. The ability to compel private information from an individual is sometimes necessitated for public safety, but as Solove (2011) so eloquently explained that reason is used far too often.

4.6. What Privacy Is Not

Privacy is often conflated with other terms such as anonymity, secrecy, and confidentiality (Smith et al., 2011, p. 995). These terms are related to privacy in that they often help us be "left alone." While these terms are related to privacy they are distinct from privacy.

Anonymity is often conflated with privacy but is a distinct idea. As Weicher (2006) notes, "Anonymity allows the individual to have a voice without having a name" (p.1). Smith et al. (2011) note, "Anonymity is the ability to conceal a person's identity…" (p. 996). Additionally, one can be completely anonymous or pseudonymous.

Anonymity or pseudonymity exist when a person limits the ways that he or she can be identified; this may help individuals exercise control over their privacy (Smith et al., 2011, p. 996). Anonymity, according to the Common Criteria for Information Technology Security Evaluation standard,[21] is a requirement to ensure privacy along with pseudonymity, unlinkability, and unobservability (Yanes, 2014, p.1). Anonymity is strictly concerned with a person's identity; but the ability to control one's identity is necessary to control one's privacy.

Secrecy is also confused with privacy at times. Secrecy involves concealing information that is likely viewed negatively by the excluded audience (Smith et al., 2011, p. 996). The revelation of secrets can cause a change in the interpretation of an identity by others; secrecy affords opportunities to control how others view an individual. "[P]rivacy, by contrast, protects behavior which is either morally neutral or valued by society" (Smith et al., 2011, p. 996).

Finally, confidentiality is also mistakenly thought of as privacy, however, privacy implies that the individual holds sole discretion on when to release personal information. Confidentiality involves the release of private information, shared with a third party, under controlled circumstances (Smith et al., 2011, p. 996). Therapists and insurance providers often specify what the terms are for the release of confidential information, or what was once private information, before being shared with a third party. Individuals entrusting biometric and other sensitive data to third parties may want to check on the security of data storage before releasing it. Data breaches wreck the controlled release of information that confidentiality specifies. Security ensures that data is not manipulated

[21] Common Criteria is an organization that certifies information technology products for security, efficiency, and cost-effectiveness (Common Criteria, 2015).

or that other parties can use an individual's data for authentication purposes (Smith et al., 2011, p. 996).

4.7. Discussion on Privacy

Privacy lacks a coherent and accepted definition and has been conceptualized in many different ways, all with certain merits. Privacy suffers from numerous conceptions because of the complex relationships between an individual and other entities as well as varied ideological perspectives exacerbated by varied technologies and their ability to monitor, record, and manipulate data. The established social and legal norms allow for a variety of personal privacy preferences to be accommodated. Any discussion of privacy is predicated on how it is initially conceived and valued. For these reasons, individuals may want to think of privacy not as a subjective value with varying levels, or the differences between physical or informational privacy but instead focus on *interference*. No matter the conception of privacy, individuals, for the most part, know when they are interfered with and are free to decide how they would like to handle the interference. By thinking about interference, there exists a concept that allows for the varied conceptions of privacy and the subjective reactions of individuals being interfered with.

Interference sounds similar to the legal concept of *invasion of privacy*. There are certain parallels to the concepts. The basic difference is that invasion of privacy is a legal tort. There are legal guidelines that define when an individual's privacy has been invaded. Depending on the individual, there are exceptions for public figures and celebrities, and the nature of the interference because legal remedies can be pursued. Interference, however, is a broader concept because a host of privacy annoyances occur during daily life that are not illegal. Invasion of privacy only deals with illegal acts,

while interference acknowledges a perceived threat to privacy and allows the law/people to deal with it at the individual level. The concept again allows for subjective valuations, or perceived threats to privacy.

Since there are varied conceptions of privacy and because privacy is dependent upon the individual's need or use of it, focusing on privacy in terms of interference can unite the many conceptions of privacy and also allow for its subjective nature. If one speaks of physical privacy, or the intrusion upon one's person or private space such as a bedroom, the individual is allowed to determine what level of interference they are willing to tolerate.

If one conceives of privacy as a natural human right, interference still works as a concept. If we concede that there are natural rights, those rights have to be defended and fought for. Decisions that intrude upon an individual's privacy, whether a natural right or one outlined legally, are still subject to interference. Tribes of people without formal laws may still have privacy expectations subject to interference. Similarly, in the U.S. there are a number of troubling cases where the court found there was no "expectation of privacy", most notably including the taking of pictures in locker rooms, as in the case of *Thompson v. Johnson Community College*.

When we view privacy as a commodity that can be exchanged for benefits, interference is present as well. Online, users are subject to a variety of advertisements, tracking cookies, and other forms of privacy intruding tools. Some users may be willing to let the interference convince them that trading some privacy for a benefit is fine, while others will view the interference as too intrusive and decline the offer or avoid online commerce altogether. The same goes for brick and mortar retail stores. For example,

Home Depot may solicit shoppers with a rewards card in exchange for a user's private information; some users will undoubtedly perceive the benefits of the rewards card as an advantageous exchange. Privacy centric individuals may be so adverse to interference that they only pay with cash, surrendering very little if any of their privacy. Both individuals, those who value privacy and those who have less value for privacy, may be caught on a security camera which will reveal any of a number of details about the individuals.

No matter how we conceive privacy there will always be interference or unwanted intrusions on our privacy. Thinking of interference allows all conceptions of privacy to be discussed in terms of a common idea. Furthermore, privacy seen in terms of interference allows for the subjective nature of privacy as well. All persons will be subject to interference in regards to their privacy, but how they act after that interference will vary.

4.8. Modes of Resistance to Facial Recognition Technology

An individual's face is an inherently public part of one's identity. Face is how we recognize, remember, judge, and make a host of other evaluations about individuals. To a certain extent, humans enjoy the recognition that their faces provide; it is how we are immediately comfortable engaging with friends and family, how we remember business associates, and how we recall individuals as helpful and friendly or harmful and rude. Society also has the expectation that we will keep our faces public. After all, it would be suspicious, unacceptable, and unlawful, to conduct one's banking business while wearing a ski mask. Since citizens have few options but to keep their face public, this section describes a way citizens can protect their face or resist FRT.

There are companies like *Justicecaps.com* that have conjured up interesting ways for privacy centric individuals to protect their privacy. Their product is a baseball cap with built-in infrared lights on the brim. Humans cannot see infrared light so most individuals perceive the cap as a normal baseball hat. However, infrared light effectively "blinds" cameras, distorting the individual's face to the point of opaqueness to the camera. One limitation to the product, however, is it only works at night (Charlie, 2014). Currently facial hair, hats, and eye glasses can confuse the technology but these obstacles appear to be surmountable as FRT continues to develop.

4.9. Communication Technology Regulation Studies

Communication technology regulation can be tracked all the way back to the telegraph and we find attempts at regulation of communication technologies today, specifically FRT. The first piece of legislation concerning the telegraph was passed in 1845, and it imposed a fine on those who might damage the telegraph poles and wires along public roads (Nonnenmacher, 2001, p. 21). In a sense, this regulation had the effect of promoting and protecting the growth of the new technology. As with most technologies, there are several ways to implement regulation, in this case rival patents were issued, most likely to protect the competitive advantages of rival companies.

As the telegraph continued to spread across the country, new legislation was required by smaller companies. Smaller companies demanded that their messages be transmitted in a "timely fashion" on larger company lines. This in turn revealed information about the messages and senders so that *disclosure protections* were required as well (Nonnenmacher, 2001, p. 22).

The next major communication technological breakthrough was the telephone. This was the first communication network that was designed to be accessed by the entire population (John, 2008, p. 507). The two dominant providers of early telephone services were Western Union (nationwide) and American Bell (regional). Western Union remained mostly unregulated until the New Deal thanks to political lobbying and consumer demands being substantially met, so there was minimal outcry from the public concerning regulation (John, 2008, p. 509). Inventors still enjoyed patent protections for their inventions making it harder for outsiders to enter the market. The patents commanded large sums of money and could be sold. Local municipalities began ownership of some telephone networks to prevent fraud and promote innovation.

While the U.S. was figuring out how best to regulate its own communication industries, the international community gathered for a similar purpose. The International Telecommunications Union (ITU) was created in 1934. The formation of the ITU led to international regulation consistency, such as the International Frequency List for broadcasting. A central consideration of the ITU was the large number of developing countries involved. Developing countries outnumbered developed countries and started to gain traction for assistance by the ITU with technical expertise and funding (Codding, 1994, p. 505). The ITU ensures that telecommunications around the world follow a standardized format and have partnered with the World Trade Organization (WTO) to ensure compliance and fairness with laws and regulations. As the oldest international organization, the ITU is an important historical and current regulator, one that has a majority of developing countries as members. As technology progressed so did regulation.

The next major communication technology development was the radio. The radio has a limited band of frequencies that can be used for transmission. As such this is a scarce resource that could either enjoy private property rights or regulation by the government. The following information comes from R.H. Coase's (1959) *The Federal Communications Commission*. In 1910, the Navy sent a letter to the Senate describing the relative chaos of radio frequencies in the air. Despite bickering in the house and senate licenses were issued by the Secretary of Commerce for radio use outlining certain legal obligations such as wave length. Several other proposals included giving radio authority to the Post Office and the Navy. By the early 1920's broadcast stations began to proliferate. After Secretary of Commerce Hoover refused to accept a license renewal because it interfered with other stations, Intercity Radio Company filed suit. After more suits were filed by various broadcasting companies, the Federal Radio Commission was established and the 'ether' (of air) was deemed property of the people of the United States. This required that offensive content could not be broadcast and that advertisers must be announced by name. The commission, however, did not have the authority to regulate government radio stations. In 1934 the commission's powers were transferred to the Federal Communications Commission which was also responsible for telegraph and telephone businesses (Coase, 1959, p. 7).

A more contemporary example of communication technology regulation is the Internet. The Internet Domain Name System (DNS) is governed by the International Corporation for Assigned Names and Numbers (ICANN). There are other communicative bodies, such as the Internet Governance Forum (IGF). These international groups are representative of the connected world. Globalization among

international bodies has forced national governments to regulate these matters. ICANN does not "run" the Internet, but rather provides technical expertise (Fuller, 2001, par. 11). While ICANN is not intended to run the Internet, it is "dedicated... to coordinate policy through private-sector, bottom-up, consensus-based means" (Fuller, 2001, par. 12).

Bottom up regulation created through consensus is a stark departure from the old top down legislative means previously employed by the government. This departure is likely due to the global nature of communicative technologies, the complexity of the technologies, and the rapid pace at which these technologies are innovated. Instead of legislation, governments have been content to allow *multistakeholder processes* to convene in certain circumstances, often where great technical expertise is needed. Technologies, such as FRT, require such expertise and corporations involved in utilizing the technology are often international in nature.

4.9.1. Theories of Regulation

Regulation is generally thought of in terms of restricting or preventing some action. Regulation can also allow certain behaviors or action to begin but in a more structured way. There are different views of regulation some more narrow and others broader in context. Regulation can be seen as focused control or a set of specific commands that must be obeyed. Regulation has also been viewed as state influence on social or organizational behavior. Finally, regulation can be seen as any form of social or economic influence (Baldwin, Cave, & Lodge, 2012, p. 3).

The seminal question to ask regarding regulation is: "Is regulation needed?" There may be a variety of situations in which regulation is needed or desired. One reason to regulate may be lack of information available to the consumer. Situations arise when

there is very little reward for providing consumers with information, and, Internet based businesses are notorious for having hard to find, jargon filled, and non-negotiable privacy policies and end user license agreements. In fact, *unequal bargaining power* is another reason regulation may be needed (Baldwin, Cave, & Lodge, 2012, p. 20).[22]

Another situation that may call for regulation is when services or opportunities to individuals are offered *without consistency*. Perhaps the most famous regulatory example to encourage fairness and consistency of opportunities would be Affirmative Action policies. Concerns have arisen that FRT could be used in a manner called *facial profiling* to offer certain opportunities to one race or gender in a discriminatory fashion.

Regulation need not always be viewed as hampering an activity, but permitting activities as well. For example, the need for regulation can be seen as good for the public in instances of security. FRT has been deployed at airports to enhance security and allow for accurate identification, subsequently allowing passengers to more conveniently navigate airport security. Regulation is often created because it is in the public's best interest.

Regulation occurs due to market failures, specifically concerning examples previously mentioned. However, regulation can also fail and create odd externalities in the market. Affirmative Action policies were created to enforce fair hiring practices for minorities. Currently, there are some in the minority community who feel that the laws hold back minorities, while others view them as a crutch that leads to stigmatization

[22] FRT was famously deployed at the 2001 Super Bowl without notice to the fans in attendance (McCullagh, 2001). Concerns have been expressed that deployment of FRT without notice or consent may be problematic.

(Navarette, 2014). Choosing when regulation is needed is a consideration that requires careful evaluation.

As shown, regulation should be chosen when there are market failures, but regulation can also have negative effects as well. Creating regulation that produces maximum benefit and minimal problems is the optimal goal. Then again, what constitutes "good" regulation? Baldwin, Cave, and Lodge (2012) have created the following five questions to determine if regulation is worthy of support. Is the action or regime supported by legislative authority? Is there an appropriate scheme of accountability? Are procedures fair, accessible, and open? Is the regulator acting with sufficient expertise? Is the action or regime efficient? (p. 27). Regulation authorized by the government is often seen as legitimate. However, regulation can be broadly worded with a good deal of latitude in how the regulation is actually implemented. This results in a need for an accountable group implementing the regulation. Regulation needs to treat individuals fairly and allow for their participation. Expertise is often a central part of creating regulation. Often technologies are complicated, and the various ways they impact the market need to be considered. Finally, a lack of bureaucracy and red tape leading to increased efficiency is desirable.

At this point regulatory regime needs to be defined as it is a central theme to this dissertation. David Levi-Faur (2011) writes that regulatory regimes encompass the actors making decisions as well as the norms and mechanisms used to make regulatory decisions. Levi-Faur (2011) also notes "an increasingly popular concept in the study of regulation and regulatory reform, which probably attests to the emergence and consolidation of systemic rulemaking to govern different issues, arenas, and sectors" (p.

20). Regulatory regimes are the norms and rules for making decisions as various interests converge around a specific issue or group of issues.

How does regulation arise? There are many reasons and models for the development of regulation, but one explanation most closely follows the MSH meetings on FRT. The 'Power of Ideas' explanation closely resembles the MSH meeting format. This explanation places primary importance on conversation and deliberation (Baldwin, Cave, & Lodge, 2012, p. 49). "This 'argumentative turn' follows Habermas and points to the importance of interpretative communities that are supposed to deliberate and come to a shared understanding regarding the regulatory issues and processes" (Baldwin, et al., 2012, p. 51). During conversations and deliberation knowledge is gained by the participants and the learning that takes place is a tangible outcome of the process.

There are various strategies that regulators can pursue in order to ensure that the regulation is enforced. Some strategies are punitive, incentive based, market based, or pursued by other means. The enforcement of the voluntary code of conduct will be done under the Section 5 authority of the FTC to enforce against unfair or deceptive practices. This most closely resembles the command and control strategy where standards are enforced by threat of criminal sanctions, something the FTC can pursue. Command and Control strategies are seen as forceful by the public because they are backed by the power of the state. This, in turn, provides additional confidence to the public that the regulation will be enforced aggressively (Baldwin et al., 2012, p. 107). Unfortunately, not all members of the public will be able to agree that the regulation is in their best interest. Additionally, "Command methods may also lack force when court sanctioning is weak and the rules, as a result, fail to pose a credible deterrent" (Baldwin et al., 2012, p. 110).

4.9.2. Soft Versus Hard Regulation

The result of the MSH process is a *voluntary* code of conduct that organizations can agree to abide by and will be enforced by the FTC. This code of conduct can be seen as a form of 'soft' regulation. Keith Sisson and Paul Marginson (2001) noted that codes of conduct can be viewed as soft regulation but there is little agreement on what defines soft regulation or what 'hard' regulation is, for that matter. Sisson and Marginson (2001, p. 4) provide useful comparisons between soft and hard regulation. They note that soft regulation is concerned with general principles where as hard regulation deals with obligations. Additionally, soft regulation deals with obligations it tends to prescribe limited provisions, whereas hard regulation sets standard provisions. Finally, soft regulation may continue to be negotiated when hard regulation is seen as finished. As stated previously, many of the companies involved with FRT are international in nature. Soft regulation, because it is often less rigid than hard regulation, is seen by the participants as a productive way to standardize the technology. Additionally, hard regulation has a one size fits all nature that may not apply to the various uses of FRT, such as validation, identification, and demographic uses.

4.9.3. Regulation of Technology

Technology and regulation are often represented as antithetical (Wiener, 2004). Regulation can be seen as unnecessary bureaucratic requirements that slow the development of technology and stifle innovation. In fact, this view is witnessed in the multistakeholder meetings facilitated by the NTIA. The goal of the meetings is to develop a voluntary code of conduct as a mode of self-regulation instead of allowing the development of governmental regulation of FRT.

A growing body of academic literature has been exploring the false dichotomy that exists between technology and regulation. Jonathan Wiener (2004) explored concepts of technology and regulation noting that technology symbolizes progress and capitalism while regulation symbolizes bureaucracy and growth prohibition. Nevertheless, the regulation of technology does not have to be seen as inhibiting development or innovation. Some forms of regulation can actually promote the growth and innovation of technology. For instance, it has been proposed, but not yet regulated, that FRT be more effective at lower pixel rates thus increasing the accuracy of the technology.

In attempting to explain what justifies the developing regulatory regimes for new technologies some authors point to the fact that those technologies are so ubiquitous and essential that using the technology becomes compulsory. Jennifer Chandler (2012) wrote that competition between individuals and organizations drives the adoption and enhancement of technology. These individuals or organizations become dependent on the technology because the costs of discontinuation are too high. The multitude of users establishes a need for a system of rules which prevents or punishes users through negative social consequences, while also rewarding them which leads to positive social benefits (Chandler, 2012). According to Jennifer Chandler (2007), courts also play a role in regulating technology through the establishment of property rights or rights to damages, which shape the regulatory landscape. Individuals, through tort claims, can bring legal action against those who invade property rights. Technologies can be impacted by the courts when they award damages in cases.

Leo Marx (1994) found that technology is easier to view in a positive light because the consequences of new technologies often escape us. Marx (1994) wrote of the public pessimism surrounding technology only after disasters such as Chernobyl, the Vietnam War, and various oil spills. Some individuals already hold this pessimistic position on FRT because of its invasive nature. Balancing the concerns of those who are pessimistic about FRT with those who are excited about its potential will be necessary to ensure responsible regulation that allows for innovation while protecting citizens.

4.10. Discussion on the Application of Regulation Theories

Chandler (2012) discussed ubiquitous and obligatory technologies, and FRT has the potential to become one. Online identity theft has become an issue of international importance in the last decade, and FRT, as well as other biometric identifiers for authentication, are offered as a possible way to slow the rate of, or prevent altogether, identity theft. If this is the case, then future societies will depend on FRT to authenticate bank transactions, rather than rely on simple pin numbers. Pin numbers will be seen as a weak form of authentication and a dangerous way of performing critical transactions. Consequently, how the enormous amount of FRT data is going to be gathered, stored, and used, specifically by whom, becomes an issue of great social importance. The public debate, as contained by the multistakeholder (MSH) meetings convened by the NTIA, is directed toward developing the foundations of a regulatory regime for FRT, and this debate will contribute to the case study for the current research.

As photos become stored for authentication and security purposes issues of property rights are likely to arise. A recent example of these disputes is the so called "Cute Convict." According to Gabe Gutierrez and Scott Stump (2014), Megan Simmons,

who was arrested for DUI, is suing *InstantCheckmate.com* over the public use of her mug shot without her permission. The ruling will have legal implications over the use of photos and may have implications for FRT over the scanning of public photos. For instance, if the court agrees with Ms. Simmons, ruling that she has a property right to her photo, then other organizations may have to change their practices as a result. Conversely, they may rule that the photo was public and the company had a right to use it, which could make other companies more aggressive in searching the Internet for photos.

4.11. Multistakeholder Collaborative Process

Before presenting the multistakeholder format a brief history of organizational studies is necessary to provide context to the process. One of the first writings on organizational studies comes from Adam Smith and the *Wealth of Nations* where he described the division of labor (Hatch, 2006, p. 27). Following this work is Karl Marx who wrote of labor and capital. Capital theorists began with theories of labor only later to focus on management. For example, Ėmile Durkheim was concerned about the specialization of labor while Max Weber focused on the origins of managerial authority (Hatch, 2006, p. 30).

Scientific management was born from the work of Frederick Taylor. Taylor studied the most efficient way to accomplish a task. Taylor's scientific approach to labor worked to achieve maximum profit for organizations (as cited in Hatch, 2006, p. 32). Moving beyond such singular pursuits theorists started writing about systems theories and challenging the single best way to organize labor. For example, in Total Quality Management (TQM) the worker was seen as the person most knowledgeable on how to

improve an operation or an aspect of the operation. This singular input could have positive material consequences for a business's output, "Quality is not improved by after-the-fact inspection but by control over the production process as it happens" (Sashkin, 1993, p. 11). Soon organizations and the tasks they are charged with were recognized for their increasingly complex demands and organization. In turn, complex demands and the interaction of multiple interested entities led to the rise and increased popularity of the MSH format for solving such issues (Hintz & Milan, 2014).

The NTIA has been tasked with regulating a complex and nascent technology in FRT. In many ways the MSH model is the practice of participatory democracy, "Their power [practice of participatory democracy] derives from respect for their processes the openness, the flexibility, and the ability for all voices that can credibly articulate their positions to be heard and the quality of their outputs, which are intended to represent broad stakeholder consensus" (Waz and Weizer 2012, p. 336). Similarly, David Held (2006) described deliberative democracy as those who, "Champion…informed debate, [and] the public use of reason" (Held, 2006, p. 232). The NTIA meetings have involved informed debate and reasoning to pursue participant goals. Held (2006) continued,

> The major contention of deliberative democrats is to bid farewell to any notion of fixed preferences and to replace them with a learning process in and through which people come to terms with the range of issues they need to understand in order to hold a sound and reasonable political judgment. (p. 233)

The voluntary codes of conduct created at the NTIA are, in part, the result of a firm's general resistance to "excessive government laws and regulations," (Kolk, Tulder, &

Welters, 1999, p. 152). These voluntary codes are a "soft" form of regulation rather than the top down command and control style regulation that could be enacted by Congress or other governing bodies. Soft regulation has been employed to achieve a balance between consumer protection and the need to innovate the technology.

The multistakeholder process is the format the White House (2012) has required the NTIA meetings to follow. This format allows for non-governmental organizations (NGOs), which possess a better understanding of the complex technology to meet and garner greater legitimacy concerning the chosen policy (Antonova, 2011). Furthermore, "[T]he open and inclusive stakeholder process leads to accumulation of intellectual capital, development of relational infrastructure. " (Antonova, 2011, p. 426). This also leads to shared consciousness among stakeholders.

The MSH process is a collaborative one. Collaboration "is a process through which parties who see different aspects of a problem can constructively explore their differences and search for solutions that go beyond their own limited vision of what is possible" (Gray, 1989, p. 5). The goal of collaborating is to gather stakeholders together in order to gain a more complete and detailed understanding of the problem. Stakeholders bring unique knowledge, experience, and views to the process which adds to the formulation of the problem, as well as the solution.

When diverse stakeholders decide on the problem and how it is going to be solved, there will most likely be conflict. Collaboration can help resolve conflict: "Collaboration transforms adversarial interaction into a mutual search for information and for solutions that allow all those participating to insure that their interests are represented" (Gray, 1989, p. 7). Conflict does more than just ensure that stakeholders'

interests are represented; in fact, conflict often leads to unforeseen opportunities: "differences are often the source of immense creative potential. Learning to harness that potential is what collaboration is all about" (Gray, 1989, p. 11). Oftentimes, parties are only willing to collaborate if they can envision a positive outcome as the result. Remove the possibility of a positive outcome and parties may decide to withdraw or to do their best to disrupt the process.

Barbara Gray (1989), who is a prominent author on the theory of collaboration, defined the criteria for problems that are best solved by collaboration:

- The problems are ill defined, or there is disagreement about how they should be defined.
- Several stakeholders have a vested interest in the problems and are interdependent.
- These stakeholders are not necessarily identified a priori or organized in any systematic way.
- There may be a disparity of power and/or resources for dealing with the problems among the stakeholders.
- Stakeholders may have different levels of expertise and different access to information about the problems.
- The problems are often characterized by technical complexity and scientific uncertainty.
- Differing perspectives on the problems often lead to adversarial relationships among the stakeholders.

- Incremental or unilateral efforts to deal with the problems typically produce less than satisfactory solutions.
- Existing processes for addressing the problems have proved insufficient and may even exacerbate them (p. 10)

The problems identified on Gray's list are consistent with the problems surrounding the regulation of FRT. The technology is nascent, and there is often disagreement concerning the technology's capabilities and limitations. Also, many vendors, technologists, academics, and advocates have a vested interest in the technology.

Gray (1989) noted that collaboration usually proceeds in three phases. The first phase is "problem setting." This phase is marked by identifying a common understanding of the problem, a willingness to collaborate, identification of legitimate stakeholders, the role of the convener, and identification of resources (Gray, 1989, p. 57). The second phase is "direction setting." In direction setting, rules for stakeholders are set, an agenda is created, subgroups may be created, information is found, options are explored, and an agreement is reached (Gray, 1989, p. 57). The third phase is "implementation." This phase is marked by dealing with constituencies, building external support, and ensuring compliance of the agreement (Gray, 1989, p. 57). Each phase faces specific challenges that have to be met and collaboration can increase the success rate with which those challenges are met.

Collaboration is one of the central focuses of the MSH process, but how do rulemaking standards measure up to other processes? Would the rules have higher standards if they were developed under a different process? The stated outcome of the NTIA for this process is to create voluntary codes of conduct (rules) for commercial uses

of FRT. Fransen & Kolk (2007), suggested that the rules created at multi-stakeholder processes are more demanding (rigorous and elaborate) than those drawn up by non-governmental organizations (NGOs) and those of business associations (p.3). This indicates that even though the codes of conduct, created by the NTIA, are voluntary, they still have a good chance of setting high standards for consumer privacy.

Even though the expectations may be high, research also suggests cautious optimism as voluntary codes are sometimes adopted by only a few organizations (Kolk, et al., 1999, p.144). In fact, the last NTIA directed multi-stakeholder process, for mobile app transparency (2012), resulted in very limited adoption. Complicating matters, "Specificity and compliance mechanisms are seen as the crucial elements which determine the likelihood of compliance" (Kolk, et al., 1999, p. 147). This suggests that if codes are too strict or prescriptive in nature they may not be adopted by companies.

One must also be mindful of stakeholder motivations for creating a code of conduct. Ostensibly, this process has the goal of protecting consumer privacy. Kolk et al., (1999) noted that firms involved in the process may have ulterior motives, such as influencing regulators or customers (p. 151). The content of the voluntary codes of conduct determine whether companies will adopt them, how companies are regulated, whether consumers believe they are legitimate, and the level of consumer privacy protection they provide. Businesses typically try to avoid regulation; codes of conduct may be created to prevent mandatory regulation (Kolk et al., 1999, p. 152). Codes that are specific in nature allow them to be more easily measured. This clarity also encourages compliance by businesses.

4.11.1. Multistakeholder Processes and Shared Power

Bringing together diverse stakeholders who have a willingness to collaborate on issues has many benefits as explained above. One should not assume that all stakeholders possess the same amount of power to influence the process. Nigel Roome and Frank Wijen (2006) contended "that influence is the equivalent of power, as power that is not exercised is insignificant, and influence is a materialization of power" (p. 3). Ian Mitroff (1983) described stakeholder properties, such as resources, special knowledge or skills, relationships with other stakeholders, and the purpose or beliefs that the stakeholder has, as impactful on the stakeholder's power in the process (p. 36). With regard to the MSH process on FRT, specialized knowledge and skill are critical factors when considering stakeholder influence. As stated earlier, this technology is in its early stages of development and its capabilities are still uncertain, making regulating the technology challenging.

Each stakeholder exercises a certain amount of power in a limited capacity. Given the nature of MSH processes, a consensus must eventually be reached or the process will fall apart. For productive outcomes to be achieved stakeholders will have to collaborate and negotiate until there is agreement. If stakeholders are unwilling to reach consensus they may do their best to undermine the process, since they are still legitimate stakeholders until they choose to no longer participate. Depending on the stakeholder and their source(s) of power, not participating can impact the process in significant ways.

The MSH process is open, inviting diverse groups with diverse ideas that lead to stimulating conversations; however, that can also make the process lengthy. The more a stakeholder participates and speaks up during the process the more they can potentially

impact it. Even though all stakeholders have been encouraged to participate by the moderator, there are different forms of participation, including nonparticipation. Nonparticipation may invite suspicion from other participants. Another way that stakeholders exercise influence is by the "power of the pen." Stakeholders have been asked to join groups whose issues are most meaningful to them; they are then asked to produce draft language about the issue to be discussed with the entire group of stakeholders. Most of what is decided by the large group is dependent upon the smaller group's draft language.

4.11.2. MultiStakeholder Outcomes

Some outcomes of the MSH process, such as codes of conduct, are tangible and easy to recognize. Other outcomes from the process are intangible and hard to estimate and appreciate, including the knowledge acquired by stakeholders through the learning process (Antonova, 2011). Tangible and intangible outcomes are important to both the process and stakeholders as they move to other MSH meetings or revisit the original.

4.11.3. Learning

The learning that takes place at the forum is a facilitative part of the process and also an outcome of the MSH process. The learning process is affected by several factors, including "organizational antecedents, market positioning, technology, access to stakeholder networks, sensitivity to multiple perspectives, and ability to facilitate inputs from different internal and external stakeholders" (Roome & Wijen, 2006, p.6). The material presented is most likely influenced by the views and beliefs held by the stakeholder.

James March (1991) described two forms of organizational learning: exploration and exploitive. Exploration learning seeks to find new information which may include experimentation. Exploration is also described as "double loop" (Roome & Wijen, 2006, p. 7). Double loop learning "…provid[es] feedback and more effective decision making" (Argyris, 1976, p. 363). Exploitive learning, on the other hand, seeks to take advantage of known information and may include increasing efficiency or enhancing execution of something (March, 1991, p. 71). Unlike exploration, exploitive learning is described as a "single loop" or an action created as a result of a known theory (Argyris, 1976, p. 363).

Due to the emerging nature of FRT, most of the learning taking place at the forum is exploration. The stakeholders are discovering ways to protect consumers while also providing business entities the ability to continue innovating. This type of learning also provides the flexibility that regulators need to balance consumer privacy with business interests.

Learning occurs in three stages acquisition, sharing, and storage (Roome & Wijen, 2006, p.8). In the explored FRT process, but especially at the beginning, various technical experts were brought in so stakeholders could be exposed to different sources of expertise and create shared meaning for later discussions. This acquisition was marked by experts reporting on various experiments to demonstrate the technology's capabilities, accuracy, and uses.

Sharing information has been an ongoing process, and without a clear delineation at the forum. Stakeholders share information to solve larger problems (Roome & Wijen, 2006, p.8). As the process continues, stakeholders have been counted on for their various expertise; for example, lawyers have been drawn upon for legal advice, biometrics

experts have been consulted, and regulators have been brought in to discuss the scope of the code of conduct. Information storage is used for shared meaning and later problem solving; one form of information storage may include documents created based on consensus.

As previously discussed not all information is shared. Corporations may want to protect a competitive advantage and thus be reluctant to share information, or have new uses of the technology that they do not want to discuss. Others may be reluctant to discuss information as they feel it may be of advantage to them during the process.

The learning process is not limited to technical knowledge. Stakeholders may learn new social skills, enabling them to participate more effectively at the MSH forum (Turcotte & Pasquero, 2011, p. 457). Stakeholders learn where their views may be most appreciated, as well as where their organization and others stand on an issue. This social aspect of the learning process should not be discounted because it can enhance cooperation and produce tangible outcomes and partnerships (Turcotte & Pasquero, 2011, p. 457).

4.11.4. Consensus

According to Gray (1989) and Turcotte and Pasquero(2001) consensus is the expected outcome of MSH processes. These processes are convened in order for stakeholders to form consensus around specified issues in an effort to further or solve issues. Turcotte and Pasquero (2001) note that consensus may be easier to achieve on broad topics or umbrella issues. The details or specific mandates may be areas where consensus is harder to achieve or stakeholders may be unclear on what is to be agreed upon. Since MSH processes are generally convened to solve complex problems, goals

may be quickly agreed upon, but how to achieve those goals may be more difficult to agree upon. Even when appropriate solutions can be agreed upon, stakeholders may lack the resources necessary to carry them out, thus consensus must be considered in a multifaceted way. There are goals and then there are the means of achieving those goals both of which need to reach consensus to be carried out. As stated previously, the learning process may facilitate consensus on issues in multiple ways.

4.11.5. Capacity Building

Capacity building has been defined in terms of MSH processes as "the accumulation of intellectual capital, skills, and competencies; development of a relational infrastructure for the domain, as represented by stakeholder constituencies, collaborative alliances/dynamic coalitions, and network communities; and emergence of a common global consciousness" (Antonova, 2011, p. 436). These aspects of capacity building lead to innovative solutions, also known as collaborative advantage (Antonova, 2011, p. 427).

4.12. Discussion on Multistakeholder Theories Application

Anticipated uses of MSH theories include strategic silence by stakeholders to influence the process. For example, Facebook and Google have had representation in the current MSH process but had not participated directly even after repeated requests to do so. Facebook, however, did eventually contribute to the process. Why would two of the most reputable companies in the space refuse to participate for so long? Will the legitimacy of the code of conduct be enhanced or tarnished if they choose not to agree to and abide by it?

It is expected that stakeholders will exhibit different amounts of power based on their resources and relative distance to the physical meeting location. For example, there

are three main ways to follow the MSH process on FRT: telephone, webcast, and physical presence. Those who are physically present at the meetings wield the most power as they are able to speak up at almost any time during the process. Stakeholders who participate via telephone wait until the operator puts them into the question and answer mode. Stakeholders who participate via the webcast may be able to e-mail, but this was not revealed during the observed meetings. As the venue for the process has not changed, those stakeholders residing in the Washington D.C. area have the inherent advantage of easily attending the meetings, increasing their potential influence or power.

The learning process can have material outcomes on MSH processes. During this process, competing ideas often led to different learning outcomes. Both privacy advocates and industry technologists have been invited to make presentations illustrating technology usage, necessary data, and technological capabilities. These presentations have ultimately resulted in different conclusions. Who is to be believed about whether a series of numbers can be reverse engineered into an image? What are the present limitations of the technology? Answers to these questions are likely to have material regulatory outcomes.

4.13. Summary

This project is informed by the social constructivist view that FRT can be regulated in meaningful ways. The process is a rejection of the technological determinist view that the technology will change the ways humans interact. The process and its outcome clearly demonstrate that individuals not only control appropriate uses of the technology, but also the meaningful limits on its usage.

Each of the three theoretical fields presented above are complex and multifaceted on their own. These fields have converged in this project to improve understanding about the developing regulatory regime for FRT and the privacy implications that result. The MSH format has been employed to help develop "soft" regulation for FRT in the form of a voluntary code of conduct.

Given the complexity of privacy views and the international nature of many of the companies likely to be affected by this regulation, the MSH format plays an important role in ensuring the presentation of diverse views and opinions. The nature of the voluntary code ensures that the technology can continue to develop while providing consumers with confidence that their privacy is being protected.

How privacy is constructed at the MSH meetings is likely to have material effects on the regulation created. Privacy views present at the MSH meetings are anticipated to include information, physical, cognitive, and privacy conceived of as a commodity. Conceptions that have disproportionate representation through the process may have enhanced regulatory safeguards. Conversely, conceptions of privacy not represented at the process, or minimally represented, may lack meaningful regulatory protections. The safeguards developed out of the MSH process represent the only meaningful limits currently placed on the technology and its future utilization.

CHAPTER 5

METHODS

This chapter provides insight into the philosophical paradigm employed throughout this project. Explanations are provided as to why particular research methods were chosen as well as their anticipated contributions to the project. All research methods have shortcomings, and these will be discussed as well.

5.1. Philosophical Underpinnings

Much of this research subscribes to a social constructivist worldview applied to technology. Following this paradigm is the notion that individuals ascribe meaning to events and past experiences which impact their interactions (Creswell, 2009). Under this paradigm meaning is created through discussion and interactions with others. This is precisely what the multistakeholder process for facial recognition technology seeks to do; it seeks to create shared meaning among the stakeholders to produce a voluntary code of conduct for commercial uses of FRT. Much of this research focuses on the interaction between government entities, individuals, companies, and industry representatives, to build consensus on legitimate FRT uses.

Important to the social constructivist paradigm is history and culture. Many Americans strongly identify with individualism and are skeptical of too much government intervention in their lives. Multistakeholderism is a way to create governing principles without the heavy hand of government, giving citizens a chance to directly

express their concerns. Current events tend to shape human experiences, and the developmental code of conduct is occurring in the context of a post-Snowden world where Americans are more aware of privacy violations. As this is the reality, citizens may be more sensitive to issues that FRT creates than they were previously. Continually incorporating these varied perspectives is important in providing the most holistic explanations possible for this dissertation.

The varied perspectives represented at the meetings may demand a social constructivist paradigm. The complexity of views, participants, and positions cannot be adequately covered by more limited paradigms. Technologists who develop, use, and promote the technology have been responsible for educating participants on the capabilities of FRT. However, some technologists who previously supported robust growth of the technology have reconsidered and now advocate for more limited uses (Opam, 2014). This is just one dynamic that could be covered between privacy advocates, technologists, foreign government representatives, businesses, trade associations, private citizens, and physically present participants versus phone or webcast participants.

The complexity of the meetings is not just dictated by the participants and their advocatory views, but also values and controversial scientific conclusions. Privacy lacks a definition that can be agreed upon in the academic community, and amongst citizens in general. Since privacy lacks a clear definition, it has been conceptualized in many different ways. A participant's conception of privacy and its subjective value makes the issue very complex. Furthermore, these meetings are not only regulating the current uses of FRT but also potential future uses. What the technology will be capable of in the

future is uncertain, but can be determined through regulation. For instance, there is one method of facial recognition called face "hallucination" where the technology takes poorly pixilated images and begins to "guess" what the face looks like by comparing it to millions of other known images. Whether or not this is a viable method of facial recognition remains to be seen, but there are implications brought forth by this method that may not be present in current methods. Social constructivism is best suited to encapsulate the varied perspectives and participants as well as the highly complex nature of the meetings and the interactions within.

In contrast, positivist approaches, derived from scientific and observable knowledge, fail to grasp the complex issues that FRT raises. Essentialism, having certain base qualities, may seem like an appropriate approach to the technology because it is usually seen as being used for identification but there are multi-model methods of conducting FR and the debates at the NTIA meetings are too complex. It is true that stakeholders have ideas they would like to see incorporated or not incorporated into a voluntary code of conduct, but the creation of the code evolves through negotiations and stakeholders have to compromise their positions in order to broker a deal that companies will actually agree to. Other philosophical paradigms also fail to adequately explain the dissertation's aims.

Rationalistic approaches are not useful to codes of conduct that regard privacy because there is no academic consensus defining privacy. Furthermore, an individual's need for privacy is subjective. Even if consistent expectations of privacy existed, the government may continue to invade individual's privacy through taxes or privacy mandates, such as requiring clothing in public.

Technological determinism is a popular reductionist viewpoint that believes technology is an independent force which has left society in its servitude (Alvarez, 1999, p. 405). This project fundamentally refutes the idea of technological determinism. The whole point of the MSH meetings on FRT is to directly impact technology by "allowing" it to impact society in beneficial ways. If the premise of technological determinism is taken seriously, then there is no need to attempt to regulate the technology. The social constructivist view and the MSH meetings allow for normative values, such as privacy, to be embedded in the deployed formats of FRT. As David Nye (2006) stated: "Rather than assuming that technologies are deterministic, it appears more reasonable to assume that cultural choices shape their uses" (p. 21).

How the challenges of FRT are framed during the MSH meetings will largely determine the regulatory regime for the technology. For instance, stakeholders have been informed that they are to focus on commercial uses of the technology and that government uses are outside the scope of the group's work. Given these limitations, the group will only be able to regulate the technology in limited ways, further amplifying the appropriateness of the social constructivist paradigm in this research project.

5.2. Research Design

The research design for this project is that of a case study. The FRT debate, convened by the NTIA, constitutes an important case of developing a regulatory policy regarding privacy and technology development. These MSH meetings are the first U.S. attempt at regulating FRT. The case study design has been chosen specifically in relation to these factors.

Robert Yin (1984) defined a case study as a research approach that allows for investigating "a contemporary phenomenon within its real-life context, when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used" (p. 23). He specified that the case study is the most appropriate research design for studies, where "how" or "why" questions are the primary concern of the researcher; he also suggested this format for studying current phenomena on which the researcher has little or no control.

Similarly, Peter Swanborn (2010) described a case study as a research approach that focuses on one or only a handful of events, but draws data from a variety of sources, including documents and observation. Furthermore, Swanborn (2010) states that case studies are appropriate for answering broad research questions by tracking how a process develops. This research approach allows for comparisons to be made between the positions of the various stakeholders. These comparisons will underscore outcomes from NTIA meetings. For instance, heavy privacy protections may imply that NGOs, such as the Center for Digital Democracy, had a strong influence in the meetings. Conversely, if rapid innovation is favored, commercial organizations may have had a profound impact on the debate. The case study design was chosen for this project as it helps answer "why" questions, as defined by Yin (1984). The discourse analysis of meeting transcripts, research interviews, and documents collected will help answer questions of why particular provisions and considerations have been included in the code of conduct.

The case study design is not without its critics or controversy. One criticism leveled against the design is that researchers may allow their views to influence the findings and conclusions (Yin, 1984). Triangulation of multiple methods of data

gathering, interviews with participants, participant observation, and meeting transcripts are employed to try to alleviate this concern.

The case study design is suited to the project given the complexity of the MSH meetings on FRT. As "a research endeavor, the case study contributes uniquely to our knowledge of individual, organizational, social, and political phenomena" (Yin, 1989, p. 14). The NTIA MSH process on FRT is a politically directed and motivated process mandated in President Obama's CPBR. A wide variety of organizational interests are represented and advocated for during the process which will likely affect individual consumers. Given these diverse situations and the potential for profound social impact, the case study is the most appropriate research design for this project.

This study proposes the use of three qualitative methods for *data gathering*: semi-structured interviews, participant observation, and document analysis of meeting transcripts. Triangulation, according to Donald Treadwell (2011), is the use of multiple methods so that the researcher can have greater confidence in his or her findings. Kathleen DeWalt and Billie DeWalt (2011) believed that the use of multiple methods, with their own strengths and limitations, could provide cross validation of conclusions and thus to help assess the overall validity of findings.

5.3. Stages of Research

5.3.1. Data Collection

The NTIA meetings started on February 6, 2014. The debates at the meetings were recorded via Replay Video Capture 7 software and a Sony IC recorder, a digital recording device, for redundancy. The software records the NTIA webcasts in .mpg

format, which is accepted by the HyperRESEARCH platform, the data analysis software platform.

5.3.2. Participant Observation

Participant observation is a method to collect data in settings where researchers observe and/or take part in the activities of the study participants (DeWalt and DeWalt, 2011). Participant observation provides context for data, which supports the process of identifying potential interviewees, formulating questions for the semi-structured interviews, and detecting power structures in the MSH collaborative process. According to DeWalt and DeWalt (2011), participant observation has several advantages, including enhancing the quality of data obtained during fieldwork, helping to interpret said data, and aiding in the formulation of new research questions based on the observations made in the field.

This researcher traveled to Washington D.C. in order to observe the meeting that occurred on June 24, 2014. This observation provided important context for how the stakeholders actually experience the meetings. During this trip, the researcher learned a significant amount about the venue and the meeting's intricacies which could not be experienced through the webcast alone. For example, many more individuals are in the room than can be observed via the webcast. This has provided greater context and insight for this research.

Meeting notifications are posted on the NTIA website as well as emailed out to participants and viewers who signed up for the email list serve for the process. During the meetings participants were observed in regards to their attendance and participation during the meetings. When individuals participated in the meetings, their positions on

specific issues were noted as well as their reasoning for having that position in contrast to others discussed. After positions on a specific issue are offered and discussed, observations were made as to how those positions were incorporated into the code of conduct.

5.3.3. Semi-Structured Interviews

The participant observation and document analysis allowed for surveying the stakeholders' positions. Semi-structured interviews were conducted with fifteen participants selected on the basis of their expertise, level of engagement with the debate, and to be representative of the stakeholder groups. (See Appendix B for a list of interviewees.) The goal of conducting the interviews was to explore particular stakeholder positions on issues, encourage reflection on the process, and explore their feelings about outcomes for the code of conduct.

This study employs semi-structured interviews to enhance exploration of the public debate while allowing interviewees to share direct personal experiences and reflections on the subjects discussed in the NTIA meetings. Fiona Fylan (2005) described semi-structured interviews as those where the researcher has a number of topics to cover, but the conversation is free to vary and may change substantially between subjects. The semi-structured interview format is the best structure to achieve the research aims and accommodate the varied view points and opinions of the interviewees. A variety of issues and viewpoints are presented at the NTIA meetings thanks to multistakeholder collaboration. The semi-structured nature of the research interview

process allows the investigator to consistently address topics in the interview protocol,[23] as well as collect information that informants feel is pertinent.

5.4. Data Analysis

The empirical data collected through the above methods have been subjected to discourse analysis (DA). As a research method, DA has a complex history and has been adopted by many different branches of social science without clear consensus on what 'discourse' actually means (Alvesson & Karreman, 2000). However, Strauss and Feiz (2014) described discourse as, "[T]he social and cognitive process of putting the world into words, of transforming our perceptions, experiences, emotions, understandings, and desires into a common medium for expression and communication, through language and other semiotic resources" (p. 1). This definition encapsulates why the social constructivist paradigm was chosen for this research project. According to social construction epistemology, reality is discursively constructed and the examination of that discourse has important effects on society (Creswell, 2009). Under this paradigm, the conversations held at the NTIA meetings may have a profound effect on society depending on the nature of the regulatory regime being developed for this technology.

Similarly, Starks and Trinidad (2007) noted that discourse analysis, "is concerned with language-in-use; that is, how individuals accomplish personal, social, and political projects through language" (p. 1374). For the present project, discourse analysis is chosen as a research method to provide understanding for how participants attempt to accomplish their particular goals while moving collaboratively towards the creation of a code of conduct for FRT. This method of analysis has been paired with the data

[23] See Appendix G for the interview protocol.

collection method of interviewing to enhance this understanding. DA is enhanced with a variety of perspectives, "Within discourse analysis sampling different groups that participate within a given discourse can illuminate the ways in which participants appeal to external discourses and identify their influence on the discourse under study" (Starks & Trinidad, 2007, p. 1375). Utilizing multiple research methods can enhance the understandings of a singular method.

Fairclough (1995) noted that certain discourses are associated with particular social institutions. The expectation for the explored case is that certain ideologies can be identified with the particular stakeholders and social institution being represented. For example, less regulation will be associated with business entities and enhanced privacy protections will be associated with consumer advocacy groups. The discourse examined concerning FRT at the NTIA meetings, the stakeholder groups participating, and the transfer of knowledge provided an explanation on the crafting of the voluntary code of conduct and its implications.

An important layer of discourse analysis is to distinguish discourse from actions taken. Determining differences in the discourse between the MSH meetings and the emerging code of conduct, aids in identifying stakeholder positions, "Nothing in discourse is neutral. Each and every instance of discourse is imbued with some element of stance; it is motivated by a perspective" (Strauss & Feiz, 2014, p. 3). Stance is concerned with a speaker's inherent attitudes, biases, and perspectives, which are prevalent in all humans. These positions are in flux and are constantly being re-negotiated (Strauss & Feiz, 2014, p. 4). Since the speaker's stance is in a state of constant negotiation, and those speakers, at times, represent larger institutions, it can be

assumed that institutional positions are in a state of negotiation as well. In fact, the MSH format ensures that positions are negotiated through interaction and their actions or outcomes are negotiated by the stakeholders. This flux of speaker and institutional stance, as well as the negotiating of actions or outcomes, reinforces the social constructivist paradigm driving this project.

The expertise of stakeholders utilized in creating a voluntary code of conduct at the NTIA meetings facilitates the creation of the regulatory regime of FRT. The objective of this research project was to gain a clear understanding of group dynamics, to identify privileged positions of authority and expertise, to recognize resistance strategies, to create and transfer knowledge, and to realize the impact these factors had in the creation of the voluntary code of conduct. Language was looked to in terms of action, "[P]eople use their language to *do* things: to order and request, persuade and accuse. This focus on language function is also one of the major components of discourse analysis" (Potter & Wetherell, 1987, p. 32). This project is an analysis of how stakeholders "do" things, create a code of conduct, with language.

Mediated discourse analysis (MDA) has largely been employed to discover participant stances and the material impact on the creation of a code of conduct. MDA is a more recent conception of DA that has been utilized in the academic community (Jewitt, Kress, Ogborn, & Tsatsarelis, 2001; Johnston, 2004; Jones, 1999; Jones, 2007; Kress & Leeuwen, 2001; Scollon & Scollon, 2004; Raudaskoski, 2010) to interpret a wide range of social issues. This method is used to identify actions: "As a theoretical position, it [MDA] focuses on linkages between discourse and action and how these play out in complex social situations" (Scollon & de Saint-Georges, 2012, p. 66). MDA

focuses on "the outcomes of social interactive processes of production" (Scollon & de Saint-Georges, 2012, p. 66). MDA attempts to understand social action by discovering the intersection of three material entities 1) the historical body of social actors, 2) the configuration and social structure of individuals present, and 3) the discourse carries out social action (Scollon & de Saint-Georges, 2012, p. 71). In other words, "[I]n democratic public discourse positions are stated, positions are argued, positions are negotiated and the actions which are taken and which become policy and practice are the outcome of this dialectic" (Scollon, 2008, p. 162). The negotiation of positions and actions are of primary importance to this project.

The dissertation utilized MDA to discover actions taken by the participants, what their role in the process is, and why they are involved, and how discourse has shaped those actions. Transcripts were created based on the debates at the NTIA meetings on FRT and were subsequently coded for themes that help answer the formulated research questions. Specific mention of individual participants in the dissertation were only identified when their comments were made publicly. Stakeholders have been interviewed for this project and to protect their anonymity, their views are simply attributed to the larger stakeholder group they represent, NGOs, academics, government, and business.

MDA was not utilized to its full potential in this project. The research design and methods chosen were selected predicated on the initial timeline set for the MSH meetings, predicted to end around one year's time. The timeline was altered due to stakeholder concerns and scheduling logistics. As such, it was difficult to track the changes to the code of conduct that resulted from the discourse of the group. A final code of conduct has yet to be created and therefore it is problematic to pinpoint discourse

that led to material language or changes in the code. Some changes were able to be identified; however, this method fell short of expectations due to unforeseen complications that arose with the timeline for the creation of a code of conduct.

Silences in public debates have been studied as a significant discursive strategy. According to Huckin (2002), "[O]ften what is not said or written can be as important, if not more so than what is" (p. 348). Huckin (2002) defined textual silence as "'[T]he omission of some piece of information that is pertinent to the topic at hand'" (p. 348). Textual silence can take on several forms, each with unique implications. Huckin (2002, p. 348) described five types of textual silences. The first silence described is a speech act silence. This silence is demarked by such force that the listener/reader is easily able to interpret the meaning of the silence by pragmatic rules of language. Presuppositional silences occur when the speaker does not state what is assumed to be common knowledge. Individuals may employ discreet silences to avoid stating sensitive information. Genre-based silence are dictated by conventions (obituaries usually omit negative details about the deceased). Finally, and perhaps most troubling, are manipulative silences, when pertinent information is deliberately concealed. Similar discursive strategies were observed in the NTIA meetings. Technical presentations, for example, contain some presuppositional silences, which is problematic for interested laypersons. Manipulative silences were observed in the repeated calls for companies like Facebook and Google to make presentations about their use of FRT. Examining these silences produced important insight into the information omitted from the meetings and the motivations for the omissions. Huckin (2002) wrote that context is the key

component to identifying manipulative silences, otherwise all things unsaid would count as textual silence (p. 353).

Discourse analysis was facilitated by the software HyperRESEARCH. The software supports the case study design that was employed for this project (Researchware, 2014). HyperRESEARCH is a software tool that aids in qualitative research approaches by allowing the use of audio and video files for the coding of data. Audio files were created by recording the proceedings of the meetings. The files were then opened in HyperTRANSCRIBE where this researcher recorded manually the spoken details of the meetings verbatim. After the meetings were transcribed this researcher used HyperRESEARCH to create a code book[24] of important aspects of the meetings, or trends observed, and then applied these codes to the text created in HyperTRANSCRIBE. HyperRESEARCH then organized all relevant sections of text according to how they were coded facilitating the discourse analysis utilized for this research. Noticeably, responses from participants were not attributed to individuals to protect their anonymity.

To enhance the quality of the applied discourse analysis the researcher attended online webinars hosted by HyperRESEARCH. During the webinars, HyperRESEARCH employees explained the various facets of the research platform. Examples of research projects were presented along with explanations on how to code and identify important trends. This additional support ensured that the codes and research conclusions were of the highest quality.

[24] See Appendix H for a table of codes used.

5.5. Research Questions

The methods chosen and discussed above are designed to help clearly answer the research questions presented in this project. The first question this research addresses is "How is the regulatory regime of FRT emerging in the U.S.?" Currently, the voluntary code of conduct created by the MSH process are the most robust regulation to date, which is why discourse analysis was selected to examine the arguments presented, the participants who presented them, and the ultimate solutions proposed and passed to solve those arguments. Discourse analysis lends itself to understanding the meanings behind the arguments, as well as the solutions created.

The second research question is: "What are the roles of the various stakeholders in shaping the commercial regulation of FRT?" Semi-structured interviews, discourse analysis, and participant observation were employed to answer this question. Semi-structured interviews allowed the participants to define how they see their roles in the process and describe in detail the ideas and solutions they are advocating for. To help provide further insight to their answers, discourse analysis and participant observation were employed. Discourse analysis analyzed stakeholders within the context of other participants, as well as by the discourse created using the MSH process. Finally, participant observation provided a unique "behind the scenes" perspective. Those who call in to the meetings, or follow along with the webcast, miss the conversations that occur during the breaks. They are also not privy to all the people in attendance. Being present for the meetings provides a larger perspective in seeing the collegiality of the group, and it helps identify which participants have better working relationships than others.

The final research question is "How does FRT challenge our current conceptions of privacy?" Discussion of the various uses of the technology has revealed new challenges to our current understandings of privacy. Analysis of the discourse at the meetings as well as the varied privacy conceptions of the stakeholders has provided insight as to how FRT challenges how privacy is understood.

CHAPTER 6

EVOLUTION OF DATA PROTECTION REGULATION

Data protection has been an important topic of regulation between the U.S. and the European Union (EU) since the differing views on how to regulate data protection have created some tensions. The Edward Snowden revelations of the National Security Agency spying on U.S. and EU citizens (collecting phone records and meta-data without warrants) have even caused animosity between the entities. The EU is in many ways leading the fight for the protection of citizen data and increased privacy protections for citizens. Since many U.S. based companies involved in the facial recognition technology space are international in nature it is important to understand the data protection relationship between the U.S. and EU.

6.1. History and Development of Data Protection

Increased use of technology led to greater accumulation of user data. In light of the increased amount of data collected, the first data protection law was enacted by the German state of Hesse in 1970 (Cate, 1994, p. 431). The rise in the use of information technology provided motivation for Germany to enact this state law nationally; it was the first data protection law in the world (Wilhelm, 2015). In 1983, the Highest Court in Germany declared a *constitutional right* to what was referred to as *informational self-determination*. This decision was in part, due to a population census and rising fear of surveillance amongst German citizens (Hornung & Schnabel, 2009, p. 85). German

citizens are acutely aware of the power of the census given their history prior and during WWII. Informational self-determination was as a cornerstone of democratic exchange because "The protection of personal data is essential for a free and self-determined development of the individual. At the same time, the self-determined development of the individual is a precondition for a free and democratic communication order" (Hornung & Schnabel, 2009, p. 86). The Germans understood that information about the individual needed to be under his/her control. Information regarding dissent not under control of the individual, could have a chilling effect on free and open communication. Hornung and Schnabel noted that:

> If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom. If citizens are unsure whether dissenting behaviour is noticed and information is being permanently stored, used and passed on, they will try to avoid dissenting behaviour so as not to attract attention. They may even abstain from making use of their basic and human rights. In a potentially all-knowing state, freedom of speech and freedom of choice are virtually impossible. (p. 86)

Providing citizens with robust data protection strengthens open communication and uses for political dissent, important components of healthy democracies. The right to informational self-determination benefits the individual and the public in fostering open communication.

Before the formation of the EU in 1993, guidelines were issued to further advance notions of data protection, "In 1980 the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD) issued Guidelines on the Protection of Privacy and Transborder Rows of Personal Data (Guidelines)" (Cate, 1994, p. 431). The guidelines had no real legal force and allowed for flexible implementation by individual nations. Data protection had important implications for not only democracy, but also commerce. In 1981, the OECD released a document titled "For the Protection of Individuals with Regard to Automatic Processing of Personal Data," a convention very similar to the guidelines previously issued, but with a focus on protecting personal privacy.

In 1990, the European Community Commission published a draft document that would later become the EU Directive on Data Protection entitled, "Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data" (Cate, 1994, p. 432). The directive was passed after adding an amendment which eliminated the distinction between public and private sector data. Treating public and private sector data as equal is a novel protection that puts government on an equal footing with private entities, a provision not currently adopted in the U.S., they share equal protections and require equal thresholds for examination. The directive required countries to create laws governing the processing of personal data. Processing personal data was broadly defined as, "any operation or set of operations including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"

of data (Cate, 1994, p. 433). Laws compliant with the directive provided an individual with robust data protections including accurate information, legitimate use, consent of the individual, the right to access data, and other protections[25]. The last point of the directive is perhaps the most important for this MSH process under investigation in this dissertation as it stipulated that each member state must: *Establish laws prohibiting the transfer of data to non-member states that fail to provide adequate data protection* (emphasis added).

This last point has become the center of tension between the U.S. and the EU. The EU has asserted that the U.S. is doing an inadequate job of protecting its citizens' data. The U.S. has no comparable data protection regime and is seen as "behind" the EU on this front. Failure to offer adequate data protection could threaten commerce between the U.S. and the EU, a relationship worth billions of dollars in trade.

6.2. Safe Harbor

The U.S. and the EU take different approaches to protecting citizens' privacy. As has been shown, the EU relies on comprehensive legislation with government bodies that ensure the data protection laws are followed. The U.S. has a variety of approaches to protecting citizens' data, including "legislation, regulation, and self-regulation" (Export, 2013, par. 1). The U.S. and the EU worked together to create the *Safe Harbor Framework,* which was formally adopted in July of 2000, so that the two entities could share data and still be in compliance with the EU data directive (Wilhelm, 2015). Participation in the Safe Harbor Framework is voluntary; entities that comply with Safe Harbor must notify the U.S. Department of Commerce yearly that they are in compliance

[25] For a full list of provisions please refer to Appendix F.

with the Framework (Export, 2013, par. 5). There are seven principles in the Framework that must be complied with[26].

The first principle that must be complied with is that of *notice*. Organizations must notify individuals about the purposes for which they collect and use personal information. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

Notice is the precursor to the second principle which is *choice*. Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

The third principle is *transfer to third parties*. To disclose information to a third party, organizations must apply the notice and choice principles. If an organization wishes to transfer information to a third party that is acting as an agent, it may do so only if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such a third party requiring that the third party

[26] The principles can be found on *export.gov* (2013).

provide at least the same level of privacy protection as is required by the relevant principles.

The fourth principle of the Framework is *access*. Individuals must have access to personal information held about them by organizations and be able to correct, amend, or delete that information where it is inaccurate; however, if the burden or expense of providing access is disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual are violated then organizations are not required to allow individuals access.

Security is another important principle of the framework. Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Recent government and commercial data breaches have highlighted the importance of this principle in the eyes of the public. In concert with security is *data integrity*. Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Finally, there is the Framework principle of *enforcement*. In order to ensure compliance with the Safe Harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) must have procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented; finally, must instill (c) obligations to remedy problems arising out of a

failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and Safe Harbor benefits will no longer be assured.

Many of these same principles have been discussed in the development of a code of conduct for FRT. Due to the international nature of many companies that use or want to use FRT, compliance with Safe Harbor will be paramount in order to transfer data to and from the EU. The U.S.'s fragmented approach to data protection has led to its use of the private sector for most of the enforcement. If private entities fail to comply they can be prosecuted under federal unfair or deceptive practice legislation, which is largely accomplished through the FTC but, also through state legislation (Export, 2013).

Despite having both the U.S. and the EU operating under the Safe Harbor Framework there were a series of events that left the EU wondering if they had inadvertently created a data transfer loophole due to lower U.S. data protection standards (Wilhelm, 2015). Shortly after the Edward Snowden leaks, which caused increased concern in the EU about Safe Harbor principles being violated by the U.S., the EU recognized that Safe Harbor needed to be updated. In March 2014, the EU strongly recommended that the U.S. create new data transfer rules to protect EU citizens' data; in the same month, the EU Parliament also called for a suspension of Safe Harbor (Wilhelm, 2015). The main concern of the EU, regarded public authorities processing data. Primarily, it wanted to ensure that exceptions for national security were limited to only what was necessary for safety. In 2014, the Center for Digital Democracy filed complaints against U.S. companies that had not complied with Safe Harbor. The FTC

then filed a complaint against the TRUSTe brand for failing to recertify companies for Safe Harbor compliance. In light of these complaints the EU has considered suspending Safe Harbor because of inadequate data protections, an act that would have serious consequences for trade relations between the U.S. and the EU. Currently, as of March 2015, the European Court of Justice is hearing a case against the NSA that could have a profound impact on the U.S. - EU Safe Harbor agreement (Wilhelm, 2015).

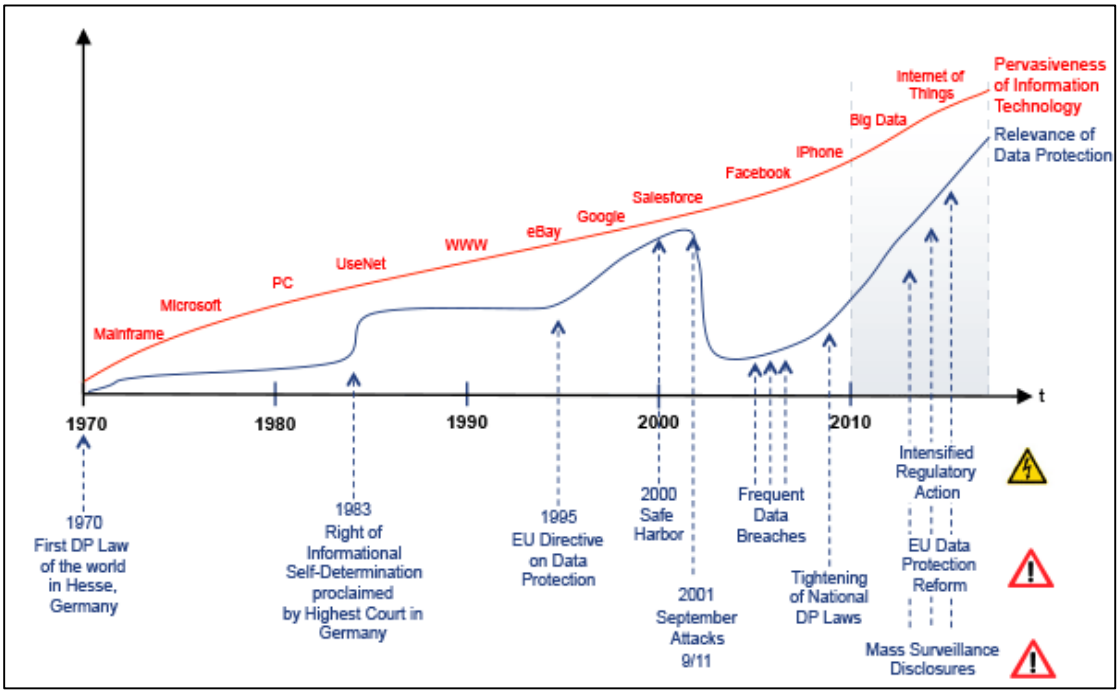

Figure 5. EU data protection timeline. Adapted from the Privacy Association (Ernst-Oliver, 2015).

6.3. U.S. Data Protection

Data protection regulation in the U.S. is a patchwork of state and federal legislation enforced by multiple regulatory bodies. Financial firms follow standards set in the *Gramm-Leach-Bliley Act* which promulgates rules for collection, use, and disclosure of private information (Sotto & Simpson, 2014, p.191). Similarly, health care providers are bound by the rules set forth in the *Health Insurance Portability and*

Accountability Act (HIPAA). For non-regulated industries the Federal Trade Commission (FTC) is the primary enforcement body. The FTC, under Section 5 of the FTC Act, can enforce the *unfair or deceptive acts or practices* clause against businesses that violate the section rules. State laws are generally enforced by state Attorney's General; otherwise, state laws allow for individuals to file suit against entities that have broken the law. The following lists states other important laws that concern privacy and data (Sotto & Simpson, 2014):

- Electronic Communications Privacy Act: "[S]tatutory frame-work of privacy protections and related standards for law enforcement access covering electronic communications and remotely stored electronic records. Significantly, the ECPA established the standards that currently control law enforcement access to personal e-mail and electronic records, such as pictures and date books, stored on remote servers" (Mulligan, 2003, p. 1557).
- Computer Fraud and Abuse Act: Originally created in 1984 to criminalize federal computer crimes, the act has been expanded five times and may now cover all uses of computers in the U.S., with the potential to regulate abroad (Kerr, 2009, p. 1561)
- Fair Credit Reporting Act: Designed "to protect the privacy of consumer report information and to guarantee that the information supplied by consumer reporting agencies is as accurate as possible" (Stokes, 1999, p.1)
- Fair and Accurate Credit Transactions Act: Designed to fight identity theft, increase consumer access to credit, and improve accuracy of credit information (Pu Holt, 2004, p.3).

- Children's Online Privacy Protection Act: This act severely limits the collection of information about children under the age of thirteen without parental consent. It also curtails the ability of children under the age of thirteen to obtain an email account without parental consent as well (Belmas & Overbeck, 2012).

One of the most important set of laws in the U.S. for privacy and data protection is the Fair Information Practices (FIPS). The FIPS began as a report to the Department of Health in the late 1970s, but now some of its principles have been discussed and implemented internationally (Gellman, 2014, p.1). Provisions in addition to the FIPS, have become common place in policy discussions and laws regarding privacy. The FIPS have evolved over time. The Department of Homeland Security in 2008 issued their version of the FIPS but updated and renamed it the Fair Information Practice Principles (FIPPS) (Gellman, 2014). The Consumer Privacy Bill of Rights (CPBR) also embraces the FIPPS. The CPBR FIPPS outline the following protections (Gellman, 2014, p. 16). *Individual Control*, "Consumers have a right to exercise control over what personal data companies collect from them and how they use it." *Transparency*, "Consumers have a right to easily understandable and accessible information about privacy and security practices." *Respect for Context*, "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." *Security*, "Consumers have a right to secure and responsible handling of personal data." *Access and Accuracy*, "Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is

inaccurate." *Focused Collection,* "Consumers have a right to reasonable limits on the personal data that companies collect and retain." *Accountability,* "Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights" (Gellman, 2014, p. 16).

Despite the lofty protections that the FIPPS tries to achieve, it is inconsistent with interpretations found in HIPAA and those put forth by the FTC (Gellman, 2014). Most notable for this project is the inconsistency with the FTC, the enforcement agency for any voluntary code of conduct created for FRT. It remains unclear how the FTC will deal with inconsistencies found between the FIPPS, the FTC interpretation of the FIPPS, and privacy protections created in the code of conduct for FRT.

The U.S. has weaker data protection laws than the EU because big businesses are often able to lobby very effectively in Congress. Coleman (1982) made it clear that businesses have grown increasingly influential and powerful in the U.S. However, the EU has taken the opposite approach, granting consumers greater control over their data and providing robust protection for them. As Simon Davies (2015) noted, "Silence from the United States over collection of data from non-U.S. persons has fueled support for strengthened legal protections over the collection and processing of data on EU citizens" (p. 57). The EU may well suspend the Safe Harbor agreement if the U.S. does not take action to provide better protection for consumer's data and privacy.

The established U.S. and EU laws are reflected in the development of a code of conduct for FRT. The code of conduct must comply with existing laws as the NTIA does not have the authority to supersede existing laws. Since many of the corporations involved in the creation and use of the code of conduct for FRT conduct business in both

the U.S. and the EU, it is important to understand how both protect data. The U.S. and EU will likely need a new privacy agreement, along with data protection rules and laws, so that trade can continue and citizens' rights and data be protected. Another important right for U.S. citizens is the First Amendment, which applies to photography and is important to the FRT debates.

6.4. Photography, the First Amendment, and Copyright

Since FRT is applied to photos, photo creation and photography are important legal concepts to discuss. The United States Supreme Court (USSC) has yet to consider the First Amendment rights of photographers, yet it is clear that they have a right to expression and a property right interest in the work that they create, usually in the form of copyright. Intellectual property law covers copyright, which exist to, "[P]rotect creative works such as books, periodicals, manuscripts, music, film…." (Belmas & Overbeck, 2012, p. 237). Photographs constitute creative works and as such can be protected by copyright, but there are limits as to what can be photographed publicly. Similarly, there are limits on the protection that the First Amendment provides photographers.

6.4.1. Photography and the First Amendment

The USSC has yet to fully address the First Amendment rights of photographers; however there are some court cases that do tangentially address the issue. The First Amendment is not limited to strictly the spoken or written word, but also includes communicative conduct (Kenworthy, 2012). In public, to be protected by the First Amendment two criteria must be met for communicative conduct (photography). "To achieve First Amendment protection, a plaintiff must show that he possessed: (1) a message to be communicated; and (2) an audience to receive that message, regardless of

the medium in which the message is to be expressed. (Hurley v. Irish-American Gay, Lesbian, & Bisexual Group, 1995)" (Kenworthy, 2012, par. 6). One court found a limitation when a father taped his daughter's choir performance, citing that there was no "communicative or expressive purpose" and therefore was not protected by the First Amendment (Kenworthy, 2012). With communicative and expressive purposes in mind it is clear that most news gathering is covered under the First Amendment, but individual citizens can also be afforded the same protection. In *Lambert v. Polk County*, an individual citizen took a video tape in a public circle with the intent to sell any newsworthy content. The individual happened to tape a fatal fight and the police confiscated the tape. The plaintiff sued the police and the court found that the police had violated his First Amendment right, noting that "It is not just news organizations… who have First Amendment rights to make and display videotapes of events – all of us…. have that right" (Kenworthy, 2012, par. 22).

6.4.2. Photography and Copyright

As stated previously, copyrights provide owners with a property interest. Images, written works, and databases are but a few examples of media that can be protected by a copyright. The 1976 Copyright Act also protects these works for a very lengthy amount of time, 95 years (Belmas & Overbeck, 2012, p. 237). While the First Amendment protects free speech and freedom of the press it is important to note that the news cannot be copyrighted. One major individual copyright concern, with regard to FRT, is where an individual's image resides. In years past, photo albums were a popular place to store photos, usually copyright free. Today, most or all of an individual's photos reside online, using Twitter, Facebook, LinkedIn, and other popular social networking and interest

forums. In many instances, when an individual agrees to the terms of use or the EULA presented by the company, they grant the website service rights to use the images and an individual's likeness for commercial gain. Furthermore, the individual also grants third parties that same right under the EULA. For example, a recent paragraph in Facebook's terms of service read,

> 1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
>
> 2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others) (Facebook, 2012, par. 4).

What is most concerning about online image storage and usage is not the "relatively" short 95 year copyright protection that the government affords an individual, but the ability for an image to survive and be used freely on the Internet for, hypothetically, forever. Facebook's terms specifically indicate that once content has been shared it will not be deleted from another's account even if the original individual deletes his or her profile or profile content.

Presently, there are countless numbers of images on the Internet. Individuals currently post "selfies," profile pictures, vines, and other such content featuring their image without much thought to potential consequences. As FRT is employed more frequently for secure access to property or privilege access the plethora of individual photos may prove problematic for secure access. Individuals are likely to become increasingly concerned about where their images reside and how they are being used when the government and other businesses grant individuals access to their privileges (government benefits) or property (bank accounts) through FRT. It remains unclear what remedy, if any, an individual will have in controlling their image, unless it was taken in a manner protected by the First Amendment or if the owner has protected the image with a copyright.

A final thought concerning copyright and FRT revolves around the algorithms and the data they produce. Suppose an image is copyrighted but FRT is still applied to the image, keeping in mind multiple algorithms from different FRT vendors could be applied to the image. Are the integers created by the algorithm protected under the copyright? If the integers are protected under a separate copyright and the image can be reverse engineered from the integers, who owns the resulting image and the underlying data? These conflicts are bound to appear as courts deal with difficult questions.

CHAPTER 7

HOW IS THE REGULATORY REGIME OF FACIAL RECOGNITION TECHNOLOGY EMERGING IN THE U.S.?

7.1. Stakeholders

A primary consideration of any multistakeholder process is the identification of stakeholder groups, also referred to as stakeholders. Minue Hemmati (2002) defined stakeholders as "[T]hose who have an interest in a particular decision, either as individuals or representatives of a group. This includes people who influence a decision, or can influence it, as well as those affected by it" (p. 2). For the MSH process on facial recognition technology four distinct stakeholder groups are represented. The groups were determined by this researcher and citizen members of the public have yet to speak up and identify themselves. The meetings include non-government organizations (NGOs), academics, businesses (sometimes called industry or private sector and also includes trade groups who represent several businesses), and government.

7.1.1. Non-Governmental Organizations

NGOs involved in the MSH process for FRT consist primarily of consumer protection and privacy advocates. This stakeholder group consists of Consumer Action, Consumer Federation of America, Center for Digital Democracy, American Civil Liberties Union, Common Sense Media, Center for Democracy and Technology, Online Trust Alliance, Technology Freedom, Secure Identity and Biometrics Association, Computer Communications Industry Association, and the Electronic Frontier Foundation.

This stakeholder group advocates for increased consumer protections, increased protection of privacy, and increased transparency and choice offered by businesses. NGO's have been advocating for the responsible use and deployment of FRT, as well as notification, transparency, and consumer choice, all of which will be explained in detail later.

7.1.2. Academics

A number of academic presentations have been made to the group. Academic presentations regard diverse issues, including the accuracy of FRT, how FRT works, various uses of FRT, how FRT may be used to discriminate against vulnerable groups, and how FRT can pose threats to privacy. Representatives of this stakeholder group include UCLA, New York University Information Law Institute, Carnegie Mellon University, and Rutgers. Academics have been invited by various stakeholder groups or by the NTIA on behalf of a stakeholder group. Academics serve the group by filling in gaps of knowledge that are not present by the stakeholders.

7.1.3. Businesses

Businesses have a vested interest in utilizing FRT. Facebook has the world's largest biometric database and its system works better than the FBI's FR (Brandom, 2014). Business interests range from security, loss prevention, interactive advertising, and a variety of authentication purposes. Members that have been identified in the meetings include the Internet Association, International Biometrics and Identification Association, Motorola, Interactive Advertising Bureau, NetChoice, IBG, Sotero Defense Solutions, Business and Performance Research, Software Information Industry Association, Application Developers Alliance, Computer Communications Industry

Association, Direct Marketing Association, and Marketing Research Association. While businesses have readily identified themselves as supportive of the process most have been reluctant to discuss what they are doing or plan to do with the technology in the future. As a general statement, business entities have advocated for minimal privacy protections, wide latitude in deploying the technology, and minimal regulations to promote the innovation of FRT.

7.1.4. Government

There have been two main government bodies represented at the NTIA MSH meetings for FRT. The first is obviously the NTIA itself. The NTIA is housed in the Department of Commerce and has been tasked with convening the MSH process for FRT. The only notable foreign government represented has been the Information and Privacy Commissioner's office of Ontario Canada. Officials from this office have made presentations at the meeting and have provided technical support for the duration of the meetings. Other U.S. government agencies represented during the meetings have been the Federal Trade Commission and the National Institute for Standards and Technology. The FTC has made presentations about their enforcement authority as well as previously identified best practices. NIST has provided technical expertise about the capabilities of the technology.

7.2. Historical Results Impacting the Multistakeholder Process for Facial Recognition Technology.

The Consumer Privacy Bill of Rights (CPBR) directs the NTIA to convene MSH processes regarding privacy issues. There was one previous MSH effort before the NTIA convened meetings for FRT. During the Mobile Application Transparency Process

(MATP) stakeholders met and ultimately created a code of conduct, yet stakeholders encountered several sources of adversity that have impacted the FRT process. As reported by the participants in the interviews conducted for this project, the adverse sources included: perceived inefficiencies, issues of participation, differing expectations, trust issues, and questionable motives regarding the outcome of the process. Historical results and interaction of stakeholders are important to note for mediated discourse analysis as they likely have an impact on the actions designated for the FRT code of conduct (Scollon & de Saint-Georges, 2012). Data that was recorded during the public meetings for FRT will be reported with individuals' names included; data recorded during private interviews will be identified only by stakeholder groups to maintain the confidentiality of the interviewees. Interviewee data is reported according to the stakeholder group they represent, this does not imply that stakeholder groups are uniform in their advocacy goals, interests, or knowledge base.

7.2.1. Inefficiencies

Inefficiencies in multistakeholder processes can transpire in a variety of forms. Some sources of inefficiencies include participation (too much or too little), process management , lack of information, decision making, and the inability to implement results. As stated previously, the learning process is very important to multistakeholder processes. Stakeholders need to know how companies use data and information in order to understand what regulatory safeguards are needed.

Inefficiency 1: Participants and stakeholders may be reluctant to share information to protect proprietary advantages or to avoid regulation. The MSH process can be slowed or halted due to lack of information. According to Susan Grant (2014) of the Consumer

Federation of America, "As you know I wasn't thrilled with the last process, but at least we had active participants from the mobile app community." Businesses were reluctant to provide relevant information to the group in order to protect proprietary advantages over other businesses that attended the meetings.

Inefficiency 2: Lack of participation by some stakeholders might best be categorized by Huckin (2002) as discreet silences, or not revealing sensitive information. John Morris (2014) of the NTIA stated:

> My perception of how the last process played out is that a lot of stakeholders kind of got more involved once the conversation moved to a straw man or a set of principles or something….I think there's at least a chance that if this group moves down a direction of actually talking about principles, or a code, that there may be broader engagement.

This data shows the importance of active stakeholder involvement throughout the MSH process. Stakeholders are cognizant of the importance of collaborating with all participants to enhance their understanding of the problem's challenges and solutions (Gray, 1989, p.5). In the end, very few companies adopted the code; Intuit and Lookout were among the few to adopt it (Tummarello, 2014). One possible reason for the limited adoption of the code of conduct in the MATP was the delayed participation of stakeholders until the code was being drafted. Businesses decided not to be actively involved until the code of conduct was being drafted, presumably to protect competitive advantages.

> There were certainly inefficiencies early in the process. As it progressed, and everyone was transitioning from the research and background into

> drafting a code, there were a lot of complaints that a few people in the room ran away from, that and proposed language that others weren't happy with, but it was too late. The draft had been written and the precedent had been set. (Business).

Lack of participation and information sharing by businesses in the beginning led to creation of language in the code of conduct that, ultimately, very few were able to implement.

Inefficiency 3: How decisions are made can have significant impacts on the efficiency of MSH processes. During the MATP process, a drafting committee was formed to create language for the code of conduct. There was a lack of transparency, or access to information concerning the decisions being made, and stakeholders were left out of the decision making process (Hemmati, 2002, p. 41). "So I don't think we are ready for a drafting committee and I'm hoping we never get to a drafting committee as opposed to some other way" (Business). This comment underscores previous comments made about how "insular" the drafting group was. Creating a decision making process that was inefficient was not a goal of the group. "Since I'm the one he's talking about I will say it didn't happen on purpose that way. There were a lot of things that happened in the last process and we were doing the best we could" (NGO). This comment suggests that unfamiliarity with the MSH process in general may have contributed to the inefficiencies experienced by stakeholders. Lack of familiarity with the MSH process was a theme echoed by several interviewees. Borrowing from the literature, no "capacity building" had transpired for the MATP (Antonova, 2011). Creating a complete code of conduct and taking a vote on the final product led to animosity among stakeholders in the MATP.

Ultimately, this decision making process increased tension among stakeholders, thus voting on a final code of conduct with limited input from stakeholders led to a product that few could adopt.

7.2.2. Participation

In MSH processes, who the stakeholders are and how they are able to participate can have material consequences on results. Minu Hemmati (2002) defined participation as "[T]hat all stakeholders have a voice in influencing decision-making. Participation is the foundation of legitimacy in all democratic systems" (p. 41). An NGO representative noted, "What happens is big business gets behind these issues and put a lot of money in their lobbyists and can over dominate discussion. That puts the advocates at a disadvantage. So issues stall. That happened in do not track [Mobile Application Transparency Process]." Money also makes attending the meetings easier as well, "The other thing is also when you have these meetings they are all in D.C. and not all groups are in D.C. who can afford to fly there all the time" (NGO). Mitroff (1983) noted that resources impact the power stakeholders have to influence the process. No mention is made of physical proximity to the MSH venue as a factor impacting stakeholder power. Given the static nature of the venue, stakeholders with close proximity to the Washington D.C. area have an advantage in terms of ease of attendance and cost savings in terms of travel. This observation confirms that companies with greater financial resources can have disparate effects on the process if they so choose (Mitroff, 1983).

Advocates have expressed frustration with what they feel is underrepresentation compared to industry stakeholders. Underrepresentation appears to be mostly a financial problem. Frustration has also been expressed in terms of limited financial resources in

comparison to industry stakeholders, expressed in an interview that occurred July 23, 2014:

> There are highly paid lobbyists or tech companies and they can spend all day talking about the word "if" because that's what they are paid to do. And you have the public interest community who numbers maybe five advocates who care a lot about it but don't have the personnel to do that…there's an imbalance there. Certain industry participants have disproportionate financial means to influence the proceedings if they so choose (NGO).

One individual felt that the MSH format favored industry participants, he stated in an interview on October 13, 2014 "…[T]he structure would be unfair to non-profit groups, consumer groups, because industry would be able to dominate those proceedings in numbers [and] in terms of resources etcetera. So I've been critical" (NGO). Advocacy stakeholders have expressed concern about representation from a purely numerical standpoint. Industry stakeholders have countered these concerns by noting that only one person can speak up at a time. In an interview occurring September 5, 2014 one business representative expressed:

> You can be company X and bring 20 people to the meeting, having 20 people there provides you no particular advantage other than it might look good for people back at your company. If you're a law firm having lots of people there is good for your billable hours. I don't see that having any impact on the process. [It matters little] if you represent yourself or a gigantic company, the process tends to be quite a leveler (Business).

While equitable numbers of stakeholder groups may provide individuals comfort, meaningful participation adds value to the discussion (Mitroff, 1983). If stakeholders cannot meaningfully contribute to the discussions at the forum, they are unlikely to be influential in the process.

7.2.3. Business Resistance

The goal of the MSH process for MATP and FRT has been to create voluntary codes of conduct. The academic literature notes that businesses are generally adverse to regulation and therefore have reasons to resist the creation of new regulation (Kolk, Tulder, & Welters, 1999, p. 152). This view is substantiated by one business participant in this process in an interview occurring June 24, 2014:

> I still think industry self-regulation is probably the best approach because we also know the most about what we do. But there are benefits to this process. *If this discourages some consumer advocates from now petitioning for these hard hammer laws then I think that's a real benefit for everyone* [emphasis added] (Business).

Stakeholders are mindful of the fact that refusing to negotiate on positions can have adverse effects, "[I]t does force you to make a decision or balances that you probably wouldn't have struck on your own. If you're not open to doing that, this process is quickly going to degenerate" (NGO). Business resistance is a legitimate concern of the MSH process, one that was seriously discussed in the FRT process.

Two dominant positions have emerged from the MATP that are also present in the FRT process. NGO's have, mostly, advocated for legislation that provide "teeth" to the principles that they are creating in the code of conduct. Many NGOs have expressed

concerns that because the code of conduct is voluntary if the group enacts serious privacy protecting principles companies will not agree to its implementation. Conversely, if the group creates standards that are easy to implement and of poor quality many businesses may sign on to the code out of convenience and to give consumers the pretense of real privacy protection. Businesses also feel that they are in the best position to regulate the technology and their own business practices because of their expertise in utilizing the technology. Both stakeholder groups have legitimate positions. These positions have been relatively stable throughout the current MSH process for FRT and both stakeholder groups are cognizant of the other's desires and their likely actions towards a code of conduct (Scollon & de Saint-Georges, 2012). The voluntary nature of the code of conduct remains a point of contention for both groups. NGOs worry that businesses will not sign on because of privacy protections, while businesses often worry about spending time and resources on a code of conduct that ultimately no one will adopt.

7.2.4. Trust

Presumably, participants in the MSH process are there to develop codes of conduct. Determining the motivations of participants is part of developing trust in other stakeholders and the process in general. Stakeholder motivations for the FRT process will be discussed in detail later. Some participants may not be interested in collaboration "[A] source of adversity includes sometimes you have groups that are unwilling to budge or want to use the NTIA process as more of a stage rather than a meeting room. That's where you are going to see some challenges" (Business). Stakeholders have misgivings about participants who are at the forum to grandstand rather than work towards the development of a code, and are particularly cognizant of how fragile the MSH format can

be. "The fact is, if you are not buying into the MSH process, you can end up sacrificing [time and resources], essentially you can turn the whole thing into a farce very quickly" (NGO). Due to the fragility of the process stakeholders have to trust that all participants are interested in brokering a fair deal. Unwillingness to collaborate is detrimental to the MSH process, and can determine its success or failure (Gray, 1989, p. 59). The concern about the process failing is if some stakeholders feel they are better served by preventing an agreement (Gray, 1989, p. 63).

With stakeholders obstructing the process trust is vital within the content of the document. During the MATP there was concern that language proposed by participants did not end up in the completed document, "Of course the concern is having gone through this process once before, we sometimes know that brackets have a tendency to just disappear and underlying text remains" (Business). Returning to issues where immediate consensus could not be reached apparently resulted in the exclusion of language that was important to certain participants.

Stakeholders have concerns about trust beyond the other participants in the room and the document created. The convener of the meetings, the NTIA under the Department of Commerce, has been a source of mistrust for some stakeholders, "Right away I knew this was not a good way to develop privacy policies" (NGO). One individual noted that the NTIA is housed in the Department of Commerce. The participant felt that the NTIA was incapable of brokering a fair deal when the agency is housed in a department whose main directive is to promote American business and has not historically been involved in privacy protection, "It's corrupt in a sense that really the loyalties of the Commerce Department are industry" (NGO). These comments make

clear that certain stakeholders lack trust in the Department of Commerce, a question substantiated by looking at the mission statement of the Department of Commerce, where there is not a single mention of the word privacy. (See Appendix D for mission statement).

7.2.5. Expectations

The codes of conduct created outline acceptable uses of the technology and are prescriptive about aspects of the technology including data protection. The expectation for a code of conduct is to be actionable so that companies can adopt it, "I would like to see something that companies would actually sign onto and agree to follow and see where we go with that" (NGO). Companies must adhere to responsible practices that can be adopted and are actionable or consumers may choose other services. "And the question is what can we actually get industry to agree to adhere to that will make consumers better off. And frankly, the only thing that matters is whether they will come to the table and sign on" (NGO). The ability to broker a fair deal is an important prerequisite to collaboration (Gray, 1989, p. 62). Provisions in the code of conduct can determine whether companies will sign onto the code of conduct or not. Code provisions must be actionable so they can be implemented, but they must also protect consumers or consumers may choose alternative services or products. Businesses may be reluctant to agree to all consumer protecting provisions, in the meeting on December 15, 2014 Carl Szabo of NetChoice stated:

> I'm talking about the potential benefit to getting people to sign onto the code. I'm going to look at Bill as the resident attorney at the big law firm advising clients. But if you had a client asking you, "Hey should I expose

> myself to greater data breach liability?" you are probably going to say no (Business).

Expectations from stakeholders are not to simply create a code of conduct, but create one that can be adopted by companies to provide consumers with privacy protection.

7.2.6. Moderator

Moderators are responsible for facilitating MSH meetings, and they can have a profound impact on the results of MSH processes. According to most interviewees, the initial moderator for the MATP had a negative impact on the proceedings. One interviewee summed the position up best in an interview occurring September 5, 2014.

> We had a facilitator who was anything but. He was a condescending jackass and tried to treat a room of hundreds of people as if they were elementary school children. Which in one respect, if you knew a lot of these people, you could understand why he might approach them that way, cranky, childish (Business).

The relationship between the moderator and stakeholders can have an important impact on the proceedings. The NTIA initially brought in an outside moderator, probably to avoid being seen as biased, however the moderator lacked a significant stake in the process. "What the mistake is, is they brought in a 3rd party facilitator and they [NTIA] raised their hands as to giving it some direction" (NGO). The NTIA, in its effort to avoid biased behavior, disengaged too much from the process, leading to conflict and a deterioration of the process. One participant described the moderator's effect on the process as, "This wasn't going to work, it was going to fail. Part of it was the facilitator was bad" (NGO). These views express the importance stakeholders place in the

moderator for having satisfactory outcomes. Moderators can be productive facilitators leading to productive outcomes, or can obstruct the process as was seen in MATP. Academic literature also notes the importance of moderators on the process: "Nevertheless, competent moderators who facilitate, push, and maintain the process were seen as indispensable (Schwilch, et al., 2012, p. 56).

7.3. Previous Processes Regarding Facial Recognition Technology

The founding document that sought to regulate FRT was the Consumer Privacy Bill of Rights. The CPBR designated the National Telecommunications and Information Administration to convene multistakeholder processes on a variety of privacy related issues. After conducting a MSH process on mobile application transparency the NTIA convened its second process on FRT. The NTIA multistakeholder process was also predated by an FTC workshop on commercial uses of FRT, held in December of 2011. The FTC invited "Researchers, industry representatives, consumer advocates, and privacy professionals" (Federal Trade Commission, 2011). The workshop observed commercial uses of FRT. For a month following workshop completion, public comments were allowed concerning the content. The FTC received 80 public comments from a variety of stakeholders. In October of 2012, the FTC issued a staff report entitled "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies." The report did not cover every single use of FRT, but focused on commercial uses of the technology. Stakeholders are often mindful, and in some cases involved, with previous processes and those experiences inform their positions and thought processes for the current MSH process on FRT. Understanding this history is important when tracking the creation of

the current code of conduct (Scollon & de Saint-Georges, 2012). The scope of the current MSH process on FRT is discussed later in this chapter.

The FTC recommendations from the workshop were based on a March 2012 FTC privacy report *Protecting Consumer Privacy in an Era of Rapid Change* and consisted of privacy by design, simplified consumer choice, and increased transparency. "Privacy by design" refers to the recommendation that companies should incorporate privacy protections into each stage of the development of a product. "Simplified consumer choice" specifies that companies be consistent with the context of a business relationship or transaction, or provide consumers with an alternative option at an appropriate time. Finally, "increased transparency" directed companies to make data collection and use practices visible to consumers.

It is expected by this researcher that the regulation of FRT will emerge via the MSH process. Diverse stakeholders have been invited to offer opinions and information towards developing a voluntary code of conduct. According to Patrick Erwin (2011), codes of conduct "are designed to explicitly detail an organization's commitment to CSR (corporate social responsibility) and outline expected conduct from the organization's employees" (p. 535).

7.4. The Current Multistakeholder Process on Facial Recognition Technology

The MSH process on FRT has not occurred in a vacuum. Stakeholders who are interested in participating have preconceived notions about multistakeholderism. Some of these notions may be informed by the previous MATP or experiences they have had in the past with other processes. Gaining insight into what stakeholders perceive as the benefits and deficits of the MSH process may affect how they approach the current

process for FRT. Opinions differ, but they can be grouped into two broad categories; those who perceive benefits from the process and those who have frustrations with the process.

7.4.1. Perceived Benefits From the Multistakeholder Process

Multistakeholderism encourages collaboration and cooperation between diverse interests. Often the process results in positive outcomes for most or all parties. Stakeholders have noted the diverse interests represented in the MSH format and view this diversity as a positive development. One interviewee expressed praise for the MSH process stating in an interview on October 15, 2014:

> I think one of the benefits to the MSH process is its casting a wider net. It's inviting consumer and privacy advocates, academics, in addition to my attendance there's been representatives from the Canadian government and so it seems to be putting together a wider group of stakeholders (NGO).

The diversity of stakeholders has had a positive impact helping some understand the technology better. One interviewee supported the academic literature on stakeholder learning stating in an interview on June 23, 2014:

> Well some of the benefits, clearly you are getting a much more expansive view of the technology, you're getting it from multiple perspectives, not just the perspective of individual company products or an industry association that wants to promote the technology itself without really sensitivity, necessarily, to what other people might not be as enamored to the technology, you get more breadth of opinion (NGO).

Bringing together diverse parties not only aids in understanding the technology but also in the outcome of the process, "[T]here's a benefit to having both parties at the table so there's buy-in on both sides" (Business). When parties meet to discuss issues they disagree on, they can come to solutions that both are willing to accept. This sentiment was echoed by another stakeholder, "[I]t's a longer process but the benefit is you get a lot more buy-in" (Business). There are business benefits identified with the MSH process as well.

One of the motivators for stakeholder participation can be to avoid legislation by Congress (Kolk, Tulder, & Welters, 1999, p. 152). Stakeholders have recognized that participating in the MSH process on FRT may lead to better business outcomes. The following analogy, provided by an interviewee on June 23, 2014, provides insight into this line of thought:

> [C]ongress has said, make the water cleaner. Now you can do that just by fiat, the EPA can say here's how you are going to make the water cleaner. Alternatively the EPA can get a bunch of people in the room and say "how do we make the water cleaner in a way that has the least impact on your business, has additional environmental benefits that we don't know about" There can be a lot of value in that. In other words, you want to do as little damage as possible and that's one of the things MSH is very good for. (NGO).

Business participants recognize the potential to collaborate with other stakeholders and achieve goals in ways that can enhance their business or at least limit any damaging effects to their business interests. Stakeholders are also cognizant that legislation can

often be a “one size fits all” approach to nuanced problems. One interviewee on June 24, 2014 phrased it as follows:

> Sometimes legislation has a tendency to go down with more of a hammer, than with a "let's identify the problem we are trying to address" which is discrimination. Let's say you can't use FR for purposes of discrimination. But it's much harder to get those very narrow tailored laws through. But that type of nuance is something we can achieve through the course of these MSH meetings (Business).

These comments echo the literature in that codes of conduct can create elaborate rules to resolve problems (Erwin, 2011). Both business and privacy advocates realize that Congress may not protect their interests as well as the MSH process; therefore, the threat of legislation has been a source of industry motivation to participate in this process.

7.4.2. Criticism of the Multistakeholder Process

Just as there are perceived advantages to the MSH format, stakeholders also have expressed several reservations about the format. Perhaps the most widely cited complaint about the MSH format is the length of time it can take. One business participant stated: “It's longer, it's a lot longer” (Business). An NGO participant confirmed the previous observation stating: “What you sacrifice of course is speed” (NGO). Stakeholders are frustrated with the amount of time and resources that the process demands. Participants also recognize that quality products take time to develop and they do not want to rush through the process either, “Yeah, we are trying to create something that lasts and Rome wasn't built in a day, for lack of a better phrase, and of course that didn't last, maybe not

the best analogy. But you get the point" (Business). In short, what is sacrificed in speed may be gained in creating a quality outcome.

Another frustration with the MSH process on FRT for some stakeholder groups is that its outcome is a *voluntary* code of conduct. The NTIA cannot compel individuals or groups to participate. "So we did one already on mobile app transparency. It exposed some value but also the difficulty in doing MSH absent underlying legislation. You really do need a stick to get people to cooperate" (NGO). It is difficult to achieve stakeholder cooperation for multiple reasons. Stakeholders may be reluctant to participate in order to protect competitive advantages, discreet silences (Huckin, 2002). One interviewee (September 17, 2014) was cognizant of the silence but was understanding of their rationale:

> That'd be great to get more information on their (business) process but I recognize why a company doesn't want to tell us what they are doing or planning or researching. I don't know what they would gain on the corporate side (NGO).

Observers who do not participate in the process have caused some stakeholders consternation. It is important to hear from business entities that are implementing the technology or that have plans to. Knowing what businesses plan to do with the technology can help enact privacy protections for those uses. Without this input, the efficacy of the code of conduct may suffer.

7.4.3. Convener

The role and power of the convener have been broadly discussed in the literature on MSH processes (Hemmati, 2002; Schwilch et al., 2012). In the current FRT case, two

views have been expressed in relation to the NTIA, where the convener has faced criticism refuting its stance as an impartial broker who facilitates the MSH process on FRT. The NTIA is housed under the Department of Commerce. One stakeholder noted, "[The Department of] Commerce has never historically been supportive of protecting consumer privacy. Department of commerce is an agency that protects the interests of American business" (NGO). After examining the Department of Commerce's mission statement, there is not a single mention of privacy included in the document (see Appendix D for mission statement). On the other hand, the code of conduct created will be enforced by the FTC under its Section 5 authority against unfair or deceptive practices. Certain NGOs have suggested that the FTC would be a more appropriate convener given its previous experience with the technology, as well as being the entity that will enforce the code of conduct. "We recommended it to the White House to shift it [MSH on FRT] to the FTC. The FTC recognizes that the Obama plan is basically a joke" (NGO). This individual felt that, for political reasons, the FTC was not eager to convene the MSH process on FRT; a MSH process for FRT convened by the FTC would likely be seen as redundant given their previous efforts.

Other participants, though, felt that the FTC, as an enforcement agency, may not be the most appropriate convener. One interviewee expressed his rationale in an interview occurring September 25, 2014 as follows:

> [T]he fact that they are an enforcement agency, they come at this with a certain perspective; I think you can argue that NTIA may be a better broker in this type of discussion. I think when you look at the agency or the administration's influence on the process, I think you would see a

> heavier hand in some sort of FTC process. I think NTIA has really made the best of, what is a difficult process [MSH processes generally, not FRT specifically] (Business).

In fact, FTC representatives have echoed their support for the NTIA as convener. An interview was conducted with an FTC representative occurring October 15, 2014 where she expressed the following:

> My thoughts to that are, we are observing this process and participating at the meetings but really our role would come into play when we would enforce the code or enforce against companies that said they would comply with the code and then did not. Whereas [the] NTIA is working as a convener of this process. So I think there are different roles (Government).

Despite differing opinions on which agency is the most appropriate convener for this process, stakeholders were also asked if they felt the NTIA had a particular influence on the process. Several stakeholders acknowledged the difficulty of the process and felt the NTIA has been a fair broker. One interviewee expressed the following (September 15, 2014):

> I think from my perspective the Department of Commerce, the NTIA has done a good job of bringing together… have done a good job of acting as a convener of the meetings and organizing and helping to move the discussion along amongst stakeholders. I feel like it's been a discussion amongst the stakeholders at the meetings (NGO).

It is important that stakeholders and the public feel that the NTIA, as convener, is a fair broker in this process otherwise the legitimacy of the outcomes will be questioned. Other stakeholders felt the NTIA did have a particular influence on the process. One interviewee expressed the importance of the role of the NTIA in an interview occurring June 23, 2014:

> We wouldn't be here if they hadn't convened a process. That's important. If somebody doesn't get the table and the room and get people talking and give it a cover of officialness it won't happen. [However] the NTIA doesn't have any power. They can't threaten to shut the process down and just go with the civil society stakeholder proposal unless industry brings something forward. So what they're essentially doing is trying to convene a group of people and cajole people. But… it's a tough task (NGO).

Stakeholders who felt the NTIA influenced the process indicated that the agency has added legitimacy to the process. Even though stakeholders reported influence by the convener, they felt said influence added legitimacy to the process which will hopefully translate into broad agreement and adoption about the negotiated code provisions, "we are here, giving you the venue, the time, we help convene, but we will not be an active creator of standards, that makes it a little bit slower. They have their reasons for doing it that way" (NGO.)

It is important that the NTIA is not seen as a creator of standards for the code of conduct. If the NTIA was accused of creating standards, they may be accused of negotiated rulemaking, which involves the creation of an advisory committee by an agency, the NTIA in this case, for the purpose of creating rules (Coglianese, 1997, p. 1256). Creation

of such a committee would undermine the structure and potential benefits of the MSH format.

7.4.4. Scope

The FRT meetings began in February 2014, only several months after the June 2013 Snowden leaks concerning the National Security Agency (NSA) spying on the American public. Through a series of revelations, highly publicized news reporting, and an eventual Ted Talk (March, 2014), the American public became increasingly aware of privacy issues and digital technologies. These revelations prompted some participation at the FRT meetings to address what they perceived as a legitimate privacy concern government use of FRT. However, the process was enacted to address commercial uses of FRT, and not government uses. "I just think that the NTIA has a certain jurisdiction and law enforcement is not within that jurisdiction it doesn't mean the process is invalid just that it's not as broad as people would like" (NGO).

The frustration surrounding the inability to address governmental uses of FRT have been an ongoing issue during the meetings. Business representatives in an effort to avoid regulation want the process to be constrained so that they can continue to work with government entities as a client. One interviewee noted the NTIA's role in constraining the scope of the process in an interview transpiring on September 5, 2014:

> They have done a reasonably good job keeping it contained. One of the flashpoints that keep coming up is Government access to FR data and government use of FR data, which is completely outside the scope; and different activists both left and right tried to take it in that direction and its

> combination of most other people in the room as well as folks at NTIA saying that's not our purview at all. (Business).

At first glance there seems to be a very clear delineation between government and commercial uses of FRT. However, the commercial sector often drives technology innovation, and the government frequently contacts commercial entities as a customer for the use of certain technologies. "Exactly, they [NTIA] don't want to go there and it's another example of how constrained or restrained the process is" (NGO). Other participants felt that government use could be in the scope of the process in the meeting occurring February 6, 2014:

> [W]e can talk about the role of commercial data collection in relation to subsequent uses by the government, and it would fit the structures of the purpose of the work. It doesn't run afoul of that, and I think it would make the discussion a little bit more kind of refined… it just strikes me as the right way to address the issue without restricting what the government does (Unknown).

Some stakeholders feel that government use of FRT may not be out of the scope of the process so long as the government comes to a commercial provider as a consumer. However, enforcement of a code of conduct when the government is the customer remains less clear. This has been a point of contention amongst stakeholders and the convener since the first meeting (February 6, 2014):

> The intent of this process is to implement the Consumer Privacy Bill of Rights and to draft a code of conduct that applies those top level principles to commercial facial recognition technology. When companies adopt that

> code and move forward, the FTC has the authority to make sure they keep their promises. The FTC does not have authority over government entities. (Verdi).

Some privacy advocates feel that limiting the scope of the code of conduct to strictly commercial use undermines the legitimacy of the code. Participants countered in the next meeting (February 25, 2014) that government use was needed so they could determine the overall protection level of the code. Chris Calabrese from the ACLU said,

> I understand that this group cannot regulate what the Department of Justice does or the Department of Homeland Security, that's self-evident. However, it's equally evident, at least to me, that what the department of Justice or state and local police choose to do with the technology impacts the privacy of everyone it impacts whether I want to be in a biometric system, whether I can give meaningful consent or not. So without understanding those things I don't see how I can tell anyone yes this is a privacy protective code or it isn't.

However, since the FTC does not have enforcement authority over other government entities, it remains unclear how the code of conduct would apply to the government when they act as a consumer of FRT.

Beyond contending with the U.S. government, and issues with the government as a commercial customer, many of the companies involved in FR are global. Entities such as Google and Facebook must comply with not only U.S. law but international law, as well as the laws of the countries in which they operate. For the first time, during the

December 15, 2014 meeting, a representative from Facebook articulated this multinational view stating:

> I think when we are looking at a lot of companies like Facebook, Google, and others that are multinational. We have obligations in other jurisdictions and by saying a U.S. based standard, even if it does evolve it could prove problematic if there might be different standards. I'm trying to be open-minded and look more towards the global view and hoping the code be interoperable with other requirements in other jurisdictions (Business).

The code of conduct is clearly limited to U.S. jurisdiction because of the FTC's enforcement capacity. Stakeholders must contend with the international nature of some companies while also ensuring they comply with U.S. standards. It should be noted that Facebook's initial participation at the meetings was to try and avoid U.S. regulation.

The NTIA is charged with convening and moderating the MSH process on FRT, but has also been influential in limiting the scope of what the group, and ultimately the code, will address. One interviewee (June 24, 2014) described their role in limiting the scope of the process as:

> They also helped to keep it tailored. One of the things that John Morris [Associate Administrator and Director of Internet Policy, John Verdi's boss] was lambasted about was the removal of government from this [MSH process]. But it was important to remove that at the outset because as much as we may want to limit government access… [An] industry code

> of conduct cannot regulate the federal government. That takes an act of Congress or that takes an act of the executive branch itself. (Business).

The NTIA finds itself in a precarious position around the regulation of FRT with limited ability to regulate government use, particularly after the Snowden revelations heightening public awareness about government intrusions on individual privacy. In the public's eye, failure to adequately address the concerns of the stakeholders and the public could jeopardize the legitimacy of the voluntary code of conduct.

7.4.5. Moderator

Several stakeholders expressed disappointment in the third party facilitator initially brought in by the NTIA. Others expressed increased satisfaction after the facilitator was replaced by John Verdi, the NTIA's director of privacy initiatives since 2012. As one participant put it, "He [Verdi] is night and day from the professional facilitator that we had for the first few meetings [of the MATP, April 2012]. It's pretty amazing. John hadn't done anything like it before but he is a natural facilitator" (Business). Broad stakeholder acceptance of the moderator is an important aspect of facilitating MSH processes (Hemmati, 2002, p. 222). Verdi (2014) explained his role in an interview as strictly a facilitator, he noted:

> I'm a facilitator. That's it. [T]here are different models; I'm not an active chair. There are some organizations that have an active chair that rules up or down on issues. I don't do that. I don't hold the pen on drafts. I facilitate discussion. I try to identify areas where conversation is going to be constructive. I try to help folks identify and refine areas of agreement

> and sort of work towards consensus on areas of disagreement. But it's facilitation pure and simple (John Verdi, 2014, used with permission).

Being a facilitator in this way limits the opportunities for stakeholders and observers to claim that the moderator is influencing the process. Verdi has been explicit about his role with stakeholders which is another important aspect of facilitating MSH processes. Verdi also has a background in computer programming, privacy advocacy, and is a lawyer, so he is "representative of the various stakeholder groups" and has valuable knowledge that contributes in identifying issues and promoting consensus (Hemmati, 2002, p. 222). Contrarily, an approach that is too involved also caused problems with the previous process on mobile apps. Verdi may be aware of his role in facilitating the process due to his previous experience as a privacy advocate.

John Verdi remains the moderator for the MSH process on FRT. It is important to note that Verdi could be seen by some stakeholders as inherently biased. Formerly, John Verdi was senior counsel at the Electronic Privacy Information Center (EPIC). EPIC is an important non-profit organization that advocates for privacy self-described as, "EPIC is an independent non-profit research center in Washington, DC. EPIC works to protect privacy, freedom of expression, democratic values, and to promote the Public Voice in decisions concerning the future of the Internet" (Electronic Privacy Information Center, 2015b). Despite being a former privacy advocate, stakeholders seem receptive to Verdi moderating the meetings. During the current process, stakeholders have expressed positive sentiments about John, stating. "I respect John; he has done a really good job in a difficult position in terms of having to corral a lot of people with different viewpoints and can be hostile" (NGO). Having broad stakeholder support for the moderator is

certainly a positive aspect of this process, especially considering that the animosity towards the previous facilitator had a negative impact on the MATP. Stakeholders kept the moderator who was productive at facilitating the process, an action drawn from historic results (Scollon & de Saint-Georges, 2012).

Beyond having a personal affinity for Verdi, stakeholders attribute positive facilitation of the meetings to his moderation style. His facilitation of the meetings has been described in the following terms: "I feel like John Verdi and the NTIA have been very good at trying to speak with everyone and get everyone involved and make sure people are heard and run the meetings so they are efficient" (NGO). The previous observation was confirmed by another participant who stated, "I think John Verdi has done a really good job of trying to make it much more inclusive" (Business). Stakeholders seem to not only appreciate Verdi, but the NTIA's job of inviting stakeholders and making their contributions heard and valued. "I applaud John Verdi for being able to facilitate such a diverse group" (Business). Verdi seems to have garnered the respect of many participants involved in the process

7.4.6. Participation

As with the MATP, issues of participation again cropped up in the FRT process. There are other groups that some feel have been left out. "There's no minorities, there's no academics. The NTIA has been just terrible. The NTIA is a creature of the industry ultimately and the NTIA has no courage, no interest" (NGO). These comments are directed at the NTIA because they are housed within the Department of Commerce, which is mandated to support American business. No minority advocacy groups have been explicit about their participation in this process; the groups closest to representing

minorities would be the ACLU and Common Sense Media. As to the statement that there are no academics, this is patently false, but there are individuals who would like more presentations from academics to be made in order to increase stakeholder-knowledge on the issues and technology. Susan Grant of Consumer Federation of American explained to the group in the meeting occurring April 29, 2014 that companies who operate/employ FRT are missing from this process:

> As you know I wasn't thrilled with the last process, but at least we had active participants from the mobile app community. We don't have the active participants that we need in this [process]. We've got the vendors, but I think very little of this has to do with the vendors actually and more of it has to do with the users of facial recognition and we don't have them actively participating (NGO).

Google was noticeably absent for the entirety of the process, Facebook has been mostly absent, and both have been a source of concern for some stakeholders. There are two ways of addressing the silence that Google and Facebook have exhibited. These businesses would describe themselves as employing discreet silences in not wanting to reveal sensitive business practices (Huckin, 2002). Conversely, these companies can also be viewed as employing manipulative silences to deliberately conceal current or future business practices that they wish not to fall under the code of conduct (Huckin, 2002). "[W]ill the NTIA ask that Google and Facebook present for the next session" (NGO). This question was immediately followed up in the next meeting on March 25, 2014 by Jeff Chester from the Center for Digital Democracy:

> I have a question John. At the last meeting I, and I think we were seconded by several others, asked that Google and Facebook come to this meeting to talk about what they do in terms of commercial recognition given the fact [that] they are market leaders, to explain what they do and what they plan to do. When we talked yesterday you told me that you did request that they speak and that they declined (NGO).

Despite the NTIA making the requests, the MSH process is voluntary, thus facilitators cannot compel groups to come forward and share information. As previously discussed, businesses have legitimate reasons to keep proprietary information private to protect their competitive advantage in the marketplace.

There have also been issues of false or incomplete representation among stakeholders.[27] There has only been one instance, so far, of a stakeholder misleading participants as to the totality of the constituents they represent, a manipulative silence (Huckin, 2002). While this was a brief point of contention, it was most likely known by all stakeholders involved in the MATP that Mr. Sperapani represented the Application Developers Alliance, which "[I]s a non-profit global membership organization that supports developers as creators, innovators, and entrepreneurs. We promote the continued growth of the industry and advocate on behalf of our members on public policy and industry issues" (Application Developers Alliance, 2015). Misrepresentation could cause confusion or lead to animosity amongst participants as was seen in the MATP.

[27] "Chris Calabrese- I'll ask a moderately pointed question. You introduced yourself as Tim Sperapani concerned citizen, are you representing app developers who want to adopt a code as part of this process." Tim Sperapani- "Yes and they do want to adopt a code"

7.4.7. Expectations

During the meetings, the moderator has repeatedly stated that the goal of the CPBR and the NTIA is a voluntary code of conduct for FRT to protect consumer privacy. This goal has been questioned by Chester and by the convener at the March 25, 2014 meeting.

> This is a stakeholder driven process. What we just heard [is] that the NTIA goal, the administration's goal, is to develop a code of conduct. But… if the stakeholders decide that it's too premature… to develop a code, then won't in fact [the] NTIA and the administration simply accept the will of the stakeholders?

This was the first occurrence of a participant questioning the stated outcome of the process. NGO participants have expressed a strong desire to provide consumers with robust privacy and data protections, if that cannot be achieved they are unwilling to endure the process for a result that will question their legitimacy and abilities in the eyes of their constituents. The fact that the process could end without achieving the stated outcome after only three meetings caught the moderator off guard. Verdi countered, "It's a stakeholder driven process… with the goal of developing a code of conduct. Is your goal to develop a code of conduct or to not develop a code of conduct?" Jeff Chester (Center for Digital Democracy) responded in kind stating:

> My goal is to protect privacy. But I'm certainly not willing… I could not be railroaded to do it because that would not be dealing with the public interest that I hold in my job. So it's a stakeholder driven process with conditions and that's quite interesting.

At this point the ACLU decided to support the notion that acceptable privacy protections must be achieved by this process or the NGO participants could not participate further. Calabrese stated:

> I think Jeff's got a point. Fairly stated, the end goal is to advance privacy through a code of conduct. However, if the stakeholders can't do that then we won't have a code of conduct. You know, I think that goes without saying doesn't it?

The exchange clarified that everyone had the same expectations; to create a code of conduct. The discussion also highlighted the power stakeholders have to ensure a strong code of conduct is created, particularly one that protects consumer privacy. Expectations were again questioned as issues of representation cropped up later in the same meeting. Rather than scrap the process if a code of conduct could not be created Susan Grant proposed an alternative way forward.

> I'd like to make a constructive suggestion picking…if we shouldn't be thinking more in the way of principles and less in the way of a code of conduct, that we have no indication that the real players here are going to help fashion and adopt anyway.

Grant was unsure that the current expectations for the group could be met and tried to further privacy protection via less formalized principles, similar to the best practices issued previously by the FTC.

7.5. New Strategies Adopted to Encourage Stated Outcome Success

As stated in the MDA discourse, historic positions and actions can affect the actions presently taken by individuals, thus understanding how the historic results affect

future action is important for the present study (Scollon & de Saint-Georges, 2012). The current MSH process on FRT has had the benefit of learning from the experiences of the previous effort on the MATP. Some stakeholders have been involved in both of the processes. One of the frustrations with the last process was the limited adoption of the created code of conduct. Participants voiced varied opinions about the final code of conduct and its adoption. Some participants were convinced it the process was wasted, "It wasn't adopted at all" (Business). Others felt there was limited adoption, "I think there were only two or three companies that signed on" (NGO). The most positive comment regarding the previous code of conduct was this, "So we came up with something and that was fairly successful" (NGO). Current stakeholders are cognizant of the limited adoption of the previous code of conduct and have been mindful of trying to improve the adoption rate. "I'm also coming from it from the angle of I don't want to see it end up where the last approach did where basically only one company signed on, because the document was that unworkable" (Business). These comments suggest that stakeholders are aware of the results of the previous process and are willing to pursue strategies that will encourage wider adoption of the code of conduct for FRT.

7.5.1. Personal Communication Strategies

Since the comments from interviewees and individuals during the meetings suggest that many stakeholders had a negative experience during the first process, stakeholders skeptically entered the second process. One potentially positive outcome from the first process is that the stakeholders learned what processes help develop a code of conduct and which do not. Learning about the process was as important as learning about fellow stakeholders.

Learning about other participants is also important. The NTIA also learned the importance of having a moderator who can manage the process in an effective manner. Stakeholders involved in both processes have been mindful of the importance of respectful communication, as well as learning about the organizations and their goals. These previous experiences align with certain aspects of capacity building discussed in the literature. With these experiences in mind, stakeholders took steps to ensure that they had a more positive experience with the second process. "I think everyone's been very respectful" (NGO). "It's gone a lot better than the last one so far" (Business). Stakeholders appear to have adopted new modes of conduct and interaction with one another to create a more positive and productive atmosphere. "I don't think people are being willfully problematic this time around and I appreciate that" (NGO). Stakeholders have strategized ways to compromise and are respectful of diverse views. While mostly negative feelings about the MATP persist, stakeholders appear to have put that experience largely behind them and are creating an atmosphere of "good faith."

Stakeholders have changed their approach to the MSH process in several ways. From the comments listed previously in the MATP, it is evident that there was animosity in the room; one stakeholder went as far as to call other participants "pretentious." However, the FRT process has resulted in a different group dynamic as reported by in one interview occurring August 6, 2014.

> At the last process I think some people's reputations hampered their ability to make their points. There were a few people on the mobile app that were obstructive, or oppositional, or to prevent any compromise from happening. Those people were not seen favorably by the group (NGO).

Participants seem conscious of the fact that to achieve a positive outcome they need to engage respectfully with one another.

7.5.2. Decision Making Strategies

Aside from participants being respectful of one another, stakeholders changed the way that they make decisions throughout the process. For instance, they found during the first process that voting on a finalized code of conduct at the end created arguments and limited adoption. However, they changed the format for the process on FRT as noted by Carl Szabo of NetChoice at the November, 6 2014 meeting:

> One of the nice things I think we have done this time around, and the lessons learned, is we have avoided putting the cart before the horse like I think we did last time. Last time, a couple people quickly ran to the pen and started writing a code of conduct and then we started talking about the big issues and that's where things broke down. That's why I think you have seen so little adoption as we have from last time.

Stakeholders learned that this decision making approach hampered the creation of an effective code of conduct that could be widely adopted by companies. This comment also acknowledges the learning that has occurred amongst the stakeholders. The importance of learning in MSH processes cannot be overstated as "MSPs will *only* [emphasis added] work if all participants are willing to learn from each other. (Hemmati, 2002, p. 53). Having an insular group drafting language was not effective, thus "Going forward in this process we are trying to completely avoid that" (Business). Stakeholders have learned from their past mistakes, thus have changed the way that they make decisions in the MSH process for FRT.

By avoiding insular drafting groups, stakeholders hope the adoption of a new decision making process will achieve wider acceptance of a code of conduct. One interviewee described the new decision making process on September 5, 2014:

> [T]he benefit of going through that mess [MATP] was learning what works, how to work together to find common ground, how to work towards that common ground between parties that tend to not cooperate on anything. It was a very long painful dry run to work out a lot of the things that don't work. The key thing that was dropped…was the idea of having a small group of people who were designated as the drafting team (Business).

Stakeholders have adopted a more piecemeal fashion of making decisions on multiple smaller issues rather than one comprehensive code. The new decision making process has evolved in stages. The first stage identifies an issue the group thinks they can come to an "easy" or relatively easy consensus on. This is a best practice cited in the literature: "It was recommended that MSPs should always tackle the easiest objectives and common ground first in order to build trust and pull out some real initial achievements; then it can start to face the more contentious areas" (Hemmati, 2002, p. 116). Then individuals draft code language on that issue, where individuals volunteer based on interest or specialized knowledge. The draft code language is then brought back to the group to decide if consensus can be reached. Assuming consensus is reached, the language is "frozen" and stakeholder groups can take it back to their constituents for comments and suggestions. This point was explained in an interview occurring September 5, 2014 as:

> There have been sort of small groups of people that have gotten together to hash out lists, they don't make decisions but they make lists. What are the things we need to worry about on topic X. So you have a group of people working on definitions and coming up with common definitions that the group can look over and work on. Eventually perhaps agree on (Business).

The definitions list is included in Appendix C for illustrative purposes. This approach has been supported by a number of stakeholders. Bill Baker of Motorola supported the notion at the April 29, 2014 meeting stating:

> What I might prefer we have, is a point of where we have little drafting committees taking on pieces of it instead of one drafting committee taking on the whole thing which I didn't think was a particularly good way of getting it done last time.

Stakeholders have decided to have multiple working groups for issues. Participants hope that having multiple small groups working on issues will achieve broad consensus not experienced at the MATP and produce better outcomes. Evidence suggests that certain stakeholders are happier with this approach: "It's gone a lot better than the last one so far" (Business).

Stakeholders are not the only groups who have supported a change in the decision making approach. An interview respondent explained it as follows (September 25, 2014):

> This time around I think NTIA has been careful not to have groups come to the table too early with a complete code which then becomes the base

> draft. Instead trying to piece that together as more section by section and more based on where the group can find consensus. I think to their credit they are trying to be a little more, I don't know inclusive in the drafting process (Business).

Stakeholders would soon learn, however, that the new approach was not without its own set of problems.

Some stakeholders expressed frustration with the smaller groups. "One of the problems with this process is that there's no executive committee or a designated group of people to actually draft something" (NGO). Despite not having a designated drafting committee, other participants felt that drafts would still get done, "My experience last time is the way this tends to work is you find a couple of people on the same page as you and you look for some buy in. That may not work on a piece by piece basis" (NGO). A fragmented approach lacks a complete document to work with and has resulted in new frustrations such as increased length of the process. Walter Hamilton, of the IBIA, at the December 15, 2014 meeting noted:

> I might also say that… I have no real issue with most of the language that is there, but it's me speaking for myself. We have not had… [an] opportunity to go back and fully vet this language, or the code in general since this is a piecemeal approach, with our members and down through our members to their customers where there could be legitimate concerns expressed about various aspects of this. That's where we are today.

Without a complete document it is difficult for stakeholders to take anything substantive back to their constituents. Since some stakeholders represent several companies

soliciting all of their opinions and meaningful comments is very important. "This demonstrates the need for participants to work closely with their constituencies, particularly in MSPs which aim at agreements and implementation" (Hemmati, 2002, p. 117). A third decision making process was suggested to avoid previous problems and any current complications that may arise from the new fragmented approach.

To avoid the problems of the MATP as well as the complications arising from the disjointed format adopted in the FRT process, it was suggested that the NTIA hold the pen as an independent unbiased body. Yet, there are limits to what the NTIA feels comfortable contributing in this process. The NTIA has defined their role in the process and self-imposed not drafting language for the group. Verdi in the November 6, 2014 meeting stated:

> I actually don't have authority to say NTIA can pick up the pen on something like this. To be honest, it makes me a little nervous to have NTIA do much more than we have which is group issues, figure out related stuff, mechanical fair broker type process. That is something I'm comfortable doing because I think it helps the group move forward and I'm using stakeholder language. In terms of NTIA picking up the pen and creating language, my suspicion is that will cause angina. I don't know that's the role that we are best situated to play in the process but I am happy to take it back.

This suggestion received resistance from other stakeholders, particularly Szabo of NetChoice stating:

> I was going to second your comments just from the optics of it. The optics of the government, it might be misconstrued as the government is creating a privacy policy, can we really trust them after all the issues that they have had recently.

The suggestion for the NTIA holding the pen on a complete code of conduct was not adopted. In fact, the opposite has tended to be the case; rather, the NTIA has been instrumental in getting stakeholders to hold the pen on various issues. "But who wants to take the pen on this?" "Others who want the pen?" The NTIA has been vocally hesitant to even appear to hold the pen on any issue. Verdi offered an alternative option stating:

> A third way to do this is I can comb through I, John Verdi, can comb through the documents submitted by stakeholders and other principal documents submitted…and put together a combined document which won't look like a rational code and isn't me holding the pen because I will just copy and paste.

This supports the position of the NTIA as strictly a process facilitator. The NTIA has the difficult job of moving the process forward while traversing diverse views and a complicated past with the MATP. It makes sense some participants would want the NTIA to hold the pen to avoid the drafting problems experienced in the MATP. However, if they do create the draft language, it would no longer be a stakeholder driven process and would detract from the legitimacy of the MSH format. The NTIA has been mindful of both of these views and has struck a middle ground between them by compiling comments received from stakeholders; in doing so, they help to facilitate and move the group forward, while maintaining transparency and adjusting any language

submitted in view of the whole group. In fact, Verdi has the webcast cameramen show before and after screen shots of code language so that viewers at home can see what has been changed. Providing this level of transparency and facilitation is a good compromise between holding the pen and maintaining the legitimacy and benefits of the MSH format.

7.6. Complications With the Multistakeholder Process on Facial Recognition Technology

7.6.1. Disparate Opportunities to Participate in the Decision Making Process

Despite adopting new strategies for making decisions, not all stakeholders have had equal influence on the process. The meetings can be "attended" in one of three ways: physically, via telephone, or via webcast streaming. These three methods are employed to facilitate convenient access to the meetings. An unintended consequence of these modes of access is stratification of participation, and thus influence.

Ease of attendance and financial travel savings are not the only advantages for stakeholders who can physically attend the meetings. "Unfortunately, when you are on the phone you have about one tenth the ability to interact and such" (NGO). An interviewee provided further insight (October 15, 2014):

> I think you are limited by calling in mainly because it's hard to break into a conversation that's going on among a bunch of people in a room if you're on the phone. I also think you are a little more limited because it's hard to maintain focus for four hours if you're on the phone (NGO).

Through meeting observation, participants are able to monitor the process and contribute over the phone, but in limited ways. Attendees in the room can speak into the microphones located at their seats at almost any time they desire, though there is usually

an order designated by the moderator. For phone participants, the moderator designates to the operator when to enter "Q and A" mode where phone participants can be heard by the rest of the group. Callers are muted by the operator when not in "Q and A" mode. Additionally, stakeholders who monitor the meetings via the streamed webcast have no opportunity for interaction with the proceedings, as there is no way for webcast viewers to communicate with the group. Therefore, stakeholders who are able to physically attend the meetings have a distinct advantage if trying to influence the process.

The NTIA has done a good job of being inclusive and inviting diverse stakeholders according to participants. Various communication channels, represented in the NTIA meetings, all have distinct advantages and disadvantages. Electronic communication has the benefit of "neutralizing differences in status and personality as related to gender, age and ethnicity" (Hemmati, 2002, p. 87). Electronic communication also focuses attention on the content of the communication rather than the subject. However, electronic communication also promotes heterogeneity in the group and may be ideal for gathering diversity of opinion on a given matter (Hemmati, 2002, p. 87). Since the NTIA will convene another MSH process on drones, they should consider adding an interactive component to the webcast so that online participants can more effectively engage with the process.

7.6.2. Perceived Representation Issues

The NGO representatives in the FRT meetings have voiced concerns to this researcher that they lack the resources of industry members (August 6, 2014).

> There are two advocates in the room, not everyone can be at every meeting. There probably isn't more than ten of us. [There are usually 40-

> 50 participants in the room at any given meeting] I think we are outnumbered by other interests. We don't have the capacity to monitor on the advocacy side. Everyone who goes has to be strategic about what they are doing (NGO).

NGOs continued to discuss their limited resources stating, "In addition there are about five or six advocates and the rest more or less are from industry. Of course the advocates, not only do we have small organizations but we are dealing with multiple issues" (NGO). As the literature has shown, privacy is a complicated issue that is of primary concern in many venues, thus advocates must choose strategically where to deploy their resources. However, other stakeholders, representing business interests, do not view numbers or resources as an issue. These stakeholders contend that bringing value to the discussion is the most important aspect of a stakeholder's participation, a position supported in the academic literature (Mitroff, 1983). If a stakeholder can contribute to the discussions meaningfully then they will be heard, regardless of who they represent or what their resources are. An interviewee expanded on this view stating (September 5, 2014):

> There is a guy, an elderly man who is a consultant, he is extremely cranky but he has been an interesting addition to the mix. He doesn't represent anyone other than himself but he speaks up and he has sometimes very useful things to add to the process and therefore he is influential. It doesn't matter; do you bring anything of value? Do you bring value when you speak and participate? That's the most important thing (Business).

There are differing opinions present about representation in terms of numbers and representation, in terms of value added to the discussion. Stakeholders are generally referred to in the literature in terms of unique knowledge, experiences, or resources, not in terms of their numbers (Gray, 1989; Mitroff, 1983). Participants can add value to the discussion in a variety of ways, including expertise, practical solutions to implementation problems, and clarification of diverse views, all of which can help facilitate consensus. One participant's contribution in the meetings is to clarify complicated views that appear to be oppositional. However, he is usually able to strike a compromise. Hearing from groups that would actually adopt the code of conduct is an important part of the process as well.

Those who are to adopt the code of conduct need to be represented and have their input heard. This view was expanded upon in the first meeting (February 6, 2014).

> I mean my recollection of the previous one [process]… a lot of people that weren't involved in it. And I think it would be a really good idea to make sure that everyone that might be impacted by this, [code] because even though it's not a regulation the people that might be encouraged to adopt it, ought to all try to be in the room…(Unknown).

In the MATP, the late participation of groups who were to adopt the code of conduct produced a multitude of problems in adoption of the code; stakeholders for the FRT process remember these issues and have tried to incorporate stakeholders who would adopt the code from the beginning of this process. Despite their efforts, there is a continuation of this trend as many potential adopters have yet to provide meaningful input into the process, at least initially.

7.7. Towards Creating a Code of Conduct

As a result of the efforts to increase respectful dialogue between stakeholders and adopt a more effective decision making process, stakeholders are more satisfied with this process than the MATP. Respectful communication has led to stakeholder collaboration on draft code language, as well as offline meetings to discuss differing views in an effort to reach a compromise on issues.

Part of the benefit of a negative initial start is learning which processes are most effective at creating a code of conduct (Scollon & de Saint-Georges, 2012). The last process involved a group of people drafting code language and then conducting a group vote at the end. This process was not productive in creating a code of conduct. Marking the differences between the two processes highlights effective strategies for future use.

The FRT process has differed from the mobile app process in that the group has decided to tackle issues in a piecemeal fashion, whereas the last process had a small group bring back a complete code to the group. The moderator has suggested and directed the group toward issues that appear to lend themselves to easier consensus, so called "low hanging fruit." Parties who are interested in a specific topic or topics have the ability to form a small group to develop draft language; afterwards, the entire group can add comments or suggestions and vote on whether it is acceptable. While this way of creating a code of conduct may be easier to reach consensus on, there have been some concerns about where to include certain items in the code. Stakeholders are concerned that as items are tabled for inclusion into other sections of the code of conduct, they may be forgotten.

Once sections of the code come back from the drafting group, they are presented to the group. If the group approves the language initially, it is "frozen" so that stakeholders can take the language back to their members and receive comments from their constituents before the language is finalized for the code of conduct.

7.8. Conclusion

The regulatory regime of FRT is emerging via the MSH format. Stakeholders have experienced a variety of challenges, creating a voluntary code of conduct that includes representation issues, disparate opportunities to influence the meetings, limited regulatory scope, and differing views of expected outcomes. The process has succeeded in bringing together diverse groups to holistically represent the technology and its capabilities. Stakeholders have worked to adopt productive strategies for creating regulation, including respectful discourse, completing small sections of code that can be agreed on instead of decision making from a completed code perspective, and early interaction with representative stakeholders. Although the process is far from completed, stakeholders have expressed positive sentiments about the FRT process and its expected outcome.

CHAPTER 8

REGULATION OF FACIAL RECOGNITION TECHNOLOGY

In this chapter, I will discuss the development of regulations for facial recognition technology. This development has been influenced by the knowledge obtained from experts, as well as discussing the various modalities of FRT and the privacy implications that are attached to each use. Extensive discussion of these privacy implications are covered in chapter nine. Stakeholders continue to grapple with issues related to providing appropriate consumer privacy protections.

As discussed earlier, stakeholder learning is a continuous part of the multistakeholder process and an intangible outcome of the proceedings (Argyris, 1976; Held, 2006; Gray, 1989; March, 1991; Roome & Wijen, 2006). The first part of the MSH process on FRT, between February and April 2014, was dedicated mostly to exploration learning or seeking new information on the technology (March, 1991). Not all stakeholders entered the process with the same amount of knowledge regarding FRT. In the first few meetings, stakeholders spent a majority of their time listening to technical experts reporting on the capabilities of the technology and had the opportunity to ask questions. In an effort to learn more about the technology, stakeholders wanted to know where the technology was deployed, how it was being used, what the anticipated future uses were, along with other relevant contextual information.

8.1. Deployment of Facial Recognition Technology

At the first meeting, February 6, 2014, Microsoft presented to the group about their use of FRT, which they utilize in their Xbox gaming platforms. Specifically the game system works in conjunction with Xbox Kinect.[28] Kinect tracks the game player's body movements and has the on screen character mimics the users; for example, if the user jumps so does the onscreen character. Microsoft built a user notice into the system that alerts the user to the use of FRT, which operates via a colored light on the gaming system. Microsoft also allows the games to be played without the use of FRT, so users can turn it on and off as they see fit. However, Kinect also includes an audio detection component that is always on, "In fact, the new camera and microphone system is so sensitive to your presence, that Microsoft says the new Kinect can even read your heartbeat while you're exercising, and recognize and process audio that's personalized to specific individuals" (Sottek, 2013). Notice and choice, as well as the ability to turn FRT on and off, are important concepts that merit their own discussions and will be addressed later in this chapter.

At the second meeting, February 25, 2014, Marc Vaillant from Animetrics informed stakeholders of the accuracy of the technology currently deployed as well as the factors that affect the accuracy of FRT. Vaillant discussed technical aspects of FRT including lighting, pose, false positives, false negatives, and other confounding variables to accuracy discussed previously in chapter two. Depending on the application, there are reasons to have higher and lower accuracy rates.

[28] Xbox Kinect is an add on product to the Xbox gaming system and works by utilizing a camera to track body movement, gestures, and even voice commands.

Noticeably absent from the meetings were two of the largest companies deploying FRT: Google and Facebook. Facebook finally contributed to the meetings on December 12, 2014. Their unwillingness to present has been a source of frustration for some stakeholders. Nonetheless, several other companies presented information to the group about the usage of FRT and its best practices.

At the third multistakeholder meeting, March 25, 2014, Alessandro Acquisti from Carnegie Mellon University presented a proof of concept study. In this study Acquisti determined a student's identity while they filled out a three page privacy survey. His experiment proceeded in several stages:

> So the first experiment, online to online, the idea is we use data from social networks, where people use their names to identify profiles on dating sites where people do use their photos because [if there are] no photos, no date. But they don't use their names because there is still a certain social stigma associated with using online sites for that (Aquisti, 2014).

Our identities are negotiated in the physical world but also online. Acquisti notes the importance of selective anonymity online. Consumers reveal a great deal of information about themselves via social networking sites and yet value a certain amount of anonymity in certain online interactions, in this case online dating. The experiment tested whether an individual could reveal personal information and still remain anonymous:

> Now clearly our goal was not to expose these users. Rather, it was to see whether it is even possible to remain anonymous online if you are using your face. And, therefore, if you make yourself trackable across different

> sites. [In] this approach we identified one out of ten dating site members (Acquisti, 2014).

As this experiment shows, an individual's face has the ability to link known profiles with anonymous profiles online. Currently, the technology is limited in its ability to make these linkages, but as the accuracy of the technology continues to improve, and as consumers continue to upload dozens of images of themselves online, we can expect anonymity, and privacy by extension, to erode. However, this technology is not limited to just exposing anonymity online:

> Now the second study was offline to online. The same idea only now the anonymous photo was taken from offline specifically from students walking in a campus building. The subjects were asked to sit in front of a desk and we took three shots of them using a cheap webcam. Using this approach we identified one in three subjects in the second experiment (Acquisti, 2014).

As the second experiment demonstrates, FRT possesses the ability to take anonymous individuals in the physical world and identify them via content they have posted online. Before FRT, individuals involved in unpopular speech or found in compromising situations could expect to remain anonymous; however, now with cloud computing and a camera phone these individuals can be identified.

Losing anonymity, and by extension privacy, is a compelling enough reason to be concerned about the accuracy and increased utilization of FRT but the technology can also reveal additional sensitive data. In a previous proof of concept study Acquisti and colleagues demonstrated an ability to predict social security numbers from profile

information found on social networking sites. In his follow up study Acquisti was able to derive a social security number from an individual's image.

> In other words, can we predict a social security number from a face? And the answer is yes. It's difficult of course, the accuracy as you can see keeps degrading. Its proof of…. a broader phenomenon that I call data accretion. The term is beautiful term that is not due to me and due to Paul Hall a scholar at the University of Boulder Colorado. It's like money an investment accrues over time, data, personal data, accrues across databases (Acquisti, 2014).

Often we feel the information that is collected about us is innocuous. Since the information is viewed as benign we reveal this information for our personal benefit a perfect example of, privacy as commodity. Acquisti's experiment showed that data accretion, when properly analyzed, can reveal sensitive information, such as sexual orientation, political affiliation, credit score, and other sensitive details about an individual. More concerning still is the reality that this can currently be done using technology available to the public:

> [T]his iPhone app uses the iPhone camera to take a shot of the person in front of you and then it does what the experiment did but does it in real time. So [it] takes a shot, uploads it to the cloud, the cloud the server based part of the app tries to find a match between faces from social media and the shot coming from the iPhone. And then if it finds a shot now with the presumptive name, with the presumptive name…tries to find demographic data…tries to predict the SSN and then it sends this

> information back to the phone all relying on the face of the person. This is what I'm referring to as augmented reality (Acquisti, 2014).

This example highlights some of the capabilities of FRT. Both of the studies referenced above can now be reviewed in detail,[29] but at the time of the presentation the latest experiment was unpublished.[30] Researchers can track people across the Internet, destroying virtually any sense of user anonymity. Anonymity, which is highly valued on online dating sites, is being eroded with the use of FRT and readily available technology. While FRT may have some obstacles to overcome to be viable in real time, the technology is developing rapidly. According to Acquisti (2014), "The federal program which tries to standardize the performance of facial recognition in about 14 years improved by almost 3 orders of magnitude." If this trend continues, FRT may be viable in real time in the near future.

Acquisti's experiment is impressive but is not how the technology is regularly used today. FRT is commonly used for 1) face detection 2) authentication and 3) identification. One of the most popular uses of FRT is authenticating identification credentials. Russell King from Picasso, a company involved in authenticating identifications, also presented at the March 25, 2014 meeting. King said, "Picasso provides solutions for both identity management and identity assurance."

---

[29] Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National academy of sciences*, *106*(27), 10975-10980.

[30] Acquisti, A., Gross, R., & Stutzman, F. (2014). Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, *6*(2), 1.

Picasso is headquartered in London, but also has offices in the U.S. (King, 2014). Unlike the one to many matching scenario presented by Acquisti, Picasso does one to one matching for authentication purposes as King explained:

> We take a government issued ID…We actually extract data from the ID and we then compare the photo on the ID with a live individual looking at the camera. That provides a level of confidence to our clients that they in fact have the individual they are purporting to be. Performing the one to one match is not all that useful if the identification document is forged. Picasso also looks at various features on the identification credential to ensure it has not been tampered with.

Most modern passports contain a chip that contains the individual's face and personal information (King, 2014). Picasso has the ability to read the chip. The chip also has information from the issuing authority that can verify that the chip belongs to the appropriate document (King, 2014). One of the main uses of the Picasso platform is for airport security, but they are expanding into other areas.

> So the purpose of our products is to simplify the onboarding experience of a consumer, as well as elevating the level of assurance to our client that the customer is who they say they are. Within a healthcare capacity, it's patient assurance, which is a clear patient safety issue. Unfortunately, we have a tendency of having multiple patient records. The ability of biometrics to reduce the exposure to that sort of issue is quite a useful and powerful proposition (King, 2014).

FRT has the ability to help reduce fraud, increase security with increased authentication confidence, and prevent gambling addicts from entering gaming facilities if gambler so chooses. Picasso is only one company in the FRT space, but many other companies are employing FRT for different uses.

During the next meeting, April 29, 2014, Brian Brackeen CEO of Kairos, presented on how his company uses FRT.

> We focus only on facial recognition in the commercial space, so very germane to these discussions. We do it for a number of types of customers. Facial recognition via a time clock product…we capture the image with the person kind of saying take the button, up to the cloud, back down, we've identified you and then you're checked in. That data then goes into the company's payroll system (Brackeen, 2014).

Payroll is only one finance area in which Kairos is involved. Worldwide, credit card fraud is a yearly hundred billion dollar problem. Kairos has introduced a product they call Kairos Trust to help combat credit card fraud by utilizing FRT; this product is expected to be introduced soon. Despite the firm's development just two years ago, Kairos has already had an interest in their products from over 320 companies (Brackeen, 2014). The products that these companies are potentially interested in vary greatly. During the meetings, Brackeen discussed the utilization of FRT by a cruise ship to help organize photos taken during vacations. However, the same technology can also be utilized to provide physical safety to customers and not just for mere convenience.

> Another example… is a hospital, a private hospital, it's a children's hospital actually. What they do currently is, when you go to check in,

> when you walk in any one of the doors, you give them your ID, they take a picture, the picture kind of gets printed onto your badge and that's generally how they know that people aren't on like a Meagan's Law list or things of that nature. There are also other certain doors, like ER and some other kind of back doors where there aren't guards present because they are either not used very often or because in an ER situation you don't want to stop people coming in. So there's a concern that there could potentially be predators sort of intentionally going into these like soft openings and soft doors. (Brackeen, 2014).

Age is a factor that determines whether FRT will be used or not. In the cruise ship example, FRT is only used on passengers who are the age of majority, 18 in most jurisdictions. In fact, Kairos does not accept clients who would use FRT on minors.

These three presentations constituted the bulk of the commercial uses of FRT presented to the group. Stakeholders identified numerous concerns about the possible uses of FRT; these will be discussed in detail later. Age was identified as an important concern to the NGO stakeholder group. NGOs asked for further presentations on the intersection of age and FRT.

Adriana Galvan, from UCLA, presented information on the brain maturation of adolescents at the July 24, 2014 meeting. Her presentation included information on adolescents, now to include college aged individuals, particularly concerning their decision making process and their perception of rewards and consequences.

> It's meaningful because a more excitable reward system means that people in this age group are more responsive to incentives. In other words they

> will work towards receiving incentives than other age groups with less consideration of consequences associated with those behaviors. They are more susceptible to social rewards and this includes faces (Galvin, 2014).

Common Sense Media was an NGO partly responsible for Galvin's presentation. In a consumer context adolescents present a troubling case because they are not of the age of majority yet they typically have access to money making them valuable consumers to commercial entities. Other research referenced in the presentation showed that adolescents' brains were more excited when presented with faces than children or adults and this made them susceptible to wanting social rewards more. Galvin continued noting:

> So all of these factors have implications for policy and thinking of ways adolescents should be considered a special developmental periods when making choices or regulations for adolescents. The development of an adolescent appropriate policy is critical… adolescents benefit from explicit examples of consequences. Abstract concepts are still challenging for them to appreciate. Adolescents need time to think before they act. They need to be given the tools to allow them to consider consequences to think about how their reward and behavior may influence later outcomes. It's important we provide the scaffolding they need (Galvin, 2014).

Fairly stated, Galvin's research underscores the goals of Common Sense Media, to provide special protections for children and adolescents in the code of conduct. A one size fits all code would simply fail to address the special treatment that developing minds need for robust consumer protection.

Since adolescents have limited ability to recognize long-term rewards and consequences, the deployment of FRT around minors may need special consideration (Galvin, 2014). It is easy to imagine that advertisers may want to take advantage of the youth market by combining peer pressure for products, showing individuals that their friends are wearing or using certain products. The previous research shows that minors are more excitable when they see images of people they know, including friends wearing or using various products, combined with their limited ability to grasp long-term rewards or consequences and it may be quite easy to persuade minors to purchase products or services.

While it is relatively easy to imagine advertisers or businesses targeting minors for their products, it is harder to imagine a code that can appropriately address these concerns. The previous research shows that the adolescent brain is not fully developed till age 25 or 27, yet adolescents become legal adults at age 18 in most jurisdictions. The issue of adequately protecting adolescents becomes more difficult when factoring in intelligence and emotional maturity differences present at each age. Presumably, a code of conduct for FRT can only cover "adolescents" until age 18 when they legally become adults, yet this leaves many vulnerable years for young adults with regard to FRT. Perhaps the stakeholders will address the gap when they discuss adequate notice and transparency that must be given to consumers by companies using FRT.

Age is not the only sensitive demographic characteristic which FRT is able to detect. Some NGO stakeholders worry about what was initially called *facial profiling*. The term facial profiling drew immediate criticism from some business participants, as profiling is a term with a negative connotation. Business did not want to associate their

products with a negatively charged term so they decided on determining demographic characteristics.

Jerome Williams from Rutgers University also presented information on FRT and marketing/advertising uses at the July 24, 2014 meeting. Williams expressed concern about FRT being used to advertise products:

> We are at a point in marketing today where we take a million messages and customize them for our purposes, narrowcasting. Think about all the photos available we have elevated the level of sophistication and can tailor each message to an individual. Sometimes we refer to that as segmentation (Williams, 2014).

Williams' comments echo Brackeen's, in that, there is a real interest from the business and advertising communities to incorporate FRT into their practices. Faces, due to their unique ability to link data, may now represent the best opportunities for marketers to personalize their messages to consumers; after all, the face can tell relative age, race, interest in product, and even health.

> The next slide is about face marketing; when you have the ability to capture all kinds of faces, whether its information or other it allows you to very easily target at a very sophisticated level…others that you want to use. We are at the point where you walk down the street and pass a retail store or window and the ad appears based specifically on you, your age, race, gender, ethnicity, all other kinds of socio demographic variables have been captured (Williams, 2014).

The technology has the potential to aid advertisers in crafting targeted messages to individuals. While this is a real advantage for advertisers, and potentially benefits consumers with messages relevant to their wants, this technology also presents new opportunities to discriminate against and marginalize individuals.

> Retailers are deploying FRT to identify customers as a retention technique. On the surface you might say that's a good thing detecting which individuals are more engaged in shopping and the store can help with loss prevention. In some of my work…we find some instances where one racial group only represents 5% of the customers in the store but 95% of the shoppers stopped for shoplifting. That suggests the technology and cameras are focusing on one group (Williams, 2014).

Racial profiling has been a part of society for quite some time, it appears that cameras aided with FRT have the ability to exacerbate this problem. This problem has gained the attention of the news media as well as commercial entities.

> The media has gotten some of this…the cases that talk about "shopping while black" or consumer racial profiling, people refer to it as shop and frisk. Essentially you identify people and you pay more attention to them in the store and also when they leave the store and using FRT to zero in on only certain groups and perpetuate this behavior. My concern is that if FRT is not looked at in terms of the harm it can cause, there could be perpetuation of [this] (Williams, 2014).

It became clear to the group that FRT could be a powerful marketing tool, but that it could also lead to disparate opportunities presented to individuals based on age, gender,

race, and ethnicity. Therefore, the group became even more aware of the importance of where FRT was deployed.

These presentations represent most of what the group has seen concerning the potential for discrimination utilizing FRT. This also constitutes the majority of the presentations made from invited guests. After these presentations, which ended at the July, 24, 2014 meeting, the group felt satisfied with their level of understanding and moved into more policy heavy issues, as well as the creation of a code of conduct.

These presentations illustrate some key findings found in by the group. The first theme found amongst the presentations is the ease with which FR is conducted. As Acquisti (2014) made clear, "if an economist can do FR then anyone can." Brackeen (2014) has over 320 companies viewing his company's website looking to utilize FRT for business solutions. King (2014) noted the ubiquity with which the technology is being deployed for security and international use. FRT is easier to implement, and is improving rapidly in terms of speed and accuracy. As Acquisti (2014) alluded to, increases in computing power and various FR applications will increase surveillance, making privacy harder to protect.

Currently, accuracy remains an issue with the FRT and accuracy rates decrease as the population size increases. While low accuracy rates sound like good news for those wishing to protect their privacy this may not be the case with data accretion. The Associated Press (2013) reported that Facebook alone has over one billion active monthly users. The ubiquity of social networking sites, the pictures contained on them, and the associated data stored with these profiles presents uncountable opportunities to apply and use FRT. Low accuracy rates could lead to increased use of FRT in order to find

individuals or information about them, and increased use could reveal important information about an individual's social group; this is particularly concerning for minors whose profiles can provide information about their friends and families and potentially lead to geographical tracking. Regardless, using FRT on minors is a contentious issue for stakeholders and technology providers, all of whom understand the increased concerns, some even refuse to provide FRT to individuals wishing to apply it to minors.

Data accretion and linkage is a major concern for minors not only from social networking but also from school obligations. Students are required to attend school and much state funding for schools is the result of student attendance rates (Kravets, 2013). Schools are increasingly turning to student IDs to prevent unauthorized access to students and to track their whereabouts. Students have even been suspended for refusing to wear ID's that contain Radio Frequency Identification chips (RFID). RFID equipped student IDs contribute to data accretion because they contain a student's photo, monitor his or her location and movement, and could contain other sensitive information, such as a healthcare contacts, healthcare information, and financial services used for school lunches or activities. These developments confirm Chandler's (2012) observation about the obligatory technologies necessary to participate in society.

Developments such as these highlight the concerns that Acquisti informed the group about such as offline to online linkages and online to offline linkages. While student IDs increase school security and protect students, they are also creating unwanted linkages between a student's real life and their online profiles and activities, causing additional safety concerns of their own. Student IDs are just one example; college students and many employees are required to wear similar ID badges which create similar

privacy concerns. With data accretion one must ask whether student IDs and similar photo based credentials are creating safer spaces or additional opportunities to exploit security and privacy as well as track individuals.

Student safety and secure schools are often reasons used to justify student IDs with similar reasons used to justify various forms of identification for employees and American citizens. However, another issue, and an underlying theme from the meetings and presentations, concerns the profiling of individuals. Much of the interest in and funding for FRT has been for security purposes, but these security interests can lead to the profiling and discrimination of individuals. A problem inherent with many security systems and cameras is that they are run by individuals who have their own biases. It is possible that racially biased individuals would choose to follow certain individuals around locations or apply the technology in differential ways to discriminate against others. FRT has the ability to amplify an operator's biases by providing additional information about an individual they otherwise would not have, such as credit score, political affiliation, sexual orientation, and other sensitive details.

The continued and varied uses of IDs for students, workers, and citizens should give us pause when we think about the likely increased use of FRT. These credentials are often required, meaning users have less control over their identities and privacy than they may have originally thought. The application of FRT to these credentials provides individuals with a feeling of safety and security but there is also the paradox of increased surveillance and invasion of privacy that comes as a direct tradeoff.

8.2. Stages of Facial Recognition

There are other facets of the technology that complicate the regulation of FRT beyond simply where it is deployed and the variety of individuals that can interact with it. This section contains technical aspects of the technology that have been extensively discussed by the stakeholders. The technical definitions presented throughout this section can be found in Appendix C. Appendix C is a consensus document of definitions agreed upon by the stakeholder groups; there are also different modalities of FR discussed, but please refer to chapter two for detailed discussion on their differences and capabilities.

The first task that any FR system must complete is called facial detection. Facial detection was defined by the definitions group as, "A task where the Facial Recognition System distinguishes the presence of a human face and/or facial characteristics without necessarily creating or deriving a Facial Template." Face detection is seen as mostly innocuous by the group. During this process no identifying data is stored or associated with a face, and demographic characteristics are not monitored or used. Face detection is mostly used for counting purposes. For example, retailers may use this modality to monitor foot traffic into their establishments. Retailers may be interested in monitoring traffic at their stores or monitoring numbers in facilities to ensure they are not violating capacity restrictions. The technology is capable of counting humans and providing simple and innocuous information to customers wishing to deploy FR systems for facial detection purposes. However, FRT is capable of much more than simple facial detection.

Another capacity of the technology is age estimation. Patrick Grother of NIST presented to the group at the November 6, 2014 meeting on the age estimation capabilities of FRT. Like humans, the technology is imperfect in this area, "What you

get there's a data point and it says that 67% of estimates are within 5 years of correct" (Grother, 2014). This is to be expected as "Some people look genuinely young for their age" (Grother, 2014). The technology becomes less accurate when trying to estimate older individuals as Grother explained:

> Somebody can be in the 80's and you don't know if they are in their 90's or 70's. This distribution gets wider naturally but never the less the numbers are what they are. Age estimation accuracy gets less as we get older.

While imperfect, age estimations by FRT can be expected to improve as the technology evolves. Age estimation by FRT may be used in the future to allow or prohibit individuals from entering a bar or other locations that are age restricted. Age estimation was seen as a mostly noncontroversial issue by the group unless its deployment was used to discriminate against an individual based on their age.

Another use of face detection may be identifying products the individual is interested in at a retail store. Face detection may be coupled with eye tracking technology to identify how long a person has looked at a product while also attempting to determine the emotions on the face as they engage with the product. Marketers are interested in these capabilities of FRT so that they can more effectively advertise products to consumers. This effective and targeted advertising strategy is developed by intruding on the mind's thought process. I refer to this intrusion as interference with cognitive privacy, or the privacy we take for granted when we choose to conceal or reveal our thoughts to others. This form of FRT is in its infancy but poses a significant threat to one of our most trusted conceptions of privacy cognitive privacy or privacy of the mind.

Another popular use of FRT is facial authentication. Facial authentication was defined by the group as:

> A task where the Facial Recognition System attempts to confirm an individual's claimed identity by comparing the template generated from a submitted face image with a specific known template generated from a previously enrolled face image. This process is also called one-to-one verification.

Facial authentication is a mostly unobjectionable use of FRT because an individual has normally enrolled their image in a database so it can be authenticated. Facial authentication is commonly used for security purposes and gaining access to privileges, like access to a database or an area of a building. Facial authentication has been deployed in Canadian casinos to prevent gambling addicts from betting. One interviewee explained how the technology was being deployed in detail (July 29, 2014).

> All the gambling in Ontario are state owned [casinos] but people of course lose money and it creates social problems. This corporation tried to promote responsible gaming. So they created a self-exclusion program. So some gamblers that feel they need help ask Ontario Lottery and Gaming Corp to put them on the self-exclusionary list. So OLG would take their photograph and name and basically said they wouldn't let them enter the facility (Government).

Previously, casinos had their security guards memorize photos of individuals that had self-selected to be excluded from the casino. As expected, the guards had difficulty

remembering all the individuals on the list and some gamblers who relapsed into addiction sued the casinos for allowing them into the facility.

> So OLG decided to use FR. So the photographs of the self-excluded people were used to generate templates and create watch list. Anyone who enters the facility his or her facial image is taken and run against the database. If there is a match this person will be approached by security guards and they check their ID and if it's an excluded person they will be escorted out (Government).

Facial authentication can be used for prosocial purposes and is frequently used for security purposes. For these reasons, and because an individual has generally volunteered their image, facial authentication uses of FRT faced few objections from the group.

FRT used to identify an individual faced increased scrutiny from the group. Facial identification was defined by the group as "Searching a database for a reference matching a submitted Facial Template and returning a corresponding identity." Facial identification is controversial to the group because it can provide individuals with information that they would not otherwise have. As will be discussed in detail later, an individual's facial template can be linked with a wide variety of sensitive data including credit scores, criminal records, and sexual orientation. Consider, for example, walking into a dealership to purchase a vehicle and the dealership has deployed FRT. The dealership may be able to identify an individual based on their face, a feat they could not perform previously, and determine that the individual has a poor credit score. Now, instead of the promotional financing rate that they would have previously offered, the

dealership has a finance offer with a higher interest rate. Such instances could occur with facial identification.

The group has also discussed a hybrid version of facial identification which is face recognition without identification. Recognition could include an individual's image being captured on a security camera at a store and their template is stored; when they return to the store, the FR system recognizes that the individual has been in the store before but does not have additional information about the individual. Steve DelBianco of NetChoice at the May 20, 2014 meeting expanded on this point.

> You mentioned two levels of definition, one called detection, that's a face, and then recognition. *Recognition doesn't necessarily associate that with a name* [emphasis added]. Recognition could be that face has been in my store before. Without ever associating with a name it just says I've seen that face before. That's one form of recognition that doesn't associate with identification at all.

Recognition uses of FRT raise concerns about surveilling and monitoring an individual's habits or routine. This form of recognition is not the one initially thought of by most individuals and is probably being addressed so that there are two separate provisions in the code of conduct, one most likely providing less protection than the other, a business goal. Recognizing that an individual has been at a certain location could be viewed as useful or even as an acceptable form of surveillance. DelBianco continued the example with a useful application of the technology.

> So I walk into the apartment building in Manhattan. The instant the camera sees my face it does a quick detection to see where my face is with

> this guy at the door. And then it makes a template. In truth it compares the template with the known templates on the residents of the building and if there's a positive match to the threshold define the door will probably buzz and they will let them in. If it doesn't the door won't buzz. There's no requirement or expectation that that template will be enrolled or retained or shared in anyway.

In this example presented to the group, facial recognition enables convenient access to the apartment building by tenants. The use of this technology also increases the security of the building by preventing non-residents from gaining access to the building.

8.3. Facial Recognition Technology Data

Through the use of FRT, biometric data are captured. Biometric data are unique biological characteristics that are particular to each individual, in this case the face; other examples include fingerprints, the iris, and DNA (Biometrics Institute, 2015). For further discussion on biometric data please refer to chapter two. One of the initial arguments of the group concerns whether or not a face template, the information created from the face through FRT, constitutes personally identifiable information (PII). According to the National Institute for Security and Technology (NIST)[31],

> PII is ―any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place

[31] NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major handicap to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals. Today, NIST measurements support the smallest of technologies—nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair—to the largest and most complex of human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks (National Institute for Standards and Technology, 2015).

> of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (McCallister, Grance, & Scarfone, 2010, p. ES-1).

Despite biometric records being included in the definition of PII, according to NIST, there have been disagreements about whether data derived from FRT should be considered PII for the purposes of a code of conduct. From the outset of the first meeting (February 6, 2014), FRT data being treated as PII has been discussed:

> …when we map the data that's used by face recognition systems into a framework of PII, then we are bringing in the type of protections we are elevating… in a way that a high resolution doctored photograph that’s frontal is as dangerous being kept online as your social security being publicly published online…in the next 5 to 10 years that image is going to be harvested [collected from the Internet] (Unknown Academic).

Certain participants are concerned about facial photographs being collected from the Internet and used for purposes other than their original intention. The sensitivity of the data collected is undisputed amongst the stakeholders, and industry advocates understand the liabilities they carry when storing sensitive information. The issue is whether an individual’s face, an inherently public personal feature and one we are not normally allowed to hide, should be considered PII. The other complicating factor with the code is that companies must still comply with state, federal, and occasionally international law. Therefore, stakeholders must be careful to not write provisions that contradict those laws as Alvaro Bedoya pointed out (December 15, 2014).

> [I]f the state law covers it; it covers it, and if it doesn't you have to take certain action following breach and treat it as PII. I think here the guiding principle should be not looking at what the states have done but looking at what companies do. On biometrics…Apple, Samsung, Facebook, and Google protect the heck out of this data. They certainly treat it as PII and as a result…I would say it should be treated as PII for purposes of breach. If you have a face template that's been developed using 25, 50, or 100s of photos, you can use that template quickly to figure out who that is using publicly available information. So I think we need to protect it as PII without any connection to name or anything else. It inherently connects to other things. So we need to have some kind of breach standard. I think anything less is totally unacceptable.

Previous presentations by FRT providers helped stakeholders recognize several strong protections in industry self-regulation. Following, but also mandating, some industry best practices have been helpful to move certain issues forward.

Stakeholders have also been mindful of government precedents that have been set with regard to PII. Walter Hamilton of the IBIA explained to the group on June 3, 2014:

> When a [any] federal agency creates a system of records, they have to perform a privacy impact assessment on that system of records, identify any PII that's collected and come up with a policy and a set of rules by which that data is collected and retained and ultimately disposed of[32].

[32] The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections (U.S. Securities and Exchange Commission, 2007, p.2).

> That does not apply to commercial entities. What it does is to show that what is PII, and by the way, I think a photograph is PII, a photograph is not a biometric. A derived template from a photograph or fingerprint is a biometric and meets the definition of that term.

In 2010 the Internet Policy Task force, an entity under the Department of Commerce, endorsed the use of Privacy Impact Assessments (Wolf, 2015, p. 211). A plethora of governmental agencies support the consideration of biometric data to be included as PII as Bedoya explained at the June 24, 2014 meeting.

> The government has repeatedly recognized it as PII. The NIST and Commerce among others, Department of State, Homeland Security, OMB [Office of Management and Budget], all categorically recognize biometrics as PII. Also, I had that the companies handling the data, and certainly in Senator Franken's[33] view, have afforded it the highest protection possible and have gone out of their way to protect that data. I would argue even more so than they protect things like address [and] date of birth.

While consumers have a reasonable expectation of strong data security, there are important First Amendment implications in the balance. Photography is a First Amendment right that could pose a challenge to those who may want to use FRT. One participant was quick to note the copyright protections afforded to photos: "From a copyright perspective it's clear. I snapped a picture of you, it's my picture. I own the copyright, done. [Its] settled law, absent some contractual agreement, you have no say

[33] Sitting Senator for Minnesota.

over the matter" (Government). The complications between the First Amendment and copyright law are discussed further in chapter five. As Szabo pointed out in the June 24, 2014 meeting photography also has positive uses:

> So the ACLU [American Civil Liberties Union] for example, encourages public photography but they are trying to strike a balance between public photography versus what happens to those photos once you start using them. You hear a lot of horror stories about this being used to identify people at a marijuana rally. But then you can flip it around and say well there's a strike going on and there are some guys going down there to crack skulls, will the ACLU use FR to identify those people and for whom they work. You can make a more transparent notice of companies doing bad things.

This example illustrates the threats and protections that FR can provide to First Amendment protected activities including political support and opposition.

Since FRT can be used retroactively on photos there is a legitimate question about the scope of a code of conduct. One participant observed, "If we're talking about a jpeg[34] might later be used and put in a database, then we are writing a code for all photography, aren't we?" (Business). The code of conduct cannot limit one's First Amendment rights, and there is a clear distinction between photography and biometric data in that a photograph is not biometric data.

While a photograph is not considered biometric data, stakeholders began to wonder if the integers (whole numbers including 0) created as a result of applying FRT to

[34] A computer file format for the compression and storage of usually high-quality photographic digital images (Merriam-Webster Dictionary, 2015).

a photo should be considered PII. Predictably the business community resisted the integers being classified as PII as DelBianco stated in the February 25, 2014 meeting.

> The number that Mark generates from his algorithm is absolutely not PII. It's a vector of integers that his algorithm generated for that photo… Mr. Atick said that unless you have it married with meta-data,…or married with data that identifies a person, it is in and of itself not PII.

Stakeholders continue to struggle with which data inputs and outputs of FRT constitute PII.

As the previously mentioned big data report suggested, citizens and stakeholders should concern themselves with the use of data and not the collection of data. This conclusion is naïve in an age of NSA and IRS scandal. Citizens should be concerned about the collection of data because conclusions are reached from the processing of data and data cannot be processed unless it is collected. Consumers should be mindful about the content they post online, especially their image. As discussed previously it remains unclear if the integers created from an image being processed by FRT can be protected by copyright. Furthermore, the EULAs of Facebook and other prominent social networking platforms make clear that images and content posted by consumers can and will be utilized by these companies for their own monetary gain. Chandler (2007) noted the importance of courts assigning property rights in regulating technologies. Images or face templates created via application of FRT, if assigned property rights to the individual, could have important regulatory consequences for FRT providers.

Two primary views are represented in this discussion of PII and the integers created as a result of FRT. Business has a vested interest in keeping the status quo to

continue profiting from their consumer's content. Therefore, they are advocating for photos, and the integers created from photos via FRT, to not be protected under PII. NGOs, on the other hand, are advocating for the opposite: consumers should have property rights over their images and the integers, thus should be protected as PII. Under the business paradigm, it remains unclear what property rights consumers will have over their images and the potential to access property and privileges based on their image. However, following the NGO paradigm could potentially limit photography rights as currently conceived under the First Amendment. Also under the NGO paradigm, current business practices would have to be restructured as consumers would have a property right over their images and integers; it remains unclear how social networks and other businesses could monetize user content. The decisions made here could set important legal precedent for establishing a consumer's property right over their image, and, by extension, their identity. Although laws exist to protect an individual's name and likeness, this precedent would extend to commercial uses; in time, private use may also have equally important ramifications.

8.3.1. Reverse Engineering Data

Most companies using FRT have their own or have licensed a specific algorithm to conduct FR. Each algorithm processes the facial vectors differently, focusing on unique parts of the face that will allow the most accurate identification. Algorithms that are highly accurate create a competitive advantage for a company. Most algorithms are unique, unless a vendor has licensed their algorithm to multiple companies. The question the group maintained was: what could be done with the integers created. Could another company recreate the original photograph used by the FR software? This topic was one

of contention for the group. Some stakeholders felt that the image could absolutely not be reverse engineered. Marc Vaillant explained this difficulty at the February 25, 2014 meeting.

> What we do is extract from the image discriminating information and so it takes the image down to about 200 to 1000 numbers…and so that's a tremendous compression, you can think about the 6+ megapixel picture that it came from and now we are talking about 200-1000 numbers. And the other important point about this is that it is opaque. In other words, you can't go in the other direction, you can imagine because of this tremendous compression. Also, it's unknown how the data was generated. That's sort of the secret sauce of the algorithm and so it's only known to the algorithm…our biometric template is not the same biometric template that is used by Cognitec or NEC or NL1.

According to this view, the data cannot be reverse engineered into the original photo or be utilized by a separate company's algorithm. Other stakeholders maintained that the data could be reverse engineered. The implications of the argument involve data brokers[35] selling the created information and placing individuals back into the original photograph which can contain more potentially sensitive information. Vaillant went on to explain:

[35] "[Data brokers] are collecting, analyzing and packaging some of our most sensitive personal information and selling it as a commodity...to each other, to advertisers, even the government, often without our direct knowledge. ….[Compared to government snooping] a much greater and more immediate threat to your privacy is coming from thousands of companies [data brokers] you've probably never heard of, in the name of commerce" (Kroft, 2014, par. 1).

> [E]ven if you are not given information about the algorithm that generated the biometric template, you could work very hard to reverse engineer, the biometric template and… depending on how the biometric template was generated, and it's certainly not the case for all biometric templates, and it depends on what the vendor did to generate that biometric template, you could infer information from that biometric template.

Despite some technical limitations that may currently be present, small concessions were made by the business community at the February 25, 2014 meeting that found reverse engineering the data was possible, although admittedly very difficult. However, some stakeholders took a strong position about the ability for the data to be reverse engineered. In an interview occurring July 29, 2014 it was explained that:

> Secondly, that the image cannot be reconstructed from the template, especially the template algorithm that is proprietary, that is also not true and we showed that. Finally, there was a claim that two templates created from the same person by different algorithms cannot be linked together, in fact they can be linked together. So we tried to address and debunk that mess and published a note and it's published on the NTIA website[36].

Stakeholders felt that the best course of action was to proceed as if the data could be reconstructed as technological advances would likely make this process more accurate and easy to accomplish. Some stakeholders dissented from this position, as explained in a September 5, 2014 interview:

[36] The paper can be found here: http://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_faceena_recognition_templates_-_ipc_march-2014.pdf (Chibba & Stoianov, 2014).

> That's the Ontario Privacy commissioner and she is way off base. I think they are taking an absolutist approach that everything can be re-identified and that's an ideological view rather than something that's borne out by the evidence, including a researcher from Ottawa in a day long debate on de-identification in D.C. a couple of years ago. We couldn't do that.

Proceeding as if the data could not be reverse engineered would have potential resale benefits for industry advocates, while the opposite approach benefits privacy advocates. In the end, it was conceded that the data could be reverse engineered. Since stakeholders agreed that the data could be reverse engineered, the code will likely be worded with this agreement in mind. Proceeding as if the data could not be reverse engineered would create a privacy blind spot where images could be reconstructed, companies would be further incentivized to sell data, and consumers would be given the false impression that their data was safe. Contrarily, proceeding as if the data can be reconstructed to an image acknowledges the technological advances that are likely to occur, provides consumers with a realistic set of expectations about how their data can be used, and acknowledges the plethora of other potentially sensitive details that can be included in an image. The stakeholders' consensus on reverse engineered facial data provides consumers with an enhanced level of privacy protection.

8.3.2. Data Security

Stakeholders were charged with assigning strong protection to the data given the sensitivity of biometric data and the fact that it can be reverse engineered. Two primary areas of concern for stakeholders included when the data was in transit and when it was at

rest or in storage. It was determined that encryption would act as the primary protection for biometric data.

Stakeholders formed strong consensus on the need for robust security protections for FRT data. Encryption was determined to be an important component of the security regime. Stakeholders, however, were unable to initially agree as to what constituted encryption. Some stakeholders felt that the creation of a template constituted encryption because of the uniqueness of the algorithm used and the data it generated. This assertion was contested at the meetings "What is the intended significance or take away from declaring or asserting that FR scans are a form of encryption?" (Government). If the face template created was to be considered encryption it would eliminate a major technical requirement for companies that wanted to sign onto a voluntary code of conduct. Not all stakeholders were receptive to that idea, nor did they think the creation of a face template constituted encryption. "A faceprint is not an encryption of an image. It isn't. It's an abstraction of an image. Can you take the abstraction that is [a] faceprint and get back to the original image? No. But it's not an encryption" (Business). Stakeholders were also cognizant that, though a unique template did not constitute encryption, there was some utility to storing templates without identifying data as Walter Hamilton of the IBIA explained in the June 3, 2014 meeting.

> I do support the notion that a biometric algorithm that generates a template is not encryption. That to say, it would be encryption would be security by obscurity and I don't think that's valid. While it's less than useable in most forms if you don't know who the vendor was and their proprietary algorithm, you would have to have some knowledge about that. It is not in

> the form of a secret key as is defined generally from the term data encryption.

Facial templates do not constitute encryption in and of themselves. However, omitted information about the algorithm used on a template, makes it difficult to interpret the data, which is security by obscurity. Eventually, the definitions drafting committee did some research and prepared a draft of what they considered encryption. The group defined encryption as "The protection of data using reasonable means that have been generally accepted by experts in the field of information security, which renders such data unintelligible or unreadable." Stated another way:

> Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text (U.S. Department of Health and Human Service, 2015).

After stakeholders agreed that the creation of a face template did not constitute encryption, they still had to decipher what standard of encryption would be appropriate. A common format for encryption is 128 bit encryption. A bit is an integer of either "1" or "0." Depending upon the encryption method there may be one key to unlock the series

of integers or multiple keys to encode and decode the information.[37] As the bits of encryption increase, so does the security of the information.

Despite the desire of the group to strongly protect the data, there was disagreement about how to best address the standard of encryption required. Stakeholders are aware of the developing nature of FRT and encryption. The problem the group needed to address was how to define 1) an appropriate level of data security via encryption and 2) how that standard would last given the evolution of technology. Two separate proposals were offered in regard to the evolution of encryption standards. Some stakeholders, notably Carl Szabo, preferred vague language to allow flexibility for the standard in the future:

> We looked at the security procedure for banking which should [by] all accounts have the highest degree of security. Basically we say: Parties to this code should use commercially reasonable measures to secure facial template information. Once again, the commercially reasonable, allows flexibility for evolution yet it requires businesses and parties to the code to maintain a certain degree of protection.

This view puts the code of conduct more in line with industry self-regulation for "commercially reasonable" security practices. Businesses certainly have an interest in maintaining the security of their information, otherwise consumers may choose their

[37] If the key is 128 bits long, attempting to crack the code without the key would be 4.7 sextillion (4,700,000,000,000,000,000,000) times more difficult than cracking a 56-bit key (which itself has 72 quadrillion possible combinations)! Given the current power of computers, experts consider that a 56-bit key could be cracked by using the brute-force method in 10 million hours of computer time (14,000 computers used around the clock for 4 months)" (Kang, 2000).

competitors. However, given the recent security breaches at Target, Home Depot, and Apple, one must question the efficacy of the commercially reasonable standard.

The second proposal for the evolving nature of data protection in the code was tied to a governmental standard, "What I detail is FIPPS validated cryptographic method that has been confirmed as a base security and cryptographic measure by NIST" (NGO). This alternative proposal was justified on the following grounds by Michelle De Mooy from Consumer Action at the December 15, 2014 meeting:

> I think it's perfectly reasonable to expect a decent NIST approved level of security for such sensitive information as FR. I think the other just sort of legal aspect of this language is it puts it basically into FTC jurisdiction. They have sort of exercised that recently with Wyndham and LabMD[38]. But the important point is that it would be in their jurisdiction but it is not prescribed by them. It's taken to a more generally accepted level by NIST and that's important, because we don't want it to be something that can be invalidated by a court, we want it to stand the test of time (NGO).

It is important to note that the second method did not try to be overly prescriptive but did want to tie it to a specific standard. NGOs felt the code language needed the standard for rigor, "So where we are coming from with option B is not a prescriptive, though it may seem detailed, that's not the same thing as being prescriptive" (NGO). That standard was clarified to the group by the moderator, Verdi, who stated:

[38] Companies that have challenged the FTC's rulings against them for suffering data breaches (Privacy Association, 2013).

> To give a little background without speaking for NIST, FIPS 140-2[39] that standard is not a standard that is baked and set in concrete. That's something that has been around for a decade or better and gets updated and visited periodically.

The debate continued during the December 15, 2014 meeting and is best summarized in the following exchange between stakeholders. The business community would prefer the Uniform Commercial Code because it allows for the greatest flexibility while the NGO community would like to see the security standard tied to something concrete that provides strict assurance of protection. Both groups want something that can evolve over time so as to not have to renegotiate periodically. Szabo advocated for the Uniform Commercial Code stating:

> At the end of the last meeting we had this exact discussion and that's why I went with commercially reasonable. For example, the NIST standard says a minimum of 120 bits of security. Well if suddenly tomorrow commercially reasonable jumps to 256 that would actually engender a more strict and higher degree of security than the one we are attempting to prescribe here. So the UCC [Uniform Commercial Code] is not something that should be dismissed off hand.

Szabo goes on to note that the UCC is used by the banking industry which has strict data security protocols because of the sensitive information they handle and store. He further

[39] FIPS 140-2 was created after FIPS 140-1 entered a five year review period with a three month request for comments period. The standard was finalized in December of 2000. FIPS 140-2 dictates security standards in each of four security levels it outlines, allows for flexibility in choosing security features, ensures cryptographic modules contain proper security features, and assures that modules are in compliance with cryptography requirements (Snouffer, Lee, & Oldehoeft, 2001, p. 2).

notes that this standard has evolved over a period of over fifteen years, so it is reasonable to expect that it could continue to evolve. However, the NGO community still felt that specific assurances were necessary for robust consumer protection. De Mooy of Consumer Action countered:

> That is in fact totally erroneous. I'm going to look at something that NIST says. 120 bits affords a wide latitude for companies to choose between a whole bunch of cryptographic protections and methods. It's not a hugely high standard in terms of it being difficult in terms of companies finding a way to do that. The other thing, the security strength according to NIST is to last up [until] 2030 or 2031 according to NIST.

The De Mooy, backed by most of the NGO participants, tried to provide businesses the flexibility they need while also holding them accountable to tangible standard. This point was further argued against by the business community. Szabo argued:

> So the point I was making was that commercially reasonable is not dependent on some national board determining what is or is not commercially reasonable. It's whatever it basically becomes. [This seems to evolve according to the needs of business with little oversight] While NIST may have 128 bits today but the commercially reasonable standard may be something else much higher potentially. [But not guaranteed].

The point of contention between the two proposals was finding a method of data protection that was flexible enough for a variety of different businesses to implement and explicit enough to ensure that companies were protecting FR data in a responsible manner. As noted previously, the variety of companies that might sign onto the code of

conduct proved problematic. As can be seen in the following exchange occurring during the same meeting Emily from Facebook said:

> I just want to comment in favor of option A [Commercially reasonable standard]. I think when we are looking at a lot of companies like Facebook, Google, and others that are multinational. We have obligations in other jurisdictions and by saying a U.S. based standard, even if it does evolve, it could prove problematic if there might be different standards. [The UCC is also a U.S. standard].

Having flexibility in implementing appropriate data security was an important issue for many stakeholders. To allow for the international nature of some companies, the following proposal was put forward by Hamilton of the IBIA to secure FR data:

> Following up to Emily's [Facebook] comment. There is an international equivalent to FIPS 140-2. Which I believe is ISOIEC-19790. It defines security levels for cryptographic modules. Its lowest level to the highest level depending on what you are protecting. Administrative data, funds transfer, PII, or sensitive information used by governments in a variety of application environments. That might be a better choice if we want to have a broad worldwide aspect to the code.

It appeared that the international standard might by a compromise that both groups could agree to. For the NGO community, they would have a tangible standard that provides specified security standards. The business community would have a standard that applies internationally allowing multinational companies to continue to conduct business where

they please. Hamilton, of the IBIA, also noted a problem with the NIST standard in that it may unintentionally pass testing costs onto commercial entities.

> NIST performs module validation on hardware or software modules for FIPS 140 compliance. There is a substantial cost to the developer of those software or hardware modules in order to achieve a certification from NIST that their module has been judged to be compliant with the specifics of whatever level of the standard they are applying for….many of those modules hardware or software, have a cost to the implementer to integrate or incorporate them into a final system design. This code could unintentionally require a subscriber to the code to actually go out and make a commercial purchase…which might carry a cost aspect to it that we might not want to impose on subscribers.

The NGO community then became concerned with how much of a burden they might impose on commercial entities if they did in fact stick with their original NIST standard proposal. NGO stakeholders were aware that imposing heavy costs on commercial retailers would limit the adoption of the code of conduct. The group again looked to Hamilton of the IBIA to provide guidance on the potential costs.

> I don't think you're talking major costs but it could be a component of like a mobile telephone for example that has cryptographic security features in it. The developer of the phone may have purchased from a third party a crypto module that has been certified and approved by NIST 140-2[40] and that module may cost .... I don't know it could cost any amount of money.

[40] FIPS 140-2: Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/PubsFIPS.html (McCallister, Grance, & Scarfone, 2010, p. 4-7).

> It's hard to say. The cost to actually go through the process for the developer of that thing could be in the hundreds of thousands of dollars.

Setting forth an option that could cost companies thousands of dollars to implement was not deemed as feasible by the group. The group is currently in the midst of striking a compromise between the proposals.

> I was going to offer a compromise option. I was going to say, Carl's point that commercially reasonable may be more rigorous than NIST. At the same time, clients would like to have some sort of safe harbor. Could we take option A and add to it at a minimum "Parties should comply with FIPPS 140-2 as modified from time to time" (Business).

Ultimately, Verdi offered the resources of the NTIA to determine the way in which NIST, ISO, and commercially reasonable standards overlapped.

8.3.3. Data Access

Broad consensus was reached by the stakeholders regarding the need for strong data security in the form of encryption, but data encryption is just one aspect of data security. Another concern that needed to be addressed by the group was how the data would be stored and who would have access to it. These issues have been tangentially and less explicitly discussed by the group than the encryption issue.

Storage of de-identified data versus identified data[41] became the next contentious and problematic issue for the group as there is no uniform definition of PII nor is there a standard for what constitutes de-identified data (Wolf, 2015, p. 207). Facial recognition

[41] De-identified data is data that has the identity of an individual or individual identifiers removed from it. Identified data is data about an individual where their identity, such as name or social security number, is still attached.

works when applied to photos, but photos are not considered biometric data and are not protected as PII. However, without photos, FR cannot be conducted, so they are important, yet unprotected, PII pieces of data that stakeholders could legitimately argue for less protection in storage. Storage of an image is also a very important starting point in the process of FR. Storage of an image may constitute enrollment into a FR system, because it's the image that comparisons are made from. Does this then mean that all images recorded on surveillance systems constitute enrollment into an FR system? The definitions group defined enrollment into a FR system as, "The process of storing and maintaining Facial Recognition Data." The question of enrollment was addressed in the June 3, 2014 meeting by Bill Long of Business Performance Research Associates where the difference between an image and a template were discussed:

> Walter and I tried to distinguish in our definitions group between an image and a template. An image is a picture, anybody can take anywhere with any device, hidden or open as the cameras in this room are. That's just an image. That's not biometric data. That's an image. It's not a template. Anyone who wants to can create a template and store it in a database; then we are talking about stuff in this room [enrollment]. But just the image and storing it for 10 years, that's not part of the discussion (Business).

As discussed earlier in chapter five, photography is a First Amendment protected activity when completed in the right circumstances. The people who take photos may also have a copyright interest in them. These competing legal interests have yet to be clarified by the courts in regards to FRT. Photos and the images in them are not biometric data and are not considered PII. An image processed by FRT and used to create a template of an

individual constitutes biometric information and is considered PII. The definitions committee defined a facial template as, "A digital representation of distinct characteristics of a Subject's face, representing information extracted from a photograph using a facial recognition algorithm."

With the group defining differences between photos and face templates, specific conversations could be had about the storage of templates, which are now defined as biometric data. Walter Hamilton of the International Biometrics and Identification Association shared the following best practices of biometric data companies with the group at the November 6, 2014 meeting:

> We also support the concept, to the extent practical, depending on the application, disassociating biometric data from other personally identifiable information; to provide another level of abstraction, if you will, to minimize the effects of data breach. We also support the notion of having databases with restricted access, meaning that there should be some form of strong authentication to the users and administrators of that data such that the data is protected by a means other than simple username and password if possible.

Several important points are made in this comment. In addition to having the data encrypted while in storage, face templates should be stored in a separate database without identifying metadata. The implications of this are clear, potential hackers would need to not only break into the database where the face templates are stored, but also break into a separate database to gather the identifying metadata to associate with the template. A facial template without its identifying information is not terribly useful. Consider this

illustrative example: as humans, we leave fingerprints on all types of surfaces every day and pay little consideration to it because our names and other relevant information are not accompanying them. Walter also thought these databases should have limited access, not everyone at the company should be able to view the information, protected by strong authorization methods. Walter specifically identified a username and password as being a weak form of authentication. He goes on to explain some components of strong authentication during the same meeting:

> I would like to include in that some form of strong authentication rather than simple user name and password. That doesn't mean passwords can't be used but strong passwords at a minimum but preferably two factor authentication for access to sensitive data whether PII or biometric information should be limited. I don't want to suggest a requirement for biometric authentication for logical access control, that would be a form of strong authentication but a token or a pin plus token there's a number of different approaches to that…we just need to make sure that access to the data is restricted only to individuals that have an appropriate access privilege.

The group in drafting language has been careful to describe robust practices that it deems to be acceptable without being so granular that businesses lack the necessary flexibility to accommodate their particular needs. With regard to appropriate access to data, the group is also considering an auditing mechanism to ensure adherence to access requirements. Existing industry practices were also presented by Alvaro Bedoya, of Senator Al Franken's office, at the same meeting to inform the group on secure storage methods:

> On security I do want to point out that the big players in the space have very robust security practices. It's not just secure storage, it's also encryption according to Facebook, Apple, and Samsung. Facebook said in a letter to Congress[42] that all of their facial templates are encrypted and stored in a monitored and access restricted database. Apple has said with respect to touch ID that the data is encrypted and securely stored in a secure enclave. Samsung with their fingerprint scanner, it confirmed to me that it's encrypted and they say also in this letter that the fingerprint data is stored in a secure part of the smartphone. For security it's not just encryption but also secure storage.

This was the first time that the notion of a monitored database was introduced to the group. This monitored database seems similar to the group's auditing mechanism idea. There was no indication if the database referenced was monitored in real time or if there was an audit system in place.

The location or accessibility of a storage vessel was also a topic of concern for the group. Data may be stored on servers that have no connection to the Internet; companies may also store information in the "cloud" to utilize cheaper storage spaces. NIST defined cloud computing as:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that

[42] Facebook announced the encryption standards after receiving scrutiny from privacy advocates and members of Congress when it was discovered that user identifying information was sent to third parties, the response came in October of 2010 (Bentley, 2010).

> can be rapidly provisioned and released with minimal management effort or service provider interaction (Brown, 2011, par. 2).

Concerns about offline and online storage are centered on issues of a data breach. Verdi attempted to clarify the issue for the group stating at the November 6, 2014 meeting:

> The cloud issue wasn't really raised but I think some of the examples that were given were…think about a digital sign that performs full blown FR trying to identify folks or trying to authenticate folks, but does not have a network connection it stores the data locally. At some time is updated either over a network or physically. So then you have questions about transmittal and you have FR biometrics that are transmitted back and forth whether that's pursuant to sharing or a function of the system, that's an open question. Then you have a question which is a system that does both, both stores biometric data locally and is sort of having a constant or periodic transmittal relationship in which biometric information is exchanged and it is talking or calling back to a home server for updates or to perform other functions.

Issues of cloud storage raise questions of data transmission. It was determined by the group that data storage and data transmission both deserved robust encryption protection. Hamilton of the IBIA at the same meeting noted that data would be unprotected for a brief time:

> The NIST standards previously referenced apply to both data at rest and in transit. When data is in transmission it needs to be over a secure channel or protected in some way for some cryptographic means. However, when

> the matching function occurs, the data necessarily will be decrypted both the match candidate and the target enrollment record for that match to take place. So there is an instant of time if you will where the data is in the clear. I don't know that that represents a significant or even measureable business or social risk to these discussions. Personally, I think we should be satisfied by having a broad agreement [consensus] on the data protection in transit and in rest using accepted cryptographic means.

As has been discussed, none of the outcomes from the NTIA MSH process happen in a vacuum; many states have data breach laws that the code must comply with in order for companies to be able to implement it. Stakeholders have acknowledged that they cannot re-write laws; thus creating standards that follow existing legal requirements is a productive way to proceed. Hamilton was reluctant to redefine PII stating at the same November meeting:

> I think there are already some statutes on that breach of PII and if the definition of PII includes biometrics it would apply there as well. So I don't know that this code should attempt to redefine or visit those existing statutes…

The NGO community agreed and consensus started to form around the futility of trying to redefine PII, Michelle De Mooy stated, "I agree. I think the states have handled data breach notification very well in that realm." In concert with those comments Bill Long, victim of a recent data breach, spoke up about the notice that commercial entities provided to him.

> Having recently been the victim of a data breach called Home Depot, the rules and regulations about how to notify victims and enable large well represented companies to not disclose very much. Home Depot never got in touch with me individually. [I]f we are going to deal with breaches, maybe we have done enough to require users of this technology to have more secure authentication of users but hacking happens. When hacking happens, is it ok to rely on the state of Maryland or Virginia or Utah to ensure that if it's a Home Depot or a Target or a whoever shopping mall, I'm not sure we can write language that will do any better.

Clear consensus could not be reached on data breach notification during the November 6, 2014 meeting. Groups came back to the table at the December 15, 2014 meeting with two ways to proceed regarding data breach policy, addressing the issue or leaving it to existing laws. Issues of templates and PII once again cropped up in an exchange between stakeholders during the December 15, 2014 meeting. Szabo explained to the group:

> There are two approaches here. First is option A. Which is that we should not necessarily address data breach notification as there are already 47 different state laws that cover unauthorized acquisition of PII and regardless whether an entity adopts the guidelines or not these state laws apply. Finally when the federal government passes a national data breach standard, if ever, this section can create confusing or conflicting obligations for parties to the guidelines.

The business community must comply with state laws and the majority of states already drafted laws for data breaches. Szabo felt that creating additional standards would create

conflicts for businesses attempting to comply with the code of conduct if the standards were different from the state laws that the businesses already have to comply with. It is not unusual for business to avoid regulation (Kolk et al., 1999); however, it also seems unlikely that Congress will act to create the legislation referenced. An interesting appeal to the possible passage of a federal data breach law was used to argue for reduced regulation. As De Mooy argued during the same meeting, most existing state laws did not address biometric data in their data breach laws.

> So for 47 state laws but only about 10 of them cover biometric data. So what we did was combine language that we thought would be straightforward and that's from the state of Wisconsin and it's what we think is fair for now, definition of biometric data.

Szabo countered noting, "There are only 4 states in the country that even mention biometric in data breach law, none of which consider biometric anything that's facial fingerprints, and iris as a form of PII." The argument between the two participants centers on what should be considered PII. As discussed previously, PII lacks a consistent definition as, states define PII differently. For the purposes of data breach, group tried to determine if un-identified biometric data should be considered PII or if only biometric data with identifying information attached to it should be considered PII. Szabo continued during the December 15, 2014 meeting noting:

> In Wisconsin in order for it to be PII must be biometric data which is combined with last name and a first initial. So that is the definition of what is PII in the state of Wisconsin, Iowa, Nebraska, and North Carolina. I think that further hits home the idea that we have all been talking about a

lot today and over the past couple of months of whether a face alone constitutes PII. If we're going to rely on the state laws then the answer is no. So if we want to change option B to be in parody with the Wisconsin statute which would have biometric data including fingerprint, voice print, retina or iris image, we must include at the preface last name plus first initial or first full name would be my suggestion.

NGO participants similarly made appeals for code provisions by looking to the future and noting the likelihood of increased accuracy and additional capabilities of FRT to argue for increased protections. NGO participants are particularly concerned with the sensitivity of biometric data collected by FRT, whether attached to a name or not; as Acquisti had previously shown, it is likely that un-identified data can be identified with relative ease. The NGO community strongly supported this assertion at the same December 15, 2014 meeting:

Bedoya- Look, I think the idea that a faceprint is not PII is outside of the mainstream. I'm happy to be corrected on that. I think the reason we are all spending countless hours on this is because it is so extraordinarily sensitive.

De Mooy- I think it would be really disingenuous of the process not to address this. I think in fact it would be a huge opening for criticism of the entire code to not address biometrics in this section and to sort of blankly discuss state laws which we are very aware of the fact that they don't cover biometrics. I think that would be not working with integrity in this process and we would strongly object to that.

NGOs continued to argue for strong protection in the code for data breach provisions, suggesting the entire process would be criticized if they were not included. Business participants felt that if the code was to address data breach of PII then it should include the entire language in state law that protects PII rather than using partial language from the laws. It was noted that using partial language could create conflicts for businesses needing to comply with both state law and the provisions in a code of conduct as stated by Szabo during the same meeting.

> I'm not arguing that we would be disingenuous or operate without integrity. I'm just suggesting that if we are going to take part of the state law that we take all of it. …[W]e say look: if you are a business you must follow the state laws because you already have to today.

Stakeholders then discussed the evolving nature of state and federal data breach laws. The data breach discussion involved a comparison between state law and best business practices. The purpose was for the code to cover any gaps in state law as noted by Bedoya in the same meeting:

> I just want to say that, there has to be some kind of breach protection for this. A modified option B is if the state law covers it covers it and if it doesn't you have to take certain action following breach and treat it as PII.

A new appeal was made to the group supporting the inclusion of a provision that addresses a data breach of PII. Instead of looking to existing state laws, it was suggested that the code should follow existing best practices set by the business community interestingly this was suggested by Bedoya, an NGO stakeholder, in the December 15, 2014 meeting:

> I think here the guiding principle should be not looking at what the states have done but looking at what companies do. I'll just… that Apple, Samsung, Facebook, and Google protect the heck out of this data. They certainly treat it as PII and as a result of that I would say it should be treated as PII for purposes of breach. If you have a face template that's been developed using 25, 50, or 100s of photos, you can use that template quickly to figure out who that is using publicly available information. So I think we need to protect it as PII without any connection to name or anything else. It inherently connects to other things. So we need to have some kind of breach standard. I think anything less is totally unacceptable.

Business participants continued to push back on a provision in the code of conduct addressing the data breach of PII, arguing that such provisions would open up those companies who complied with the code to greater legal liability. It was also noted that additional complexity to the code could create an unworkable document similar to the one created in the MATP, which led to limited adoption by the business community. Stakeholders continued to negotiate a fine line between providing robust consumer protections while leaving enough discretion for companies to actually implement the potential code of conduct. The paradox of this negotiation is that adding consumer privacy protection opens businesses up to increased liability. Ultimately, it was determined that there was an important missing stakeholder, CDT, and the discussion was tabled to the next meeting; currently, as of this writing, that meeting has not transpired.

8.3.4. Data Retention

Data retention was an important topic addressed in conjunction with data storage, primarily how long and why businesses store sensitive consumer data which was determined to fall within the scope of the code of conduct. The data retention issue was broached as the group tried to decide what would happen to the consumer's data if the consumer withdrew from a service. Other entities already defined best practices regarding data retention, which were then presented to the group by Bedoya at the November 6, 2014 meeting:

> On retention, FCC and CDT have both issued best practices on retention. FTC said that companies should implement a specified retention period and dispose of stored images once they are no longer necessary for the purpose for which they were collected. If a customer deletes his or her account on the website the stored images are no longer necessary and should be disposed of even if the stated retention period has not passed. CDT echoed this, they said when a company does retain consumer information, the retention should last no longer than the purpose for which it was collected.

Providing consumers with choice about what happens to their data subsequent to a withdrawal request was important to several participants, thus data retention was a best practice identified in the FTC workshop preceding this process. Amanda Koulousias of the FTC presented this to the group in the March 25, 2014 meeting:

> And then the third recommendation for privacy by design was limited data retention. So for example in the scenario that we laid out the company

> was not storing the images which we think is a best practice in this instance because they don't need to store the images for their purpose. And we would recommend that just generally, companies limit their data retention to what is necessary.

At a superficial level, data retention seemed to be a practical principle for the code to address, but a number of issues complicated the topic. One of the caveats to the data retention principle was a consideration for minors. As noted previously, and discussed by the group, minors have comparatively limited cognitive ability to grasp long term rewards and consequences. Amanda Koulousias of the FTC expressed the following recommendations after a workshop concerning the limited mental capacity of minors to the group at the same meeting:

> So, for example, those case studies did not deal with use on children or teens. I recommend for more general guidance on those things the commission's 2012 privacy report[43] does deal with some of those issues and provides general guidance…companies might want to consider extra protections for teens. Some of the things that were suggested might be things like shorter data retention periods, privacy protective default settings, and in terms of children's data you know that was one of the categories that was laid out in the privacy report as sensitive data. Where

[43] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf The report acknowledges comments received, including privacy harms, the global nature of many businesses, and legislation to complement self-regulatory initiatives. The report outlines a privacy framework with the following main components: 1) Scope: to include online and offline companies dealing with sensitive data; 2) Privacy by Design: implemented in all phases of business practices and addressing data accuracy, retention, and security among other concepts; 3) Simplified Consumer Choice: consumers need choices for practices inconsistent with context of business relationship; and 4) Transparency: notice, access, and education.

> it was recommended that affirmative express consent be obtained before collecting that data.

Presumably, special consideration for minors seems appropriate given their use of social media, as Common Sense Media presented to the group in the April 29, 2014 meeting:

> And then you think what if: the images are used and then matched with social media profiles or other data bases so you could identify the shopper. Especially when it comes to teens, they are heavy users of social media, 91% of teens have posted a picture of themselves online, 92% use their real names, 53% post their real email address, and 20% post their cellphone number, according to Pew.

Special consideration for minors on data retention periods were not the only data retention issues discussed. While this is a code of conduct designed to protect consumers, legitimate business considerations must also be acknowledged. Many brick and mortar retailers employ security cameras for loss prevention. Therefore, stakeholders have discussed scenarios where businesses may have legitimate reasons to retain facial templates despite an individual's request that their data be deleted. Walter Hamilton of the IBIA explained this view to the group (December 15, 2014):

> [T]here was quite a bit of discussion about the need for potentially a general exclusion or statement that the code does not apply to security or loss prevention uses such as looking for known shoplifters in a retail setting or access control into a secure area limited only to authorized people where FR is being used. That those types of uses should not provide a facility for that individual to easily request and promptly receive

> removal of their FR data from a database if it is used for those kinds of purposes. There need[s] to be… some kind of preamble to this code that talks about the security or loss prevention exclusion.

Stakeholders have recognized that businesses also want to harness the potential benefits of FRT. There is legal precedent suggesting that criminals have limited rights after committing certain crimes. For example, sex offenders have to register with the police for the communities in which they live. The immediate problem is that sex offenders have been processed through the judicial system and convicted of a crime, protecting their constitutional right to due process. If retailers kept shoplifters face template without their consent before being convicted of theft he or she would be denied due process by the retailer.

While retail theft is a legitimate concern faced by the business community, these crimes do not occur without potential selection bias. Williams made a presentation to stakeholders (July 24, 2014) regarding racial profiling in the retail setting.

> Retailers are deploying FRT to identify customers as a retention technique. What will happen when a situation where there is discrimination against consumers. People refer to it as shop and frisk. Essentially you identify people and you pay more attention to them in the store and also when they leave the store and using FRT to zero in on only certain groups and perpetuate this behavior in the marketplace (Williams, 2014).

Use of FRT to address retail loss prevention brings up additional questions of profiling, including profiling convicts who have paid their debt to society. However, FRT may still

be used by retailers to protect their property, "There are uses and Alvaro has mentioned a retailer might be using FR for looking at known or convicted shoplifters or people who have tried to commit crimes in the store before" (Business). Profiling known criminals is not the only concern for "facial profiling." Stakeholders were also concerned about disparate opportunities presented to individuals based on demographic characteristics or other linked data. This notion was explained to the group by Bedoya in the February 25, 2014 meeting:

> While inaccurate outcomes are of concern, accurate outcomes when they are produced by non-consensual analysis can be equally problematic. So for example if I walk into a car dealership and an identity service provider can tell the owner of the dealership, "Hey someone just walked in… and that person uh works at X place, earns Y and just got a promotion. I think that's something that a lot of people would be uncomfortable with even if it is an accurate outcome.

Facial profiling is a contentious issue amongst the group. Some stakeholders worry about profiling based on demographic information, while others do not want to market unwanted products to uninterested individuals. Businesses do not want to waste effort on ads that are ineffective, "Whether its behavioral targeted advertising and they are taking my data, they are tracking certain kinds of data to make sure the ads you see are ones you are vaguely interested in as opposed to completely wasting your time" (Business). This exchange highlights the fact that consumers do not want their time wasted with irrelevant products and marketers do not want to waste valuable resources advertising products to consumers who have no interest in them. Profiling is a contentious issue amongst

stakeholders; some uses may discriminate while others are beneficial. Consequently, stakeholders continue to grapple with the delineations between productive and harmful uses of profiling.

8.4. Notice

Given the sensitivity of the data collected and generated by FRT, as well as its multiplicity of uses, the group determined that notice of the operation of FRT was a key component in helping to safeguard consumer privacy. One of the initial ideas for notice came in the form of a sign. Unfortunately, the suggestion came from someone in the room who did not identify themselves and their identity remains unknown:

> And then the question becomes, yes, we can put a notice we can put a sign saying CCTV with facial recognition in action in this area if you choose not to enter, you can leave, you can do something… you can give me a choice. We can create a sign maybe signage that would be iconic and maybe part of the discussion.

Notice is a key concept in the code of conduct. Consumers need to be aware of FR usage so that they can avoid the area if they choose, or take other measures to protect their image, including wearing a hat, sunglasses, scarf, or other protective measures.

Most stakeholders felt that consumers should be notified before coming in contact with FRT. If adequate notice could not be given, one stakeholder felt it should not be deployed, "Just like my casino example, I wonder whether there is any effective way of giving notice in that case. If there is not, then it strikes me that the best practice would be just to not do it" (NGO). Contrarily, there may be legitimate uses of FR where notice would not be beneficial for consumers. For example, airports that employ FRT to

identify terrorists or wanted criminals would likely not notify patrons of its usage in an effort to keep passengers safe. There may be a few exceptions to the idea of notice, but for most applications of FRT notice is the expectation.

It is expected that notice of FRT will be provided to users before they interact with the technology. Some stakeholders wondered what would happen if notice were given after an interaction with FRT. Specifically, stakeholders wondered if notice after interacting with FRT would be considered an unfair or deceptive practice that the FTC could enforce under its Section 5 authority. Koulousias of the FTC had explained to the group at the March 25, 2014 meeting that:

> And so then your other question was if consent was obtained at some later point would that be deceptive or unfair. In terms of deception or unfairness, those are things that we in terms of determining Section 5 violations we look at all those cases on a case by case basis. Consider the specific facts in a particular scenario. So it's not something that I can hypothesize right now but I can tell you it's something that we would look at on a fact specific basis.

Notice provided after interacting with the technology is counter to previously determined best practices; however, there may be legitimate circumstances where it is necessary or acceptable, especially when considering security interests in public places. The discourse surrounding notice is important as it has been extensively discussed by the group and the government recognized it as a previous best practice. Given this context it is likely to be a principal decision in this code of conduct (Scollon & de Saint-Georges, 2012). However, no matter when it is provided, notice is still a controversial topic for NGO

stakeholders. Additionally, the FTC would determine unfair or deceptive notices if provided after the fact and would be decided on a case by case basis.

The type of FRT being employed is very important to stakeholders with regard to notice. Stakeholders have begun to coalesce around the concept of multiple notices depending on the use of FRT. Vocal business participant Szabo seemed amenable to the proposal stating at the April 29, 2014 meeting:

> [I]f I as a consumer opt-into the system, unless it's disclosed to me at the outset you want to respect the information that is provided at the outset, like we would on any website. If there is material change in the privacy policy, typically most people would agree you need opt-in consent. If how I opt-in to the system is by agreeing to a privacy policy with the federal government that says they will only use this photograph for purposes of authentication. If they changed to identification then perhaps they might need a second round of authorization to do so.

If a FRT provider changes how they use the technology, stakeholders feel that consumers should be provided a second notice, and an opportunity to consent to the use of FR data.

While most stakeholders recognize notice as an important rule to include in a code of conduct, others were not convinced that notice would be taken seriously by consumers or that it provided necessary protection to consumers.

> I don't think notice and concern mechanisms are enough. And let me be clear I don't think notice and consent are bad per se, transparency controls are important but…were part of a broader package of principles which included different principles. If we only focus on those two without

> considering the others, it's as if we try to build a house without strong foundations. (Acquisti, 2014).

The worry that consumers might not take seriously the notice of FRT's use was echoed by another participant in an interview (September 22, 2014).

> The reality is consumers have been trained to be like Pavlov's dogs, they want the app so they click yes yes yes. It's also not been in the app developer's interest to say hey are you really sure you want to give me all your personal contact information that I can use to market other products. It needs to be more of a notice, but no one ever looks at [it] (NGO).

This comment was substantiated in the academic literature regarding end user license agreements (EULAs). It appears that many end users do not read the EULA before consenting to its terms. According to Earp, Anton, Aiman-Smith, and Stufflebeam (2005) an overwhelming majority of Internet users expect to see privacy policies on websites, yet only 60% of users admit to reading them. It is important to note that this covers all websites, including those carrying sensitive medical information. Legal scholars have observed a similar trend, but note that the agreement is nonetheless legally binding: "Despite the reality that consumers tend not to read these agreements, courts have consistently upheld online standard form contracts, finding sufficient assent" (Preston & McCann, 2011, p. 18). Creating a code of conduct that truly protects consumer privacy will require other principles besides a simple notification of FRT use.

8.5. Transparency

Providing consumers notice of FRT deployment is the first step to providing consumers meaningful control over their biometric data. The literature also proves, as

well as the NTIA meetings, that providing notice of FRT use to consumers is insufficient to ensure their privacy is adequately protected. Stakeholders see notice as an important first step to protecting consumer privacy, but businesses also need to be transparent about what they do with consumers' data. Will the business retain FR data? What are their retention policies? Will the company share a consumer's data? Data use questions are very important, and yet stakeholders remain divided concerning what transparency safeguards should be required of companies. One important principle of transparency is that it should be easy for consumers to understand. Legalese was a concern espoused by Susan Grant, of Consumer Federation of America, at the May 20, 2014 meeting:

> I think where the more meaty transparency comes into play, the explanation of how it's going to be used and government access and so on is in fact when somebody is being enrolled in an FR system. While it should be in plain language and not legalese, I don't think we need to worry how that would fit on the building because that's not what we are talking about.

Stakeholders are mindful that many consumers, including minors, will not understand the legal jargon contained in privacy policies. Transparency requires lay language.

The goal of the group is to give the consumer control over their data through notices and company transparency. As mentioned previously with data retention policies, consumers should have the ability to delete their data regardless of how they entered into a service. Chris Calabrese of the ACLU cited the practices of Google and Facebook during the June 24, 2014 meeting.

> Google has said that you can opt-in and they will only collect your faceprint when you opt-in. I think that's a powerful first principle. I think it contrasts sharply with some things that are in the IBIA framework. Both Google and Facebook allow you to withdraw your consent in the form of deleting faceprints whenever you want, certainly a powerful way to keep the technology under your control. Google and Facebook give a certain level of access to prints; you can know when it's being used and control how it's being used. Certainly it's not the robust audit control that we would argue for, but it's an understanding that this is the consumer's information. It needs to be handled and the consumer needs to be consulted on it.

The goal of providing a consumer with notice and transparency is to enable consumer data control. Control has been a popular conception of privacy amongst the stakeholders. When many stakeholders were asked about how they conceived of privacy, many of them used the word control to sum up their view. Control is a popular conception of privacy because it is one that can be "operationalized." As noted, privacy is a complicated, multifaceted, and subjective subject, whereas control is seen as something tangible that can be given to consumers in detailed ways.

8.6. Conclusion

The complexity of the technology, the sensitive data it collects, the protection of that data, and providing consumers with meaningful controls has the group grappling with those issues. Security of the data generated by FRT has been the "low hanging fruit" that the group has decided to address first. As shown, even though stakeholders

agreed that strong security protections were warranted they are having difficulty agreeing on the details of those protections. At the last meeting, which occurred December 15, 2014, the group was unable to achieve consensus on this issue. At this time, no other meetings have been scheduled, so it remains unclear as to how these issues will be resolved. The group still has many issues to decide, including how the technology will be specifically regulated and if companies will adopt the regulatory regime for FRT.

CHAPTER 9

HOW DOES FACIAL RECOGNITION TECHNOLOGY CHALLENGE CURRENT CONCEPTIONS OF PRIVACY?

Facial recognition technology is an emerging technology that will likely force academics to reconsider how they conceive of privacy. As explained previously, privacy is a subjective and contentious concept. There are no agreed upon definitions of privacy in the academic community. As such, many scholars have chosen to focus on specific aspects of privacy rather than deal with the entire concept which consists of, but is not limited to, physical privacy, data privacy, cognitive privacy, and information privacy. The power of FRT links these varying conceptions together and challenges the merits of splitting privacy into such narrow conceptions. This chapter will explore stakeholder understandings of privacy as their understanding will influence how privacy is conceived by a code of conduct. Also addressed, are the various academic conceptions of privacy and how the technology has the ability to link the current fragmented conceptions of privacy.

9.1. Understanding Stakeholders' Conceptions of Privacy

Understanding how stakeholders conceive of privacy is an important precursor to understanding how a code of conduct for FRT protects consumer privacy (Scollon & de Saint-Georges, 2012). Stakeholders have varied conceptions of privacy, thanks to what their organizations and constituencies value. Some constituencies are inherently privacy protective while others are privacy intrusive. Stakeholder opinions of privacy were

collected to determine what has been called "anticipatory discourse" or the sense that our actions begin as "preparation for action" (de Saint-Georges, 2004, p. 73). One can best understand an action after examining the sequence of motivations that led to its accomplishment. Understanding stakeholder privacy opinions represents an important step in understanding how a code of conduct will address the issue in regards to FRT.

When several interviewees were asked for their definition of privacy, they gave uniform answers that could be summed up in a single word: control. An interview conducted with a government official elicited this response: "Control. It [privacy] could be other things to other people and that's fine, we can have good conversations about that. But it's about control, it's not secrecy. It's about control" (Government). A similarly concise answer was given when another interviewee was asked about his/her definition of privacy, which was "Control of the information" (Business). During another interview the control theme was again espoused when asked about how he/she conceived of privacy, the responder indicated that "Privacy is about information control… the individual has the ability to know what is known about him or her, and control it. But certainly I mean that's mine. Mine is much more about information control" (NGO).

In the literature informational privacy is a popular conception of privacy amongst many others (Nissenbaum, 2009; Smith et al., 2011; White House, 2012). The uniformity of this discourse suggests that data and information control will be an important topic of discussion for stakeholders. Indeed, the first substantive issue addressed by the group in the drafting process was data security. Part of having control over one's information includes assurances that the information is adequately protected and there is limited access to it. Given the many understandings of privacy found in academic literature, the

uniform understanding of privacy as control by stakeholders is counterintuitive. One would expect a diversity of conceptualizations of privacy amongst stakeholders, but perhaps since the purpose of the process is to develop a code of conduct, operationalizing privacy as control does make sense.

Control appears to be a popular concept amongst stakeholders drafting a code of conduct for FRT because "control" can be operationalized. The popular conceptualization of control was substantiated later in actions by the group. The stakeholders first drafted language about the high security protections and limited access to this data the code should provide as an example of anticipatory discourse (de Saint-Georges, 2004).

It is virtually impossible to account for the subjective nature and the varied conceptions of privacy in a single code of conduct and achieve a satisfactory outcome; however, it is possible to provide users with tools of notice, transparency, and assurances of security that provide consumers with some level of "control" over their information. For instance, if a FRT commercial entity makes a material change in how it uses a consumer's FR data then it may have to receive affirmative consent from the consumer, thereby providing the consumer a measure of control over how their data will be used. It should be noted that control provides stakeholders the practicality of operationalization through language in a code of conduct. However, despite its conveniences, the concept of control does have some limitations despite its conveniences.

Equally clear during the first few interviews is the woeful inadequacy of the concept of control as a conception of privacy. Data breaches have occurred recently at Target, Home Depot, and Apple making it apparent that even though the consumer has

entered into agreements with each commercial entity, they ultimately had no control over how their data was accessed and used. With these events occurring during this MSH process, it is of little surprise that the group placed a premium importance on data security (Scollon & de Saint-Georges, 2012). Scandals at the IRS and NSA have also illustrated that government entities can use a consumer's or citizen's data outside of his or her control. Data breaches do not eliminate the usefulness of the concept of control but point to a potential limit of its viability in practice. This code of conduct cannot adequately address the limitation of data control, Internet service providers, the architecture of the Internet, and users' access to their data are all important points affecting the control of data. One might simply suggest storing data on servers without Internet access, but this would place limits on business practices and still would not deter rogue employees with nefarious intentions. Even if users had perfect control over their information they would still lack privacy because many individuals willingly divulge personal information for various reasons, including monetary gain or increased celebrity (Allen, 1999, p.867).

With these understandings in mind, the researcher continued conducting interviews asking interviewees for their definitions of privacy and discussing how useful the conceptualization of privacy as control actually is. A different conception of privacy was voiced by an NGO interviewee (August 6, 2014),

> I think that privacy is a right to be left alone, to be free from intrusion by companies and by the government. There's a limited space where one can be without being monitored or assessed and preserving the ability of an

> individual to have that space to feel unencumbered, uninhibited, without fear of reprisal, assessment, or judgement (NGO).

The right to be let alone is another conception of privacy found frequently in the academic literature (Rosen, 2000; Mill, 1988; Terilli & Splichal, 2011; Smith et al., 2011); one that we typically think of in regard to physical privacy but can also include our information being let alone as well. FRT can certainly intrude on one's physical privacy and informational privacy. One interviewee placed control as tangentially related to privacy rather than central to privacy:

> I think control is an aspect of what I think about it. Having control over the space is part of it but the reason we have privacy is individuals really feel the need to have part of their lives that they don't have to worry about someone else seeing them or assessing them and using that against them (NGO).

Control is thought of by this interviewee as an important component of privacy, but not all encompassing. Another conception was articulated as, "data retention, awareness, giving people consent. If I had to encapsulate it, it's about personal control" (NGO). In this definition there are components that have been explicitly discussed in the meetings, including notice, transparency, choice, and data retention, which may have been absorbed by the interviewee from the meetings (Scollon & de Saint-Georges, 2012). However, the concept of control once again materialized, in an interview occurring July 23, 2014, this time with a very different understanding:

> I think the point that people are making when they say that [control], or at least the point that I am making, is sort of highlighting the fact that that

> has been lost. Because we are talking about privacy in the sort of general way, that needs to be returned to people (NGO).

This same interviewee perceived of privacy control as something that has largely been lost. This participant felt that there has been a steady erosion of consumer control of privacy, which is what NGOs are advocating against.

> But what that does [advocating for big data] is make people feel like it's too late, this is just what's happening, or it makes them say things like "well I have nothing to hide" but that's never true, there are always things to hide. So when you say privacy in the context of this conversation it means having that control back, taking some of that back or having the ability to take some of that back. So it can be transparency which the companies would show you, this is what we are doing; this is what we are taking from you without you knowing or having any possibility. So that's the thing that advocates are trying to get to happen so we do have some control over it (NGO).

Control, notice, and transparency seem to be important components of privacy that many stakeholders can agree on; these conceptions have arisen from prior experiences of stakeholders, conversations had during this process, and compliance with existing laws. Stakeholders seem to agree on control as an important part of privacy. In an interview with a business participant (September 22, 2014), he felt that might be a point of consensus:

> I've spent time with others in the room but it's hard to judge what their perspective is. Again, I think like you said everyone does agree on

> transparency, on a level of control, again [it] depends on context, what's appropriate, and what's sufficient (Business).

Two interviewees failed to provide an answer as to how they conceived of privacy.[44]

There are two broad understandings of privacy in the meetings: one is representative of the business stakeholder group and the other from the NGOs. For example, one academic said, "Industry has a very legalistic understanding of privacy for pretty obvious reasons. Privacy groups have a much broader understanding of what it is and what it should be." Industry (Business) has a more legal understanding of privacy because of their concern to reduce legal liability. Businesses want to minimize their exposure to potential lawsuits that can arise from an invasion of privacy or the mishandling of consumers' data. NGOs likely have a broad understanding of privacy due to their varied citizen's privacy interests. Several NGOs have reported working on numerous MSH processes involving a number issues surrounding privacy. Despite there being some agreement amongst stakeholders about important aspects of privacy, it is important to understand how stakeholders view FRT in terms of being inherently privacy enhancing or privacy exploitive.

9.1.1. Big Data and Privacy

The increase of large data sets that include consumer information has been concerning for some participants. More important is the distinction between collection and use. Carl Szabo of NetChoice stated at this (June 24, 2014):

> If you go back to the White House big data report, the PCAST[45] report in particular, which is the technology arm of the White House, they said with

[44] 1) Don't have one. 2) I'd be happy to follow up with you on that.

> respect to big data don't worry about collection, worry about use. When it comes to FR the use is really a sharing, the sharing of information with somebody who otherwise wouldn't have that information. So we believe that users should have the opportunity to control the sharing of personal information with someone who otherwise wouldn't have that information. It's control of sharing. That personal information in this instance is derived from FR. That is control personal information, collected from FR software.

The start of privacy intrusion begins with the collection of big data. Steven Aftergood (2015) noted the glaring flaw in the statement "don't worry about collection, worry about use" when he stated,"[The problem with] secret collection of…records… is the … public was denied any opportunity to grant or to withhold consent to this practice" (p. 20). Citizens must be worried about the collection of their data as the government and big business continues to prove that they are both incapable of protecting consumer data and often abuse the data; the NSA and Facebook being the more recent and publicized examples. As Bruce Schneier (2015) noted, "…Government surveillance piggybacks on existing corporate capabilities" (p. 202). He goes on to explain that corporations equally rely on the government to keep their own surveillance practices legal and unregulated. The government and corporations "use each other's laws to protect their own data collection and get around rules that limit their actions" (Shneier, 2015, p. 202). Business entities also contend that they need to collect personal data to provide consumers with

[45] President's Council of Advisors on Science and Technology (PCAST), the report referenced can be found here: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/amp20_report_final.pdf

better services. The "Big Data" report has been tangentially discussed by the group, mostly because FR creates new biometric data that adds to existing data about an individual.

9.1.2. Technology and Privacy

There has been some discussion by stakeholders about whether FRT is a privacy enhancing, privacy invading, or a privacy neutral technology. How stakeholders view the technology in regards to privacy is important to understand what protections the code of conduct may provide consumers. These discussions are likely to impact the final code of conduct (Scollon & de Saint-Georges, 2012). Regulation can change how the technology is viewed in terms of privacy. As one business representative said: "As a matter of fact, many technologies are privacy protective. Or technologies can be crafted in such a way to be much more or much less privacy protective." This sentiment was reaffirmed by another interviewee (June 23, 2014):

> I think in many ways technology facilitates privacy and in many ways technology threatens privacy. I am largely of the camp that technology is neutral. The means to which we put it as human beings and the ways in which we use it determine whether or not it is privacy enhancing or whether it is privacy reducing (Government).

The degree to which FRT is inherently privacy protective or privacy exploitative might be considered extreme positions, "But those are edge cases. I think that the big fat middle is folks get to pick in terms of how they implement them [privacy protective or privacy intrusive]" (government). This middle ground where users get to choose how the

technology is used seems to be a position with broad agreement amongst the group. Walter Hamilton of the IBIA took this position at the June 24, 2014 meeting:

> First any technology is inherently privacy neutral. It is only the application or use of a technology that determines whether it is a protector of privacy, or a privacy enhancing technology, or whether it's a threat to personal privacy. It's very difficult for us to say that a technology is good or bad or characterize it as something dangerous. It is privacy neutral.

Stakeholders understand that whether or not the technology enhances or degrades privacy is largely dependent on the safeguards that they create in a code of conduct. For example, broad authentication uses may increase the security with which an individual accesses his or her bank accounts and other sensitive records; however, its uses may lead to what has been called the democratization of surveillance, or when citizens play an active role in surveilling their peers (Dupont, 2008). Equally important are the underlying values attached to the technology and largely ignored by participants. FRT has historically been funded by the government to be utilized for national defense. The military's defensive influence on the technology should not be dismissed by the stakeholder participants who immediately state that the technology is neutral.

9.1.3. Privacy and Control

Since privacy has often been conceptualized as control by stakeholders, it is important to understand this concept in greater depth. A business interviewee stated: "I think [control] is an important concept. Control without [an] adequate understanding about what the implications [privacy risks] are and what your other options [transparency and notice] are can be kind of pointless." These comments demonstrate stakeholder

awareness of the limits of privacy as control. Consumers are unable to enact meaningful control over their person or information in the absence of proper notification and transparency provided by businesses. If businesses are not forthcoming about their practices and the rights of consumers then will be unable to enact the protections provided. However, as shown in the previous chapter on the regulation of technology, providing consumers with too much notification can lead to a Pavlovian effect (please refer to interviewee comments on p. 225) where consumers simply click "accept" without reading through the terms of the agreement. Conversely, there is disagreement about the level of notice provided to consumers, which leads to consumer control of their privacy. One interviewee articulated some of the shortcomings of notice stating (September 17, 2014):

> I don't think we have meaningful notice either. No one will read these super long privacy policies. It's certainly a take it or leave it proposition in some cases. When I was talking about when companies will enter data along the lines of privacy it would be nice if these companies wanted to give people more privacy and giving people choice and control. I don't think that you have right now I don't feel like there are a lot of choices and particularly when we are talking about facial [recognition] and where you are walking down the street. It's kind of meaningless (NGO).

NGO participants have mostly expressed a lack of meaningful controls provided to the consumer. However, industry participants disagree: "…[C]onsumers have in the end a lot of control. But you have to give up certain amounts of control to receive various things in return" (Business). Industry participants appear to consider the surrender of

privacy as normal and possibly required to receive a particular product or service. Nonetheless, even business participants are undecided on the level of control that should be provided to a consumer as one interviewee stated September 9, 2014:

> Trying to determine how much should a consumer consider giving up control of X and privacy of Y in order to get product or service Z. Whether it's behavioral targeted advertising and they are taking my data, they are tracking certain kinds of data to make sure the ads you see are ones you are vaguely interested in as opposed to completely wasting your time. Is that something you care about and giving someone choice makes sense. I prefer to see the ads I care about rather than ads that disgust me or don't interest me (Business).

Despite a lack of certainty concerning the needs of consumer control, business seems to view intrusion on consumer privacy as a way to provide benefits or beneficial services to the consumer. No discussion transpired concerning businesses harming consumer privacy, nor was this issue even readily acknowledged by business participants. Notice and transparency are precursors of control, and represent the ability for consumers to keep their information private. However, providing too much notice can lead to the erosion of privacy, as shown earlier. A deeper understanding about the "appropriate" level of notice, transparency, and control is needed to protect consumer privacy and who provides those levels.

9.1.4. Privacy and Business

The business community has a somewhat conflicted position with privacy. Businesses must provide enough privacy protection assurances to consumers to gain

consumer trust so they will use the service or product, yet they also have a vested interest in exploiting consumer privacy to make money by offering relevant ads or better customer service. However, where this balance lies remains unclear as one interviewee articulated to me (September 25, 2014):

> Companies can prove through the security context and data breach or the impact it has on the bottom line or some sort of change in privacy policy that really upsets consumers, so there is a real economic incentive tied to having appropriate privacy protections and companies made of people who hold that same fundamental belief. But doing that in a way that doesn't really jeopardize future growth can be difficult as we have seen (Business).

The business community seems cognizant of the fact that if they do not have responsible privacy policies, consumers may choose other services. As one business interviewee stated (June 24, 2014):

> One of the important things to note is that when industry creates self-regulation we do it because we think it's good business. By that I mean we want to instill confidence in the market and also instill confidence in our users, especially in a post-Snowden era. That we will use their information responsibly and not outside the guise of what we say we want to do (Business).

Of course this recognition only works in business areas of competition. Where competition is scarce or where monopolies exist, companies have less incentive to prioritize consumer privacy. For example, Facebook is not very concerned about their

users leaving the service for Myspace. As noted previously, businesses generally try to avoid regulation, and, in order to do so, they must provide reasonable levels of privacy protection. "I think the companies understand the need for privacy protections. I think they don't want to be thought of as companies bad at privacy, which can be bad PR and create lots of regulatory oversight" (NGO). From a business perspective, being, or appearing to be, a business that protects consumer privacy can enhance the business's reputation, as well as its bottom line as Szabo pointed out at the May 20, 2014 meeting.

> I think there are groups who will not be bound, who do not perform FR, but are bound by reputational assets and reputational interests. So, I don't want to pick Consumer Federation out, but if Consumer Federation's decade long reputation as a defender of consumer rights is on the line, I feel like that in fact is an important sign on to a code. Equally important, I think if a company were to say we will be bound by the code as well would to my mind be their buy in.

However, the business community was quick to push back on the notion that signing up for the NTIA code would enhance its reputation and business interests. Hamilton of the IBIA stated at the June 24, 2014 meeting:

> We support privacy, we believe in privacy, we want biometrics to be seen as a tool to enhance privacy. But we also want to recognize the complexity of so many myriad of applications that there may be instances where an organization shouldn't be shunned or branded as an outlier, if they don't sign up to a code of conduct that professes to apply a biometric

> set of principles for privacy when in fact it just doesn't make sense for the way in which the organization has applied them for its use.

It is true that any code of conduct will have a hard time responsibly covering all legitimate business practices. Companies whose practices fall outside of the code should not be punished by consumers because they were unable to sign on. To this end corporate responsibility literature is informative. Corporate responsibility refers to responsible business practices, something that is particularly important giving the sensitivity of FR data. Simon Zadek (2007) noted that most companies learn corporate responsibility in the following five stages:

1. It's not our job to fix that
2. We'll do just as much as we have to
3. It's the business, stupid
4. It gives us a competitive advantage
5. We need to make sure everyone does it (p. 2).

With regard to privacy, many companies seem to be in the latter stages of the corporate learning process. After publicized commercial data breaches, businesses have realized that "It's the business, stupid"; therefore, they need to adopt data protection and privacy enhancing practices or face losing consumers. Early adopters of these methods may find it provides a competitive advantage in the form of increased user trust and thus increased consumer use. Finally, with regard to the code of conduct, the group is attempting to standardize best practices that create fair competitive spaces for businesses to engage in.

Businesses may find it difficult to abide by the code of conduct which is to address commercial uses of FRT. As David Lyon (2007) noted:

> [N]ot only have corporations outstripped the capacity of state administration to undertake mass surveillance in the twenty-first century, the surveillance activities of many corporations themselves have not become part of a large ensemble of governance alongside and intertwined with government administration (p. 163).

Companies may not be able to sign on to a code of conduct or abide by its privacy rules due to entanglement with government entities. A code of conduct that is limited to consumer uses of FR may not provide consumers with much protection because of government involvement.

9.1.5. Privacy and Anonymity

As explained earlier, anonymity is not privacy nor is privacy anonymity. Instead, "Anonymity allows the individual to have a voice without having a name" (Weicher, 2006, p.1) another interpretation states, "Anonymity is the ability to conceal a person's identity…" (Smith et al., 2011, p. 996). However, anonymity is often an important part of privacy. Often the reason citizens feel safe to exercise their First Amendment rights is that they feel that privacy will be protected through the relative anonymity that crowds provide. Certain participants, and one interviewee (July 29, 2014), fear the surveillance and identification powers of FRT, particularly the power it has to transform a world of relative anonymity to a world where all persons are known at all times.

> Even if a person is anonymous in some databases or has a pseudonym, he can change a pseudonym but not their biometrics. That's what makes surveillance, profiling, and discrimination possible and easier basically. That's basically the problem with biometrics. Those problems occur

> without biometrics as the IBIA [International Biometrics Industry Association] they submitted that biometrics isn't the biggest threat but big data is. I agree that that is true. But biometrics facilitates using big data because it can link all the databases without knowing the person's name. (Government).

Another potential threat to an individual's privacy is that FRT does not have to occur in real time. FRT can be applied to photos that were taken in the past if the photo is of sufficient quality. These implications are threatening. If an individual attended a political rally twenty years ago and now wants to run for political office, there could be devastating consequences, as that photo may no longer represent how that person wishes to be viewed. Previously, the photo may have looked ridiculous to others, but they would not have had the ability to identify the individual in that photo. FRT threatens an individual's ability to conceal their identity or to have a voice without a name.

A position paper released regarding anonymity by the IBIA during the meetings[46] was particularly troubling. The position paper states that to participate in society an individual must forfeit their anonymity (p. 5). The IBIA faced severe criticism from other participants for having such a strong position on anonymity during the June 24, 2014 meeting. Calabrese of the ACLU stated:

> "Anonymity and privacy are not synonymous terms. The former is forfeited if one chooses to live in society" [p.5]. Those are very very strong words. I'm surprised by them but I assume you meant them since

[46] The position paper can be found here: http://www.ntia.doc.gov/files/ntia/publications/ibia_statement_to_ntia__best_practice_recommendations_6-17-2014.pdf (IBIA, 2014b).

you used them throughout the document. Can you talk about them?

Anonymity is a pretty fundamental value in American Society.

Hamilton of the IBIA responded stating:

> We wanted to distinguish between privacy and anonymity. One of the examples is that: I value my privacy, privacy meaning I don't want to be intruded on or contacted by an organization…. the organization may know who I am, they may have a telephone book, they may have my address, they may have some of my demographics from other public data they have aggregated and analyzed but that doesn't give them the right to invade my privacy by disturbing or pushing unwanted things. We wanted to distinguish between anonymity because there is very little anonymity in our society if we are going to be productive members. What we are saying is that you are constantly going to be required to identify yourself or have your identity verified in order to receive services, privileges, drive a car, open a bank account, do just about anything to live in our society.

The IBIA drew criticism for having such an extreme position on anonymity, saying that to participate in society anonymity is forfeited. Individuals expect generalized anonymity but also recognize that they may be identified at unexpected times by participating in a public space. To state that being in public is to be identified is a violation of current social norms as pointed out in the same meeting by Travis Hall of New York University:

> It seems like the point is that anonymity should be or can be maintained contextually. It's not that to function in society you have to give up your identity at all times but in certain situations and circumstances you have to

> produce your identity. Contextually you should have the ability to protect your identity.

Biometric data alone do not possess a substantial threat to anonymity. For example, individuals leave fingerprints on many surfaces during the course of the day without the expectation of those prints being used to identify that person. However, biometrics do present a threat to anonymity because of their ability to link identified data. Hall continued:

> Biometric data the template by itself is also kind of useless. Biometric data is useful in as much as it is linked and has access to other information. It seems that the important crux here is the linkage of information, of biometric data to other pieces of information, to things that need to be protected…with FRT we have to make sure they can't be identified or it's not attached to biographic data, because for the most part those things are typically linked because biometric data not attached to other things is not terribly useful.

This exchange highlights the value that some stakeholders attach to anonymity and its ability to help protect consumer privacy. It is also true that there are certain situations in which we must be, or at least want to be, identified. The group has been tasked with deciding in which contexts it is appropriate for FRT to identify someone. The IBIA returned to the forum at the next meeting, July 24, 2014, and stated that privacy was not anonymity, clarifying that they were there to discuss privacy; however, that was where the conversation ended.

> We've offered some clarifying remarks which are posted to the website…the comment I did want to make is that we would like to focus the discussion around best practice recommendations that IBIA has entered… rather than on our findings and perspectives of the state of the world. We would rather close the debate on anonymity as it pertains to this forum but we are happy to discuss it offline. Now we want to focus on privacy matters that are germane to the scope of this work.

One participant had some clarifying remarks during an interview. The interviewee offered the following behind the scenes email exchange with the IBIA.

> The second part of their [IBIA]argument was, privacy is degraded but not our fault. Anonymity, which is something you could argue biometrics gets rid of…you don't actually have the right to that anymore. There's no way that you can actually think that you have anonymity period. …they were conflating the idea of anonymity at all times and in all places with anonymity as people understand it. So they were trying to deny that you have a right to anonymity but they were using the most extreme understanding of what anonymity means to deny that desire for generalized anonymity or anonymity period. They also were being willfully ignorant of the role that biometrics can potentially play within the broader context of privacy degrading technologies (Academic).

It is fair to say that participants, including the IBIA, have recognized the value of anonymity in society while also recognizing the ability FRT has to impose on an individual's anonymity. Stakeholders are still discussing principles for a potential code

of conduct, but it appears they will be mindful of protecting anonymity and the value it provides to society.

9.2. Anonymity and Free Speech

It has been established that anonymity is not privacy, but that anonymity can help maintain privacy; anonymity can also encourage free speech.

> A frequently cited 1995 Supreme Court ruling in McIntyre v. Ohio Elections Commission reads: Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views . . . Anonymity is a shield from the tyranny of the majority. . . . It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society. (Electronic Frontier Foundation, 2015, par. 4)

If we lose anonymity because of FRT we may severely damage free speech in our democracy. Using FRT for identification purposes is something that will have to be seriously discussed by the group and possibly curtailed to ensure the free flow of ideas and communication, especially unpopular ones. For now, the group recognizes the heightened stakes of using FRT for identification, but has yet to decide on its application or implementation.

9.3. Facial Recognition Technology as a Threat to Privacy

It has been proposed in this research that privacy needs to be reconceptualized because of the proliferation of FRT. FRT challenges the current conceptions of privacy in many ways, as will be explained in detail now. The first privacy challenge FRT poses

is its ability to mimic a skill in which humans are very accurate, which is detecting, remembering, and associating information with faces. FRT simulates a human skill. In other words, why should a technology be regulated in restrictive ways for a task that can be completed by humans and not subject to the same prohibitive restrictions?

9.3.1. Facial Recognition Technology Simulating Human Capabilities

During the course of the meetings, business entities have been quick to point out that FRT merely mimics a skill that humans readily perform. Business stakeholders have used this observation to advance their interests and argue for reduced regulation because they could simply employ humans and avoid the FRT regulations as Szabo pointed out to the group in the May 20, 2014 meeting.

> Today a reporter can take a snapshot of a yearbook and at a pot rally and identify people there. This can be done through Bing's image matching search. Casino card cheat program as you walk in the "eye in the sky" captures your image and right now it's somewhat manually done but it can also be automated to identify card cheats and ask them to leave.

In short, businesses could simply employ 500 interns to start looking through high school yearbooks to identify individuals of interest. Furthermore, there are legitimate public interest exceptions that must be recognized, such as newspapers covering "newsworthy" stories. NGO stakeholders have recognized these situations but are concerned about the limit of such exceptions as Bedoya countered at the same meeting.

> I totally understand where this…public interest, public information exception [is coming from]. My concern is that this [public interest exception] encompasses a few of the exact situations people are most

> concerned by. For example, if there is a political protest, or a political rally, that is definitely public interest, that involves politics, public affairs, certainly newsworthy. Should there be an exception that allows a news organization to photograph that rally a news organization a company that has decided to voluntarily comply with the code of conduct, should there be something that allows them to identify by name the individuals in that crowd because it is newsworthy.

The press has had an important role in promoting American democracy but there are also legitimate fears that this technology will have a chilling effect on First Amendment rights. Citizens expect a certain amount of anonymity, and that anonymity protects their privacy and encourages them to express their views. Nonetheless, business participants once again pushed back.

> This isn't about companies identifying anonymous people. This is in general, if it's a matter of public interest, news, affairs, etcetera. I think realistically if I took a picture of 30 people or 3,000 rallying on the steps of the capital and I want to know what kind of people I could easily send out 500 interns to compare images based on the groups that I have. This can all be done by human eye. I mean we are talking about a difference between an automated technology and what can be done without automated technology (Business).

However, there is a very important difference in scale of what a human can perform and what FRT is capable of, "Right but you would need 500 interns and probably 20 years.

FR could do that in a matter of minutes. That's what's different and that's why we are here" (NGO). To give an idea concerning the difference in scale, Bedoya had this to say:

> Basically the human mind according to most studies can remember 10,000 people at a maximum. As of 2012 the fastest FR algorithm was from Hitachi that could process 36 million people in a second. Now the technology exists that would allow the identification of every single person at the rally. That tension of privacy and public is what makes this interesting. People do have an expectation of privacy in public and FRT at its extreme threatens to undermine that.

The potential capability of the technology versus the capability of humans is radically different, especially when including both the time and money involved for similar identification outcomes. Furthermore, the decisions that FRT may be involved in making would be automated, which is potentially problematic as Chris Calabrese of the ACLU articulated in the April 29, 2014 meeting.

> So Pam Dickson and Bob Gellman[47] did a great report on scoring and the idea that we can use big data to score people. As we gather this kind of information does it go into a score? Is this something my employability is questioned because I was in a pot rally, we know that, and again the power of this is that it's automated. No one has to go through and make these judgments; they happen automatically.

[47] Pam Dickson is the founder of the World Privacy Forum. Robert (Bob) Gellman is a privacy policy consultant. The report referenced is titled *Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens* (World Privacy Forum, 2014).

There are legitimate concerns for the types of decisions FRT may make; therefore, a compromise may need to be drawn that includes news agencies covering only public events and public figures, but crowds would not be subject to identification via FRT. Akin to FR, scientists are asking computers to report what they see in images, this is very primitive currently. We need to ask what judgements FRT will make in the future and what values or motives operators will attach to those judgements. Additionally, FRT has incredible potential to link data that is already known about an individual, something that currently takes considerably more effort. Ultimately, because the technology replicates a skill that humans perform, it is difficult to regulate its actions. Of course the cost of employing humans for such a task would be prohibitive. It is hard to create strict regulations for a technology when the same task could be completed without the technology and no regulations would apply. However, the speed, accuracy, and scale of projects that can be completed via FRT ultimately warrant regulatory safeguards. The distinction between technology and humans task completion will present the most important impact on the creation of privacy safeguards.

9.3.2. Data

The data created by FRT is biometric. Biometric data poses specific threats to privacy that other information such as usernames and passwords, do not. Biometric data is permanent in nature and intimately linked with one's identity. Even when considering plastic surgery, the costs are usually prohibitive and the surgery is unlikely to change the orbital socket which is an identifying feature that most FR systems utilize for identification purposes. If biometric data was compromised in a data breach or other theft, an individual will be unable to use it for authentication purposes. More

importantly, as humans we are generally not allowed to hide our faces, imagine conducting one's banking business with a ski mask on. Since FRT utilizes our face for the creation of biometric data we are limited in the ways that we can protect our face from the technology.

> You can change your name….[but it is] very hard to change your face. And in fact even using facial hair, or funny haircuts, or glasses to fool facial recognition is working now is probably not going to work 5-10 years out because researchers keep getting better and better at algorithms which account for facial hair and so forth (Acquisti, 2014).

Not only is it very hard for an individual to meaningfully protect his/her face from the technology, but the technology is commonly used to authenticate known identities which contain a host of related biographic data as was shown at the March 25, 2014 meeting by Mathew Young of Sotero Defense Solutions: "So at the time that you collect you're the picture right there of the ID and you capture your live face, are there other details that are being collected such as a time stamp of when that actually happened?" King responded: "Absolutely we do." FRT scans and digital pictures contain a multitude of information, some necessary for FR and some that is simply inherent to the picture. Photos reveal a great deal of information about individuals, including race, age, gender, weight, height, hair color, eye color, disability, and location, all of which can be guessed with relative accuracy. As made clear in the previous exchange digital photos also contain a host of information, including a time stamp, document origination, date of birth, and possibly security clearances or other privileges. Many digital cameras capture what is called Extended File Information (EXIF). EXIF data contains information about the camera

that took the photo, such as file name, size, date, camera make, camera model, resolution, whether the flash was used, focal length, and Jpeg process (Alvarez, 2004, p. 2). Apple's iPhone is also capable of embedding precise geo-coordinates with photos and videos taken with the device (Friedland & Sommer, 2010, p. 1). Furthermore FR can be enacted retroactively. Photos from years in the past, if of sufficient quality, can be utilized for FR. More worrisome still, are the value judgements that either computers or humans can add to the picture and the people in it. Put succinctly, the data that photos reveal about an individual are much more detailed than when taken at face value, coupled with FR an individual and their privacy can be completely violated.

9.3.3. Data Linkage

Businesses have been eager to utilize FRT for a variety of purposes. Much has been made, during the course of the meetings, of the proprietary nature of the algorithms. It was thought initially that different algorithms would produce different results and that those results could not be compared due to their proprietary nature. However, one government participant from the Privacy Commissioner's Office in Canada, a technologist by trade, explained to the group that:

> There was a claim that two templates created from the same person by different algorithms cannot be linked together; in fact they can be linked together. So we tried to address and debunk that mess and published a note and it's published on the NTIA website (Government).[48]

[48] The full report, "Uniqueness of Face Recognition Templates" can be found at: http://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf (Chibba & Stoianov, 2014).

One can imagine the complications that could arise from being able to link algorithms conducted by two separate companies that were subscribed to by a consumer. For instance, if one can link a Facebook profile, potentially containing personal information, and a Match.com profile, where anonymity is valued, consumers could be put in a precarious or compromised position. One interviewee explained the ability to link data as follows (July 23, 2014).

> I don't know how many consumers are aware of this. There is never just one piece of data about you. There is a huge collection of data about you brought together from different sources to create profiles. And these profiles are secret, they are difficult for you to correct, amend, or find. And of course people have no idea that this is happening so they aren't able to give their consent. I personally think that is creepy and unacceptable (NGO).

Other participants have been frustrated with looking at FRT in isolation. FRT does require a camera of some sort, presumably on a phone, and needs to be coupled with some sort of application to process the photo, and then finally compared to a database of photos, more than likely social networks as they possess the most readily accessible photo archive. "You really can't look at any of these technologies anymore in isolation, that was has happened is an integrated offline and online 24/7 real-time advertising data collection system" (NGO). The ability FRT has to link one's existing data to make predictions about an individual is quite powerful as Acquisti has shown.

Acquisti's proof of concept experiment highlighted the technology's power to link data about an individual. Acquisti called the technology "first amongst peers" in terms of

its ability to link information about an individual. Databases have been called, "instruments of selection, separation and exclusion" (Bauman, 2000, p. 51). The ability to link various databases that individuals may find themselves in greatly increases the power of selection, separation, and exclusion. Similarly, the ability to link databases may identify personal patterns or habits of the subjects. Taken to an extreme, it has been suggested that this will lead to what is being called Personally Predictive Information (PPI) instead of just PII. The ability to anticipate an individual's routine could pose a significant threat to an individual's safety. Although many of the data linkages could be made without the technology, the process would be more arduous and sluggish without FRT. Olga Raskin of IBG presented to the group at the March 25, 2014 meeting:

> Facebook is probably the largest consumer usage of biometrics. The one thing about Facebook I would say that we considered relatively threatening is that once you tag photos they now have the graph search function which allows you to search photos more easily. So if there's more tagged photos there's more photos indexed and those searches can be conducted more easily… that can't be possible unless tagging is facilitated through facial recognition technology, or it will work much more slowly and the searches won't be as effective.

Speed, or immediacy, is not the real threat with the technology; rather it is the scale of projects, searches, and linkages that can be made because of its speed. We have good reasons to keep our data in separate piles; for example, there are things that we want to share on Facebook that are inappropriate for LinkedIn. Linkage of data poses a threat to privacy and some of those threats are yet unknown.

9.3.4. Cognitive Intrusion

Many, but not all participants, consider the mind a private sanctuary free from intrusion. We can choose to reveal our thoughts or keep them to ourselves. FRT is about to change that. Kairos, a company that presented at the meetings, made this recent announcement in an email press release:

> Today was an important day for Kairos. We've expanded our offering beyond facial recognition to include facial expression detection and emotion analysis. We did that by acquiring a company that we admire and who shares our values and vision of the future: IMRSV. With this acquisition, Kairos becomes the only facial biometrics company in the world offering both facial recognition and emotion analysis tools for developers (Business).

FRT being used for emotional analysis has broad implications. As shown earlier, the technology has already been employed to help facilitate deception detection. Marketers will undoubtedly use the technology to gauge emotional affect and make educated guesses concerning consumer opinion about products or services. Infrared FRT can tell if an individual is intoxicated or under stress based on body temperature and blood travel. When consumer data are linked (think about the products Amazon suggests based on browser and past purchase history information) with the emotional analysis component of FRT, the technology can make more accurate guesses about what the individual is likely thinking. The technology, particularly the emotional analysis capability, is in its infancy; however, the technology will continue to improve and make increasingly accurate guesses concerning an individual's thought process, thus violating cognitive processes.

In many ways, cognitive intrusion by the technology stands as the biggest threat to not only privacy, but also to the democratic way of life. Cognition is the precursor to expression. If the technology continues to improve in its ability to intrude on human cognition, the chilling effect could be profound on our First Amendment rights.

9.4. Reconceptualizing Privacy

So far privacy has been discussed from a variety of perspectives, including legal, societal, and as a right. H. Jeff Smith, Tamara Dinev, and Heng Xu (2011) discussed informational privacy by providing an extensive discussion on the many conceptions of privacy. Should we consider privacy as a value or human right? Is privacy a commodity that consumers can trade for benefits? Are we speaking of informational privacy or physical privacy, the right to be left alone? Should privacy be seen as cognitive with access to our thoughts? Can we come to a satisfactory definition of privacy through negation of the terms that get conflated with it: surveillance, secrecy, and anonymity? Is privacy simply the ability to control our information?

My aim is not to describe the many definitions of privacy. Previously, scholars tried to distinguish between physical and informational privacy, privacy as a value or a right, societal versus individual privacy, and many other conceptions. Unfortunately, FRT makes these distinctions unworkable.

Physical privacy, the ability to be let alone, is challenged by FRT. Images that have applied FRT reveal a great deal about the location of a person, including when he or she was there and possibly even why. FRT can then be used to identify the individual in the picture, revealing his or her physical information, such as age range, race, ethnicity, time of day and potentially other aspects given the context of the inquiry. FRT

challenges notions of physical privacy for these precise reasons. The photos that FRT is applied to also allow individuals to speculate about an individual and his or her motives. Oftentimes, information associated with an individual can be more damaging than accurate information about an individual.

According to Smith et al., informational privacy is the ability to control personally identifiable information (p. 990). FRT collects biometric data which are unique to each individual. By definition this is personally identifiable information. Given the ability for facial data to be collected secretly and the ubiquity of cameras, FRT challenges the notions of informational privacy, as well as individual control over personal information. Additionally, the compilation of an individual's data has been called an individual's "data-double" (Lyon, 2007, p. 125). The data-double creates a virtual person that replicates the physical person, especially with the collection of biometric data. The data-double further blurs the distinction between physical and informational privacy and raises concerns about where a data-double physically travels to and where it is stored at, which could be multiple locations. These travel and storage concerns can impact a physical person's freedom or access to privileges.

As humans, we lie on almost a daily basis, sometimes for altruistic reasons. One must ask, if physical privacy and informational privacy are pitted against one another, which is more important? Information can be associated with an individual for a variety of reasons but when an individual is physically located in space, time, and identity, that information is much more difficult to explain away. As stated by Mark Andrejevic (2002), "If, in other words, what people say is potentially inaccurate, uninterpretable, or illusory, the body is offered as a guarantee of some surplus beyond the manipulations of

discourse" (p. 481). FRT may show that we have manipulated or omitted information and it will do so by confirming our physical location or attributes as proof.

Even cognitive conceptions of privacy, the solitude of our minds to hold opinions and thoughts, are quickly becoming outdated and ineffective. We like to believe that we have "control" over when to reveal our thoughts and opinions to others. FRT has the ability to track eye movement, gauge an individual's temperature, via infrared FRT, and monitor emotional affect based on pupil dilation, and other physical facial markers such as smiling or frowning. As the technology continues to improve, it will be deployed in more locations, and has more images to compare an individual's affect; soon the human face may betray emotions, providing insight into human cognition.

Privacy has also been thought of as a commodity (Papacharissi, 2010). Private information can be given to retailers and other organizations in order to obtain some perceived benefit like targeted advertisements or possible discounts. The problem with this view of privacy, although it arguably allows for the most individual autonomy, is that there are public interest exceptions. Pictures are taken by the press, as photography is a First Amendment protected activity, and individuals are all but required to have state issued photo ID's, all of which can detract from an individual's ability to capitalize on commodifying one's privacy.

Since FRT links or challenges individual conceptions of privacy, the academic community should stop making these distinctions. Privacy must once again be thought of in its entirety. How scholarship can wrestle this complex topic is less certain. I believe that scholars should start to conceive of privacy in relation to interference of privacy. Interference is another subjective and context dependent term that is hard to pin down.

However, interference allows important research about privacy to continue. Researchers can start by polling data to identify privacy interference as defined by individuals; they can then try to understand why individuals feel this way and work on pragmatic solutions to address the interference. Since privacy must be addressed in its entirety, and because it remains a subjective and context dependent term, scholarship will need interference to address privacy considering it also accounts for the subjective and context dependent nature of privacy. Another benefit of thinking about privacy in terms of interference is that no new definitions of privacy are created or added to the numerous definitions already in circulation.

FRT at the time of this writing had yet to seriously impact the general public's views on privacy. It is anticipated that as the technology becomes more prevalent in use, more accurate in its capabilities of both authentication and identification, as well as increasingly adopted by the public (democratization of surveillance), those individuals interested in protecting their privacy, will be forced to adopt some methods of FRT resistance.

CHAPTER 10

CONCLUSION

This research has presented several findings that merit further exploration and comment. The primary research interest in this data was the developing regulatory regime for facial recognition technology and how it impacts consumer privacy. However, a rarity occurred during this process in that, numerous stakeholders present in a previous process regarding consumer privacy were also involved in the process for facial recognition technology. The multistakeholder literature noted this paucity, stating "Little information is available with regard to how processes build on or learn from previous experiences" (Hemmati, 2002, p. 119). The academic community is offered an opportunity to inquire into this area as the National Telecommunications and Information Administration is now charged with holding another MSH process on drone privacy (Mershon, 2014).

It is important to note that the same criticisms leveled against the MSH process for FRT are already being made against the NTIA MSH process for drones. Individuals are still concerned that these processes do not involve government or law enforcement use of the technology, which is seen as a major obstacle for public acceptance of the regulation. Similarly, the code of conduct to be created is voluntary, which opens the process up to further criticism. Finally, the convener has once again been questioned as to his or her expertise in the area with some holding the opinion that the Federal Aviation

Administration would be a more appropriate convener. Despite perceived or real shortcomings this new set of meetings provide an exciting opportunity for academics in the MSH field to interrogate how these processes can build on one another.

Regarding the process for FRT, this process has been limited in scope to strictly commercial uses of the technology. With citizens being all but required to have identification credentials with their face on them, such as a driver's license or state issued identification card, government uses of the technology should concern all citizens and not just consumers. Scandals at the Internal Revenue Service and National Security Agency, as well as successful hacking attempts on federal government databases and the White House, call into question the trust citizens have with the government. The government stores sensitive face data in their databases and have shown that they are not capable of adequately protecting it or providing the necessary oversight so that the data is not misused. Government and law enforcement uses not being covered in a code of conduct for FRT is an important limitation of this process.

FRT presents a threat not only to consumers but also to citizens. As has been shown FRT presents serious threats to how we currently view and interpret the First and Fourth Amendments. FRT will likely present challenges to the First Amendment in the form of photography and free speech. Who owns images and how those images are subsequently used, even for public interest exceptions, may require new interpretations of the First Amendment. Depending on how the technology is regulated, FRT has the potential to stifle free speech. Citizens may be less willing to exercise their First Amendment right, especially for controversial speech, if they feel that they will be identified by the technology. As has been previously discussed, facial images can be

collected surreptitiously. When these images are collected by the state, Fourth Amendment protections may be implicated. Since facial images can be collected without the awareness of the target, the Fourth Amendment may need clarification from the United States Supreme Court as to what constitutes a burdensome search.

During this MSH process for FRT business interests have been prominently on display. Consumers have a right to be skeptical about the privacy protections provided by a *voluntary* code of conduct. The code of conduct is further called into question by the fact that the NTIA is housed in the Department of Commerce, an entity with a mandate to promote U.S. business. As shown previously, the mission statement of the Department of Commerce does not contain a single mention of the word privacy, calling into question the value they place on such an important human right. It is also ironic the amount of privacy that the business stakeholder group has requested during this process. The IBIA and other business entities prefer to discuss sensitive parts of a voluntary code of conduct offline (protecting their privacy) while simultaneously working to limit the many of the privacy protections proposed for consumers in the code of conduct such as notice of the technology's use. Despite these limitations the data collected may provide insight into other research questions.

Further exploration of this data may reveal important findings about the learning process in the MSH format and may hold important data for those seeking to interrogate how MSH processes can build on one another. Stakeholders are generally either new to the MSH format or new to the topic of the MSH process. Carryover stakeholders in this process were familiar with both the topic of the process, consumer privacy, and also the MSH format. Many of the stakeholders interviewed in the first process admitted it was

complicated, frustrating, and disappointing. It is worth noting that despite large amounts of animosity in the first process, that many of the carryover stakeholders found productive and respectful ways of communicating with each other during the subsequent process. This suggests that stakeholders are able to start new beginnings for new processes despite aggravating results from previous processes. In isolation, this case study suggests that there are positive benefits to be obtained during subsequent processes from negative experiences in previous processes. This case suggests that stakeholders are willing to avoid similar negative experiences and find productive and respectful ways to interact.

The social constructivist paradigm has been adopted for this project. The MSH meetings for FRT have been tasked with creating a voluntary code of conduct which will dictate appropriate uses of the technology and the privacy protections that must be observed. This group will dictate how the technology is used. Humans are not subject to determinism by technology, instead we are involved in the daily creation and production of our world. As noted previously, cultural choices shape the use of technology, not the other way around (Nye, 2006).

This dissertation has asked three distinct research questions which merit further discussion. The first research question is: "How is the regulatory regime of FRT emerging in the U.S.?" The regulatory regime of FRT is emerging in the U.S. via the multistakeholder process. As of now only a set of best practice recommendations from the FTC exist for common commercial uses of FRT. The creation of a voluntary code of conduct for FRT has been under development at the NTIA for a year and a half with no tangible language yet in existence. Stakeholders have expressed frustration with the

length of the process, lack of input from important business participants, the limited scope of the process, and the proposed regulations in the code itself. It is unclear if this process will conclude with the creation of a voluntary code of conduct. It is apparent to this researcher that voluntary codes of conduct that apply strictly for consumer uses of FRT provide inadequate privacy protection to both consumers and citizens at large. It is hoped by this researcher that this process will conclude successfully with the creation of a code of conduct. Meaningful legislation can then be passed that will provide robust privacy protection to both consumers and citizens that reflect the nuanced language achieved through this process to allow for responsible innovation and use of the technology.

The second research question asked was: "What are the roles of the various stakeholders in shaping the commercial regulation of FRT?" There have been four primary stakeholder groups identified during this process: academics, government, business, and non-governmental organizations. It is important to note that none of these groups are homogenous in their interests or values. Academics have played an important role in providing information to the group on topics ranging from how the technology works to how the technology can be misused. Both business and NGO stakeholder groups have had academics present information that reflects their values. During this process, business entities have often been reluctant to discuss how they currently use the technology or what their plans for future use are. Business participants have argued for minimal regulation to allow for continued innovation of the technology. NGO participants have argued for increased privacy safeguards. NGO interests range from supporting Congressional legislation, providing special safeguards for minors, to concern

about the potential for discrimination. While these positions have been advocated for it remains to be seen how they will be accounted for in any potential code of conduct. Finally, government participants have had an important role in the process. The NTIA has convened the meetings and have had a hands off approach facilitating the process. The NTIA has exercised influence over the process by encouraging stakeholders to not consider government and law enforcement uses of the technology. The only other identified government participant has been the Information and Privacy Commissioner's office of Ontario Canada. This participant has largely observed the process but has also influenced the process by explaining that reverse engineering of FRT data is possible, increasing the privacy protections of the potential code of conduct.

The third research question asked was: "How does FRT challenge our current conceptions of privacy?" Depending on whether or not an individual has a property right interest in images, facial templates, and the integers created by the application of FRT, liberal notions of privacy may change. As previously discussed academics have discussed privacy in the narrowed conceptions of informational, physical, and cognitive privacy. FRT conflates all of these conceptions rendering them less useful than in the past. It has been argued that privacy should be thought of in terms of interference to account for these conceptions and the subjective and contextual nature of privacy itself. Should courts decide that an individual has a property right in the their image, facial template, or the integers created as a result of the application of FRT, consumers and citizens may have stronger legal recourse in protecting their privacy interests. Much remains to be seen for the future of privacy in the context of FRT depending on the

potential creation of a code of conduct, legal rulings, and possible congressional legislation.

This research contributes to the academic literature in the following ways.

- FRT conflates previous distinctions of privacy made by scholars (informational, physical, and cognitive); these distinctions are no longer pragmatic ways of viewing privacy and its violation.
- Since FRT conflates privacy distinctions, academics need to re-conceptualize privacy as interference to allow for the subjective and contextual nature of privacy.
- The emerging regulatory regime for FRT is being created via a voluntary code of conduct. The MSH process represents a novel way to regulate communication technology.
- Voluntary codes of conduct, while flexible enough to allow innovation for the technology, provide insufficient privacy protection due to their voluntary nature.
- The series of NTIA MSH meetings regarding consumer privacy protection offers researchers a unique opportunity to understand how MSH processes and its participants build upon one another in both positive and negative ways, which currently stands as an under researched academic area.
- Academic literature does not use the term "Regulation of Technology" yet such a field does exist.

Further exploration is needed to substantiate what amount to my musings on a tangentially related findings from this research. It remains unclear if the negative

experiences from the first process led to more productive interactions or if simple experience are responsible for the increased camaraderie and productivity. Since no new code of conduct has been created, it remains to be seen if the added experience will lead to higher rates of adoption or a code that has more intended benefits. These aspects of the MSH process warrant further exploration.

Secondly, this project has proposed and shown some of the merits of re-conceptualizing privacy as interference. This conception is untested and merits further consideration or study from privacy scholars. I contend that conceptualizing privacy as interference will lead the study of privacy in a more pragmatic direction, encouraging scholars to detect and solve privacy grievances rather than create definitions of privacy ad infinitum or merely point out the limits or problems of current conceptions of privacy. While I believe in the merits of interference I have not personally tested this conception nor have I received challenges on this conception, therefore, I cautiously suggest this alternative way to study privacy.

Finally, this research promised to track the developing regulatory regime for FRT via a voluntary code of conduct to protect consumer privacy. This process has been lengthy, in excess of a year and a half, and with no clear ending or tangible code of conduct in sight. The next meeting is scheduled for June 11, 2015. The regulatory regime for FRT is hampered by the voluntary nature of any code of conduct created, if there is one at all. The voluntary nature of the code of conduct is ultimately the biggest limitation of this process. If companies do not wish to, or cannot, comply they simply will not ascribe to the code. This provides the consumer with potentially very little protection even if a code of conduct is created. Consumers are also well within their

right to be skeptical of this process as it has been facilitated by the Department of Commerce, a department with no history of privacy protection and whose sole charge is to promote American business interests. Codes of conduct are simply no replacement for legislation and research has shown that the American public vastly prefers legislation to alternative proposals:

> A February 2002 Harris Poll showed that 63% of respondents thought current law inadequate to protect privacy. A June 2001 Gallup poll indicated that two-thirds of respondents favored new federal legislation to protect privacy online. A July 2001 Markle Foundation study concluded that 64% favored rules to protect consumers on the Internet, and 58% reported that self-regulation wasn't enough to ensure adequate accountability. A March 2000 BusinessWeek/Harris Poll found that 57% of respondents favored laws that would regulate how personal information is used. In that same poll, only 15% supported self-regulation (Electronic Privacy Information Center, 2015a).

Ultimately, if the current administration wants to be taken seriously by the American public with regard to privacy protection, stronger protections will need to be enacted.

I would be remiss to dismiss the benefits that a voluntary code of conduct presents to the business community, as well as the technology. If a voluntary code of conduct is created, its voluntary nature will promote innovation of the technology in potentially productive and imaginative ways, most of which will benefit the business community financially. Legislation is often strict in scope and purpose and would most likely eliminate certain uses of the technology, even those that are beneficial to society. Given

the nascent nature of the technology, caution should be exercised before advocating for comprehensive legislation regarding FRT.

Appendix A
Universal Declaration of Human Rights Privacy Principles

Principle	Definition	Context of Use
Legality	Government's legal authority to invade an individual's privacy as well as the legal restrictions involved in doing so.	Search warrants used to search communications must specify what information is being sought
Legitimate Aim	Only certain communications can be surveilled by specified state actors for legitimate reasons	Not all state actors have surveillance powers and those should only be used pursuant to a search warrant
Necessity	Gathering only the information necessary to build the government's case	Only communications detailing illegal or sought after activity should be collected
Adequacy	Appropriate levels of surveillance are to be used	The minimum amount of surveillance necessary to achieve goals should be used. Searching individuals not associated with a crime is prohibited. i.e. friends and family
Proportionality	Recognition that the government has disproportionate power to invade a citizen's privacy rather than vice versa.	Citizens do not possess mass surveillance capabilities as the government does. Government must limit scope of their inquiries
Competent Judicial Authority	Impartial judicial authority must be obtained prior to surveilling communications	Appropriate and unbiased judicial authority must be sought for legitimate invasion of privacy
Due Process	Ensures a fair, impartial, and public hearing for any human right infringement	
User Notification	Users must be notified their communications are being surveilled unless there are exigent circumstances	Search warrants must specify what is being sought from the individual.
Transparency	Citizens should be provided	Details of the surveillance

	notice about when, the extent to which, and the tools used to invade privacy	must be provided for the individual to appropriately defend themselves in court
Public Oversight	Ensures legitimacy and transparency of the government	e.g. The EU has public oversight offices to protect against government corruption or zealotry
Integrity of Communication Systems	The government cannot compel software/hardware providers to build in surveillance capabilities	Private firms cannot be compelled to aid in government surveillance
Safeguards for International Cooperation	Where state and national laws overlap, the ones with the higher individual protections should be used	The highest privacy protections for citizens should be used to balance the disproportionate powers of the government
Safeguards Against Illegitimate Access	Legislation ensuring against illegal government or private communication surveillance	e.g. Bill of Rights, or Consumer Privacy Bill of Rights

Appendix B
List of Interviewees

Alex Propes	Interactive Advertising Bureau
Alex Stoianov	Office of the Information and Privacy Commissioner/Ontario
Amanda Koulousias	Federal Trade Commission
Ariel Fox-Johnson	Common Sense Media
Carl Szabo	NetChoice
Chris Calabrese	American Civil Liberties Union
Craig Spiezle	Online Trust Alliance
Gautam Hans	Center for Democracy and Technology
Hauwa Otori	Internet Association
Howard Fienberg	Marketing Research Association
Jeff Chester	Center for Digital Democracy
Jennifer Lynch	Electronic Frontier Foundation
John Verdi	National Telecommunications and Information Administration
Michelle De Mooy	Consumer Action
Travis Hall	American University

Appendix C
Definitions for NTIA Privacy Multistakeholder Facial Recognition

Draft – July 21 - 2014

Algorithm: A limited sequence of instructions or steps that directs a computer system how to solve a particular problem or perform a function.[49]

Custodian: The entity or individual that holds Facial Recognition Data

Database: The facial recognition system's database or set of known subjects. May include Facial Templates.

Delete: To make unreadable Facial Recognition Data so that after deletion it cannot be used by reasonable means.[50]

OR

To remove (something, such as words, pictures, or computer files) from a document, recording, computer, etc.[51]

Encryption: The protection of data using reasonable means that have been generally accepted by experts in the field of information security, which renders such data unintelligible or unreadable.

Enroll: The process of storing and maintaining Facial Recognition Data.

Entity using Facial Recognition: An entity that uses Facial Recognition Systems to Collect and/or Use Facial Recognition Data about Subjects.

Existing Privacy Laws and Regulations: Any state or federal law or regulation that governs the collection or use of personal data from a Subject, where Facial Recognition Data could be considered one type of such data. These laws and regulations may include, but are not limited to, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection, the California Online Privacy Protection Act, the Electronic Communications Privacy Act, Section 5 of the Federal Trade Commission Act, and state UDAP ("Unfair or Deceptive Acts or Practices") laws.

---

[49] National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Algorithm": "A limited sequence of instructions or steps that tells a computer system how to solve a particular problem. A biometric system will have multiple algorithms, for example: image processing, template generation, comparisons, etc."

[50] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Identification:" "A task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity. A biometric is collected and compared to all the references in a database. Identification is "closed-set" if the person is known to exist in the database. In "open-set" identification, sometimes referred to as a "watchlist," the person is not guaranteed to exist in the database. The system must determine whether the person is in the database, then return the identity. *"*

[51] Merrian Webster definition of "delete": "to remove (something, such as words, pictures, or computer files) from a document, recording, computer, etc."

Facial Authentication: A task where the Facial Recognition System attempts to confirm an individual's claimed identity by comparing the template generated from a submitted face image with a specific known template generated from a previously enrolled face image. This process is also called one-to-one verification.[52]

Facial Detection: A task where the Facial Recognition System distinguishes the presence of a human face and/or facial characteristics without necessarily creating or deriving a Facial Template.[53]

Facial Detection Software: Software used to detect the presence of a human face.[54]

Facial Identification: Searching a database for a reference matching a submitted Facial Template and returning a corresponding identity.[55]

Facial Recognition Data: Data derived from the application of Facial Recognition Software, including Facial Template and associated metadata.

Facial Recognition Software: Software used to compare the visible physical structure of an individual's face with a stored Facial Template.[56]

Facial Recognition System: A system that uses Facial Recognition Software.

Facial Template: A digital representation of distinct characteristics of a Subject's face, representing information extracted from a photograph using a facial recognition algorithm.[57]

Facial Image: A photograph or video frame or other image that shows the visible physical structure of an individual's face

Operation of Facial Detection Software: Facial Detection Software is considered "in operation" when the process of Facial Detection is occurring.

Secure Storage of Information: Using commercially reasonable measures to secure information.[58]

---

[52] Definition based on comments from Walter Hamilton and John Dowden.

[53] Change based on definition of Facial Profiling created and submitted by Ariel Johnson and the FTC's report refers in the Case Study section to "the detection or recognition of demographic characteristics" (p. 13)

[54] Definition based on comments from stakeholders during May 20, 2014 meeting.

[55] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Identification" and "Detection Rate": "The rate at which individuals, who are in a database, are properly identified in an open-set identification (watchlist) application. *See also open-set identification, watchlist."*

[57] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Template": "a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model."*

[57] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Template": "a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison. *See also extraction, feature, model."*

Share Information: The disclosure of information to an entity other than the Entity using Facial Recognition or Subject.

Subject: The individual represented in a Facial Recognition System and/or a facial recognition database.[59]

Threshold: A user setting for Facial Recognition Systems for authentication, verification or identification. The acceptance or rejection of a Facial Template match is dependent on the match score falling above or below the threshold. The threshold is adjustable within the Facial Recognition System.[60]

---

[58] Based, in part, Article 4A-202 of the Uniform Commercial Code (the "UCC") requirements for bank transfers: "If a bank and its customer have agreed that the authenticity of payment orders . . . will be verified pursuant to a security procedure, a payment order . . . is effective as the order of the customer . . .if: (a) The *security procedure is a commercially reasonable method* of providing security against unauthorized payment orders;"

[59] Based on the National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "User": "A person, such as an administrator, who interacts with or controls end users' interactions with a biometric system. *See also cooperative user, end user, indifferent user, non-cooperative user, uncooperative user"* However, separated out to clarify the subject and the user are different.

[60] Based on National Science & Technology Council's Subcommittee on Biometrics - *Biometrics Glossary* definition of "Threshold": "A user setting for biometric systems operating in the verification or open-set identification (watchlist) tasks. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application. *See also comparison, match, matching."*

Appendix D
Mission Statement of the Department of Commerce

Mission Statement

The mission of the Department is to create the conditions for economic growth and opportunity.

As part of the Obama administration's economic team, the Secretary of Commerce serves as the voice of U.S. business within the President's Cabinet. The Department works with businesses, universities, communities, and the Nation's workers to promote job creation, economic growth, sustainable development, and improved standards of living for Americans. Through its 12 bureaus and nearly 47,000 employees located in all 50 states and territories and more than 86 countries worldwide, the Department administers critical programs that touch the lives of every American. The Department's workforce is as diverse as its mission. It is made of up economists, Nobel winning scientists, foreign service officers, patent attorneys, law enforcement officers, and specialists in everything from international trade to aerospace engineering.

The Department is comprised of 12 bureaus that work together to drive progress in four business facing key goal areas:

- Trade and Investment
- Innovation
- Environment
- Data

The underlying strength of the Department is the ability for its bureaus to work together and leverage expertise in all of these goal areas to drive economic growth.

Appendix E
List of Acronyms Used

ACA	Affordable Care Act
ACLU	American Civil Liberties Union
AI	Artificial Intelligence
CDT	Center for Democracy and Technology
CPBR	Consumer Privacy Bill of Rights
DA	Discourse Analysis
DNS	Domain Name System
EU	European Union
EXIF	Extended File Information
FBI	Federal Bureau of Investigation
FIPPS	Fair Information Practice Principles
FR	Facial Recognition
FRT	Facial Recognition Technology
FTC	Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act
IBIA	International Biometrics Industry Association
ICANN	International Corporation for Assigned Names and Numbers
IGF	Internet Governance Forum
IRS	Internal Revenue Service
ITU	International Telecommunications Union
MATP	Mobile Application Transparency Process
MDA	Mediated Discourse Analysis
MSH	Multistakeholder
NGO	Non-government Organization
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OECD	Organization for Economic Cooperation and Development
OLG	Ontario Lottery and Gaming Corporation
PII	Personally Identifiable Information
PPI	Personally Predictive Information
RFID	Radio Frequency Identification Chip
SSN	Social Security Number
TQM	Total Quality Management
UCC	Uniform Commercial Code
USSC	United States Supreme Court
WTO	World Trade Organization

Appendix F
Provisions of the NTIA

Provisions of the Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data[61]

- Accurate, up to date, relevant, and not excessive data
- Used only for legitimate purposes for which it was originally collected
- Stored in a form that does not permit identification for longer than the original purpose for which it was collected
- Data can be processed only with the consent of the individual, when legally required, or to protect the public interest or legitimate private interests
- Processing of sensitive data such as race, political opinion, religious beliefs and others are severely limited and generally require written consent from the individual
- Disclosure must be provided to the individual about the purposes for processing personal data, if any response is needed, the right to access and correct data, as well as provide notice when information has been collected without his/her consent
- The right to obtain data without excessive constraint, expense, or delay data relating to the individual
- The right to correct or delete information that is incomplete or inaccurate
- The right to data security against accidental or unlawful destruction, alteration, access, and disclosure.

[61] (Cate, 1994)

- Each state will establish an independent public authority to monitor data protection
- Data processors must also notify relevant national authorities before data processing
- The right not to be subject to legal decisions made about him/her from automated processing
- Laws must be established to provide for civil liabilities against data controllers for unlawful processing
- *Establish laws prohibiting the transfer of data to non-member states that fail to provide adequate data protection* (emphasis added)

Appendix G
Interview Protocol

Research Question	Interview Question	Follow Up Question
How is the regulatory regime of FRT emerging in the U.S.?	How did you get involved in this process?	It is claimed the MSH process is a novelty in public policy creation. What is your view on MSH?
	Have you been involved in similar MSH processes?	If yes. How can you compare experiences in this process as compared with others? (Internet governance, Internet neutrality)
	During the meetings, some civil society stakeholders have criticized the validity of the MSH process. Do you agree or disagree with this view?	If yes. What are your objections?
	In your opinion, is there any consensus emerging about the following issues: regulatory safeguards, privacy safeguards, regulation of innovative technologies.	Which groups have been most influential in forming consensus?
		How were process mechanisms managed for consensus building?
	Which are the areas of discussion where you learned the most?	Can you specify topics that you've learned the most about?
	In your opinion, what are the benefits or deficits of innovating a code of conduct via the MSH process versus a professional association or a private company?	
What are the roles of the various stakeholders in shaping the commercial regulation of FRT?	Describe your role in the FRT MSH process.	Were there some stakeholders who were more helpful or more of a hindrance to the process.
	Were there stakeholders who were more vocal at the meetings than others?	Were there any behind the scenes meetings?
	Other than increased participation, were there	What other factors impacted the influence that stakeholders

	other reasons why stakeholders may have had more or less influence on the meetings?	had on the meeting?
	Has the size of stakeholder organizations or their reputation influenced the MSH process?	Was there an impact on the process?
	What has been the role of the civil society in this process?	Have they been successful in voicing concerns of users? If yes. Who and on what points?
	Do you think the convener of the NTIA MSH meetings had a particular influence on the process and outcomes?	If yes. Which processes or outcomes were impacted?
		How were these processes or outcomes impacted?
How does FRT challenge current conceptions of privacy?	Privacy is defined differently by different people. Does FRT challenge our conceptions of data privacy, personal privacy, or in other ways?	In your view, how should we think about this issue differently?
	What is your definition of privacy?	
	Are privacy concerns more heightened because of this technology or is this an old problem revisited because of new technology?	If yes. What facets of FRT are presenting challenges and why?
	From you observation, would it be accurate to say that all stakeholders understand privacy in similar terms? If not, what are the distinct interpretations of privacy?	
	If we define privacy differently, are there new safeguards we must consider?	Why are these safeguards important?
	What are the most important considerations we must now think through for a new definition of privacy?	

	"Security vs. Privacy" is the usual argument when issues of surveillance by the government are discussed. Are there any alternative arguments proposed during the NTIA multistakeholder process on the FRT regulation?	

Appendix H
Table of Codes

Developing Policy	Multistakeholder Process
A) Data	A) Advocacy Limited Resources
1)Data Linkage	B) Alternatives to Codes of Conduct
2)De-Identified Data	1)Behind Scenes Meetings
3)Reverse Engineering Data	2)Criticism of Multistakeholder Process
B) Policy Formation	3)Praise for Multistakeholder Process
1)Consensus Formation	4)Skepticism of Legislation
2)Conflict	5)Sunset Plan to Revisit Code of Conduct
3)FTC Enforcement	C) Convener
4)Industry v. Advocate Tension	1)Convener Influence
5)Motive of Stakeholder Involvement	D) History
6)Procedure Preference for Code	1)History: Previous Processes and Results
7)Scope of Code of Conduct	E) Stakeholder Opinions and Participation
8) Stakeholder Participation	1)Feelings about Moderator
C) Privacy	2)Stakeholder Learning
1)Privacy and Anonymity	3)Stakeholder Participation
2)Privacy and Business	F) Venue
3)Privacy and Control	1)Venue Preference or Description
4)Privacy Opinions	
5)Technology and Privacy	
D) Security Protocol	
1)Notice to Consumer of FRT	
2)Security Measures and Standards	
E) FRT Uses and Applications	
1)Evasion of FRT	
2)Facial Profiling	
3)Human Simulations of FRT	
4)Stages of FRT	
5)Surveillance	
6)Technology Uses	

REFERENCES

Acquisti, A. (2014). [Real Time Face Recognition Study]. Unpublished raw data.

Aftergood, S. (2015). Privacy and the imperative of open government. In M. Rotenberg, J. Horwitz, & J. Scott (Eds.), *Privacy in the modern age: The search for solutions* (pp. 204-216) New York: The New Press.

Allen, A. L. (1998). Coercing privacy. *Wm. & Mary L. Rev.*, *40*, 723.

Allen, A. L. (1999). Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm. *Conn. L. Rev.*, *32*, 861.

Alvarez, M. R. (1999). Modern technology and technological determinism: the Empire strikes again. *Bulletin of Science, Technology & Society*, *19*(5), 403-410.

Alvarez, P. (2004). Using extended file information (EXIF) file headers in digital evidence analysis. *International Journal of Digital Evidence*, *2*(3), 1-5.

Alvesson, M., & Karreman, D. (2000). Varieties of discourse: On the study of organizations through discourse analysis. *Human Relations*, *53*(9), 1125-1149.

American Civil Liberties Union. (2003). Q&A On Face-Recognition. Retrieved from https://www.aclu.org/technology-and-liberty/qu-face-recognition

American Civil Liberties Union. (2014). About the ACLU. Retrieved from https://www.aclu.org/about-aclu-0

American Institute of Architects. (2014). About the AIA. Retrieved from http://www.aia.org/about/facilities/

Andrejevic, M. (2002). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4).

Antonova, S. (2011). Capacity-building" in global Internet governance: The long-term outcomes of "multistakeholderism. *Regulation & Governance*, *5*(4), 425-445.

Application Developers Alliance. (2015). The Application Developers Alliance. *Application Developers Alliance.* Retrieved from http://www.appdevelopersalliance.org/about/about-the-alliance/

Argyris, C. (1976). Single-loop and double-loop models in research on decision making. *Administrative science quarterly*, 363-375.

Associated Press. (2013). Number of active users at Facebook over the years: How Facebook has grown: Number of active users at Facebook over the years. *Yahoo News.* Retrieved from https://news.yahoo.com/number-active-users-facebook-over-230449748.html

Atick, J. J. (2011). Face Detection & Face Recognition Consumer Applications. (White Paper). Retrieved from International Biometrics & Identification Association website: http://www.ibia.org/resources/

Atick, J. (2014, February). *How Facial Recognition Technology Works.* Paper presented at the National Telecommunications and Information Administration Multi-stakeholder Meetings on Facial Recognition, Washington D.C.

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: theory, strategy, and practice*. Oxford University Press.

Ballantyne, M., Boyer, R. S., & Hines, L. (1996). Woody bledsoe: His life and legacy. *AI magazine*, *17*(1), 7.

Bauman, Z. (2000). *Globalization: The human consequences*. Columbia University Press.

Belmas, G., & Overbeck, W. (2012). *Major principles of media law* USA: Wadsworth

Bentley, L. (2010). House Bipartisan Privacy Caucus Wants More on Facebook Data Leak. ITBusinessEdge. Retrieved from http://www.itbusinessedge.com/cm/blogs/bentley/house-bipartisan-privacy-caucus-wants-more-on-facebook-data-leak/?cs=43851

Biometrics Institute. (2015). About Biometrics. *Biometrics Institute*. Retrieved from http://www.biometricsinstitute.org/pages/about-biometrics.html

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the internet: self-regulation or government regulation?. *Business Ethics Quarterly*, 323-342.

Brackeen, B. (2014). *Kairos Facial Recognition Uses*. Symposium conducted at the meeting of the National Telecommunications and Information Administration Multistakeholder Meetings for Facial Recognition, Washington D.C.

Brandom, R. (2014). Why Facebook is Beating the FBI at Facial Recognition. *The Verge.* Retrieved from http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition

Brickhouse Security. (2015). What is CCTV? *Brickhouse Security*. Retrieved from http://www.brickhousesecurity.com/category/video+surveillance+security+cameras/about+cctv+cameras.do

Brown, E. (2011). Final Version of NIST Cloud Computing Definition Published. *Tech Beat.* Retrieved from http://www.nist.gov/itl/csd/cloud-102511.cfm

Cate, F. H. (1994). EU Data Protection Directive, Information Privacy, and the Public Interest, The. *Iowa L. Rev.*, *80*, 431.

Center for Democracy and Technology. (2014). About CDT. Retrieved from https://cdt.org/about/

Center for Digital Democracy. (2014). About CDD. Retrieved from http://www.democraticmedia.org/about-cdd

Chandler, J. (2007). The Autonomy of Technology: Do Courts Control Technology or Do They Just Legitimize Its Social Acceptance?. *Bulletin of Science, Technology & Society*, *27*(5), 339-348

Chandler, J. A. (2012). "Obligatory Technologies": Explaining Why People Feel Compelled to Use Certain Technologies. *Bulletin of Science, Technology & Society*, 0270467612459924.

Charlie (personal communication, January 5, 2015).

Chibba, M. (2014). *Technical Privacy Safeguards for Facial Recognition*. Symposium conducted at the meeting of the National Telecommunications and Information Association, Washington D.C.

Chibba, M., & Soianov, A. (2014). *On Uniqueness of Facial Recognition Templates.* Symposium conducted at the meeting of the National Telecommunications and Information Association, Washington D.C.

Coase, R. H. (1959). The federal communications commission. *Journal of Law and Economics*, 1- 40.

Codding Jr, G. A. (1994). International Telecommunications Union: 130 Years of Telecommunications Regulation, The. *Denv. J. Int'l L. & Pol'y*, *23*, 501.

Coglianese, C. (1997). Assessing consensus: The promise and performance of negotiated rulemaking. *Duke Law Journal*, 1255-1349.

Coleman, J. S. (1982). *The asymmetric society*. Syracuse University Press.

Common Criteria (2015). About the common criteria. *Common Criteria*. Retrieved from https://www.commoncriteriaportal.org/ccra/

Common Sense Media. (2014). Our Mission. Retrieved from https://www.commonsensemedia.org/about-us/our-mission#about-us

Consumer Federation of America. (2014). Overview. Retrieved from http://www.consumerfed.org/about-cfa/overview

Creswell, J. W. (2009). Research design: qualitative, quantitative, and mixed methods approaches.

Davies, S. (2015). Privacy opportunities and challenges with Europe's new data protection regime. In M. Rotenberg, J. Horwitz, & J. Scott (Eds.), *Privacy in the modern age: The search for solutions* (pp. 204-216) New York: The New Press.

de Saint-Georges, I. (2004). Materiality in discourse: The influence of space and layout in making meaning. *Discourse and technology: Multimodal discourse analysis*, 71-87.

DeWalt, K. M., & DeWalt, B. R. (2011). *Participant observation: A guide for fieldworkers*. Rowman Altamira.

Dupont, B. (2008). Hacking the panopticon: distributed online surveillance and resistance. *Sociology of Crime Law and Deviance, 10*, 259-280.

Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *Engineering Management, IEEE Transactions on*, *52*(2), 227-237.

Electronic Frontier Foundation. (2015). Anonymity. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/issues/anonymity

Electronic Privacy Information Center. (2014). EPIC v. FBI – Next Generation Identification Seeking documents about the FBI's expansive biometric identification database. *Electronic Privacy Information Center.* Retrieved from https://epic.org/foia/fbi/ngi/

Electronic Privacy Information Center. (2015a). Public Opinion on Privacy. *Electronic Privacy Information Center.* Retrieved from https://www.epic.org/privacy/survey/

Electronic Privacy Information Center. (2015b). About EPIC. *Electronic Privacy Information Center*. Retrieved from https://epic.org/epic/about.html

Ernst-Oliver, W. (2015). A Brief History of Safe Harbor. *Privacy Association*. Retrieved from https://privacyassociation.org/resources/article/a-brief-history-of-safe-harbor/

Erwin, P. M. (2011). Corporate codes of conduct: The effects of code content and quality on ethical performance. *Journal of Business Ethics*, *99*(4), 535-548.

Etzioni, A. (1999). *The limits of privacy*. Basic Books.

Export (2013). Welcome to the U.S.-EU Safe Harbor. *Export.gov.* Retrieved from http://export.gov/safeharbor/eu/eg_main_018365.asp

Facebook (2012). Terms of Service. Retrieved from https://www.facebook.com/legal/terms

Fairclough, N. (1995). Critical discourse analysis: The critical study of language. Routledge.

Federal Trade Commission. (2011). FTC Announces Agenda, Panelists for Facial Recognition Workshop. Retrieved from https://www.ftc.gov/news-events/press-releases/2011/11/ftc-announces-agenda-panelists-facial-recognition-workshop

Federal Trade Commission. (2014). FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies: Companies Using the Technologies Should Design Services with Consumer Privacy in Mind. Retrieved from http://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

Foucault, M. (1995). Discipline and punishment the birth of the prison. New York: Random House.

Fransen, L. W., & Kolk, A. (2007). Global rule-setting for business: A critical analysis of multi-stakeholder standards. *Organization*, *14*(5), 667-684.

Friedland, G. F. (2010, August). Cybercasing the Joint: On the Privacy Implications of Geo-Tagging. In *HotSec*.

Frith, M. (2004). How Average Briton is Caught on Camera 300 Times a Day. *The Independent.* Retrieved from http://www.independent.co.uk/news/uk/this-britain/how-average-briton-is-caught-on-camera-300-times-a-day-572781.html

Fuchs, C. (2011). An alternative view of privacy on Facebook. *Information*, *2*(1), 140-165.

Fuller, J. (2014). Rand Paul Files Suit Against Obama, NSA Wednesday. *Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/post-politics/wp/2014/02/12/rand-paul-files-suit-against-obama-nsa-today/

Fuller, K. E. (2001). ICANN: The debate over governing the internet. *Duke Law & Technology Review*, *1*(1), 1.

Fylan, F. (2005). Semi structured interviewing. *A handbook of research methods for clinical and health psychology*, 65-78.

Galvin, A. (2014). *Adolescent Brain Development*. Symposium conducted at the meeting of the National Telecommunications and Information Administration Multistakeholder meetings for Facial Recognition, Washington D.C.

Gates, K. (2011). Our Biometric Future. NYU Press.

Gellman, R. (2014). Fair information practices: A basic history. *Available at SSRN 2415020*.

Grandoni, D. (2014). Facebook's New 'DeepFace' Program Is Just As Creepy As It Sounds. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2014/03/18/facebook-deepface-facial-recognition_n_4985925.html

Gray, B. (1989). Collaborating: Finding common ground for multiparty problems. San Francisco: Jossey-Bass.

Grother, P. (2014). *Automated Facial Age Estimation*. Symposium conducted at the meeting of the National Telecommunications and Information Administration Multistakeholder meetings for Facial Recognition, Washington D.C.

Gutierrez, G., & Stump, S. (2014). 'Cute Convict' Suing Website Over Use of Her Mug Shot. *Today*. Retrieved from http://www.today.com/news/cute-convict-suing-website-over-use-her-mug-shot-2D79315363

Hatch, M. J. (2006). *Organization theory: modern, symbolic and postmodern perspectives*. Oxford university press.

Hatcher, C. (2001). Silent Video Surveillance in the Absence of Probable Cause – A Brief Legal Checklist. Retrieved from http://www.daviddfriedman.com/Academic/Course_Pages/21st_century_issues/21st_century_law/video_surveillance_01.htm

Held, D. (2006). *Models of democracy*. Stanford University Press.

Hemmati, M. (2002). *Multi-stakeholder processes for governance and sustainability: beyond deadlock and conflict*. Routledge.

Hintz, A, & Milan, S. (2014). In Multistakeholderism We Trust: On the limits of the multistakeholder debate. Retrieved from http://www.global.asc.upenn.edu/in-multistakeholderism-we-trust-on-the-limits-of-the-multistakeholder-debate/

Hiremath, P. S., & Hiremath, M. (2013). Depth and Intensity Gabor Features Based 3D Face Recognition Using Symbolic LDA and AdaBoost. *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, *6*(1), 32.

Holt, T. J. (2004). The fair and accurate credit transactions act: New tool to fight identity theft. *Business Horizons*, *47*(5), 3-6.

Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Review*, *25*(1), 84-88.

Huckin, T. (2002). Textual silence and the discourse of homelessness. *Discourse & Society*, *13*(3), 347-372.

Hurley, D. (2015). Taking the long way home: The human right of privacy. In M. Rotenberg, J. Horwitz, & J. Scott (Eds.), *Privacy in the modern age: The search for solutions* (pp. 204-216) New York: The New Press.

International Biometrics and Identification Association. (2014a). About Us. Retrieved from http://www.ibia.org/association/

International Biometrics and Identification Association. (2014b). IBIA Privacy Best Practice Recommendations for Commercial Biometric Use. Retrieved from http://www.ntia.doc.gov/files/ntia/publications/ibia_statement_to_ntia_-_best_practice_recommendations_6-17-2014.pdf

Jafri, R., & Arabnia, H. R. (2009). A Survey of Face Recognition Techniques. *JIPS*, *5*(2), 41-68.

Jewitt, C., Kress, G., Ogborn, J., & Tsatsarelis, C. (2001). Exploring learning through visual, actional and linguistic communication: The multimodal environment of a science classroom. *Educational Review*, *53*(1), 5-18.

John, R. R. (2008). Telecommunications. *Enterprise and Society*, *9*(3), 507-520.

Johnston, A. (2004). Files, forms, and fonts: mediational means and identity negotiation in immigration interviews. *Discourse and Technology*, 116.

Jones, R. H. (1999). Mediated action and sexual risk: searching for'culture'in discourses of homosexuality and AIDS prevention in China. *Culture, health & sexuality*, *1*(2), 161-180.

Jones, R. H. (2007). Imagined comrades and imaginary protections: Identity, community and sexual risk among men who have sex with men in China. *Journal of homosexuality*, *53*(3), 83-115.

Kang, T. (2000). Cryptography. Retrieved from http://cyber.law.harvard.edu/privacy/Encryption%20Description.html

Kaste, M. (2013). A Look Into Facebook's Potential to Recognize Anybody's Face. Retrieved from http://www.npr.org/blogs/alltechconsidered/2013/10/28/228181778/a-look-into-facebooks-potential-to-recognize-anybodys-face

Kenworthy, B. (2012). Photography & the First Amendment. *First Amendment Center*. Retrieved from http://www.firstamendmentcenter.org/photography-the-first-amendment

Kerr, O. S. (2009). Vagueness Challenges to the Computer Fraud and Abuse Act. *Minn. L. Rev.*, *94*, 1561.

Kincaid, J. (2011). Google+ Introduces Automatic Face Recognition To Photo Tagging (But It's Completely Opt-In). *TechCrunch*. Retrieved from http://techcrunch.com/2011/12/08/google-introduces-automatic-face-recognition-to-photo-tagging-but-its-completely-opt-in/

King, R. (2014). Picasso. Symposium conducted at the meeting of the National Technology and Information Association, Washington D.C.

Kolk, A., Van Tulder, R., & Welters, C. (1999). International codes of conduct and corporate social responsibility: can transnational corporations regulate themselves?. *Transnational corporations*, *8*(1), 143-180.

Kong, S. G., Heo, J., Abidi, B. R., Paik, J., & Abidi, M. A. (2005). Recent advances in visual and infrared face recognition—a review. *Computer Vision and Image Understanding*, *97*(1), 103-135.

Kravets, D. (2013). Student Suspended For Refusing To Wear RFID Chip Returns To School. *Wired.* Retrieved from http://www.wired.com/2013/08/student-rfid-chip-flap/

Kress, G., & Van Leeuwen, T. (2001). *Multimodal discourse* (Vol. 208). London: Arnold.

Kroft, S. (2014). The Data Brokers: Selling Your Personal Information. *CBS News*. Retrieved from http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/

Lessig, L. (2006). *Code*. Lawrence Lessig.

Levi-Faur, D. (2011). Regulation and regulatory governance. *Handbook on the Politics of Regulation*, 1-25.

Liu, C., Shum, H. Y., & Freeman, W. T. (2007). Face hallucination: Theory and practice. *International Journal of Computer Vision*, *75*(1), 115-134.

Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity.

March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization science*, *2*(1), 71-87.

Marx, L. (1994). The idea of "technology" and postmodern pessimism. In *Technology, pessimism, and postmodernism* (pp. 11-28). Springer Netherlands.

McCallister, E., Grance, T., & Scarfone, K. A. (2010). SP 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

McCullagh, D. (2001). Call it super bowl face scan I. *Wired.* Retrieved from http://archive.wired.com/politics/law/news/2001/02/41571

McLuhan, M. (1994). *Understanding media: The extensions of man*. MIT press.

Mellinger, P. T. (2011). Cracking Watergate's infamous 18 ½ minute gap. *Forensic Magazine.* Retrieved from http://www.forensicmag.com/articles/2011/02/cracking-watergates-infamous-18-1-2-minute-gap

Merriam-Webster. (2015). JPEG. Merriam-Webster Dictionary. Retrieved from http://www.merriam-webster.com/dictionary/jpeg

Mershon, E. (2014). NTIA to take up drone privacy guidelines — Increasingly partisan FCC under Wheeler — Oversight hearing takes aim at FTC's practices, authority. *Politico.* Retrieved from http://www.politico.com/morningtech/0714/morningtech14761.html

Meyer, P. (2010). *Liespotting: proven techniques to detect deception*. Macmillan.

Mill, J. S. (1988). *On Liberty*. New York: Penguin Books Ltd.

Mitroff, I. I. (1983). *Stakeholders of the organizational mind*. San Francisco: Jossey-Bass.

Morozov, E. (2012). In Your Face. [Review of the book Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance by Kelly Gates]. London Review of Books. Retrieved from http://www.lrb.co.uk/v34/n07/evgeny-morozov/in-your-face

Mulligan, D. K. (2003). Reasonable expectations in electronic communications: A critical perspective on the Electronic Communications Privacy Act. *Geo. Wash. L. Rev.*, *72*, 1557.

Murray, M. (2014). Congress on Track to be Least Productive in Modern History. Retrieved from http://www.nbcnews.com/politics/first-read/congress-track-be-least-productive-modern-history-n169546

Navarette, R. (2014). Why a minority opposes affirmative action. Retrieved from http://www.cnn.com/2014/04/24/opinion/navarrette-affirmative-action/

Necessary and Proportionate. (2014). International Principles on the Application of Human Rights to Communications Surveillance. *Necessary and Proportionate*. Retrieved from https://en.necessaryandproportionate.org/text

Neier, A. (1975). *Dossier: The secret files they keep on you*. New York: Stein and Day.

NetChoice. (2014). About Us. Retrieved from http://netchoice.org/#about

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nonnenmacher, T. (2001). State promotion and regulation of the telegraph industry, 1845–1860. *The Journal of Economic History*, *61*(01), 19-36.

Nye, D. E. (2006). *Technology matters: Questions to live with* (pp. 194-198). Cambridge, MA: MIT Press.

Opam, K. (2014). Pioneering facial recognition scientist now fears his work's consequences. *The Verge*. Retrieved from https://www.theverge.com/2014/5/18/5726904/pioneering-facial-recognition-scientist-now-fears-his-works

O'Toole, J. (2014). Facebook's new face recognition knows you from the side. *CNN Money*. Retrieved from http://money.cnn.com/2014/04/04/technology/innovation/facebook-facial-recognition/

Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday*, *15*(8).

Pavlidis, I., Eberhardt, N. L., & Levine, J. A. (2002). Human behaviour: Seeing through the face of deception. *Nature*, *415*(6867), 35-35.

Pew Research Center. (2014). Congressional Favorability. Retrieved from http://www.pewresearch.org/data-trend/political-attitudes/congressional-favorability/

Potter, J., & Wetherell, M. (1987). *Discourse and social psychology: Beyond attitudes and behaviour*. Sage.

Press, G. (2014). *Forbes*. 12 Definitions of Big Data: What's Yours. Retrieved from http://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/

Preston, C., & McCann, E., (2011). Unwrapping shrinkwraps, clickwraps, and browsewraps: How the law went wrong from horse traders to the law of the horse. *BYU Journal of Public Law*, *26*(1), 1-35. Retrieved from http://ezproxy.library.und.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=74716653&site=ehost-live&scope=site

Privacy Association. (2013). Wyndham, LabMD, Cases Challenging FTC. *Privacy Association.* Retrieved from https://privacyassociation.org/news/a/wyndham-labmd-cases-challenging-ftc

Pu Holt, T. J. (2004). The fair and accurate credit transactions act: New tool to fight identity theft. *Business Horizons, 47*(5), 3-6

Radford, T. (2004). How We Recognize Faces. *The Guardian*. Retrieved from http://www.theguardian.com/uk/2004/dec/13/sciencenews.research

Rainie, L., Kiesler, S., Kang, R., and Madden, M. (2013). Anonymity, Privacy, and Security Online. *Pew Research Internet Project*. Retrieved from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Randolph, J. J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research & Evaluation, 14*(13), 2.

Raudaskoski, P. (2010). "Hi Father", "Hi Mother": A multimodal analysis of a significant, identity changing phone call mediated on TV. *Journal of Pragmatics, 42*(2), 426-442.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Univ of North Carolina Press.

Researchware. (2014). Hyperresearch. Retrieved from http://www.researchware.com/products/hyperresearch.html

Robertson, A. (2013). Federal Judge Rules NSA's Bulk Phone Record Collection Likely Unconstitutional. The Verge. Retrieved from http://www.theverge.com/2013/12/16/5217064/federal-judge-rules-nsas-bulk-phone-collection-likely-unconstitutional

Roome, N., & Wijen, F. (2006). Stakeholder power and organizational learning in `corporate environmental management. *Organization Studies, 27*(2), 235-263.

Rosen, J. (2000). The unwanted gaze. *New York: RandomHouse*.

Rouse, M. (2008). Biometric Verification. *Search Security*. Retrieved from http://searchsecurity.techtarget.com/definition/biometric-verification

Russell, I. F. (1991). Neural networks in the undergraduate curriculum. *Journal of Computing Sciences in Colleges*, *6*(5), 92-97.

Sashkin, M. (1993). *Putting total quality management to work: what TQM means, how to use it, & how to sustain it over the long run*. Berrett-Koehler Publishers.

Schauer, F. (1981). Categories and the First Amendment: A Play in Three Acts. *Vand. L. Rev.*, *34*, 265.

Schneier, B. (2015). Fear and convenience. In M. Rotenberg, J. Horwitz, & J. Scott. (Eds.), *Privacy in the modern age: The search for solutions* (pp. 204-216) New York: The New Press.

Schreiner, B. (2009). KFC Stores Colonel's Secret Recipe In New, Safer Vault. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2009/02/10/kfc-stores-colonels-secre_n_165630.html

Schwilch, G., Bachmann, F., Valente, S., Coelho, C., Moreira, J., Laouina, A., & Reed, M. S. (2012). A structured multi-stakeholder learning process for Sustainable Land Management. *Journal of Environmental Management*, *107*, 52-63.

Scollon, R. (2008). *Analyzing public discourse: Discourse analysis in the making of public policy*. London: Routledge.

Scollon, R., & Scollon, S.W. (2004). *Nexus analysis: Discourse and the emerging internet*. London: Routledge

Scollon, S., & de Saint-Georges, I. (2012). Mediated discourse analysis. In Gee, J.P. & Handford, M. (Eds.), *The Routledge Handbook of Discourse Analysis* (pp. 66-78), New York: Routledge.

Sisson, K., & Marginson, P. (2001). *" Soft Regulation": Travesty of the Real Thing Or New Dimension?*. ESRC" One Europe or Several?" Programme, Sussex European Institute, University of Sussex.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, *35*(4), 989-1016.

Snouffer, R., Lee, A., & Oldenhoeft, A. (2001). *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2* (No. NIST-SP-800-29). BOOZ-ALLEN AND HAMILTON INC MCLEAN VA.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Sottek, T. C. (2013). The Xbox One will always be listening to you, in your own home (update) Did Microsoft just invent the Telescreen from '1984?'. *The Verge*. Retrieved from http://www.theverge.com/2013/5/21/4352596/the-xbox-one-is-always-listening

Sotto, L. J., & Simpson, A. P. (2014). United States. In Jay, R.P. Editor. *Data Portection and Privacy in 26 jurisdictions worldwide*. Retrieved from http://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdf

Starks, H., & Trinidad, S. B. (2007). Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. *Qualitative Health Research, 17*(10), 1372-1380.

Stokes, R. (1999). Fair Credit Reporting Act.

Strauss, S., & Feiz, P. (2014). *Discourse Analysis: Putting our worlds into words*. Routledge.

Swanborn, P. (2010). *Case study research: what, why and how?*. Sage.

Terilli, S. A. Jr. and Splichal, S. (2011). Privacy Rights in an Open and Changing Society. In Hopkins, W. W. Editor (Ed.), Communication and the Law. Alabama: Vision Press.

Treadwell, D. (2011). *Introducing communication research: Paths of inquiry*. Sage.

Turcotte, M. F., & Pasquero, J. (2001). The paradox of multistakeholder collaborative roundtables. *The Journal of Applied Behavioral Science, 37*(4), 447-464.

Tummarello, K. (2014). Apps look to simplify privacy notices. *The Hill.* Retrieved from http://thehill.com/policy/technology/200818-apps-look-to-simplify-privacy-notices

Tunick, M. (2009). Privacy in Public Places: Do GPS and Video Surveillance Provide Plain Views? *Social Theory and Practice*, 597-622.

Tyson, A. (2014). Obama viewed as more caring than Bush, but no more effective. Pew Research. Retrieved from http://www.pewresearch.org/fact-tank/2014/07/16obama-viewed-as-more-caring-than-bush-but-no-more-effective/

U.S. Department of Commerce, National Institute of Standards and Technology. (2014). National Strategy for Trusted Identities in Cyberspace. Retrieved from http://www.nist.gove/nstic/NSTIC-FIPPS.pdf

U.S. Department of Commerce, National Institute for Standards and Technology. (2015). About NIST. Retrieved from http://www.nist.gov/public_affairs/nandyou.cfm

U.S. Department of Health and Human Services. (2015). Health Information Privacy: What is Encryption? Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2021.html

U.S. Securities and Exchange Commission, Office of Information Technology. (2007). Privacy Impact Assessment (PIA) Guide. Retrieved from https://www.sec.gov/about/privacy/piaguide.pdf

Vaillant, M. (2014, February). How Facial Recognition Technology Works. Symposium conducted at the National Telecommunications and Information Administration Multi-stakeholder Meetings for Facial Recognition, Washington D.C.

Volz, D. (2014). FBI's Facial-Recognition Technology Has Achieved 'Full Operational Capability' No Turning Back: Next-gen facial-recognition technology has arrived, despite concerns from privacy groups. *National Journal*. Retrieved from http://www.nationaljournal.com/tech/fbi-s-facial-recognition-technology-has-achieved-full-operational-capability-20140915

Wagstaff, K. (2014). Smile, Seattle! Police Now Can Use Facial Recognition Software. *NBC News*. Retrieved from http://www.nbcnews.com/tech/security/smile-seattle-police-now-can-use-facial-recognition-software-n51311

Wang, S., Li, W., Wang, Y., Jiang, Y., Jiang, S., & Zhao, R. (2012). An improved difference of gaussian filter in face recognition. *Journal of Multimedia*, *7*(6), 429-433.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Waz, J., & Weiser, P. (2012). Internet governance: The role of multistakeholder organizations. *Journal of Telecommunications and High Technology Law*, *10*(2).

Weicher, M. (2006). [Name withheld]: Anonymity and its implications. *Proceedings of the American Society for Information Science and Technology*, *43*(1), 1-11.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

White House. (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Retrieved from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

White House. (2014). Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights. Retrieved from http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

Wiener, J. B. (2004). The regulation of technology, and the technology of regulation. *Technology in Society*, *26*(2), 483-500.

Wilhelm, E. O. (2015). A Brief History of Safe Harbor. Privacy Association. Retrieved from https://privacyassociation.org/resources/article/a-brief-history-of-safe-harbor/

Williams, J. (2014). *Consumer Profiling.* Symposium conducted at the meeting of the National Telecommunications and Information Administration Multistakeholder Meetings for Facial Recognition, Washington D.C.

Wolf, C. (2015). Envisioning privacy in the world of big data. In M. Rotenberg, J. Horwitz, & J. Scott (Eds.), *Privacy in the modern age: The search for solutions* (pp. 204-216) New York: The New Press.

Wood, C. (2014). Are We Truly Ready for Government to Use Biometric Identifiers? If a new survey says. Government Technology. Retrieved from http://www.govtech.com/public-safety/Are-We-Truly-Ready-for-Government-to-Use-Biometric-Identifiers.html

World Privacy Forum. (2015). WPF Report – Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens, Part III in a series. Retrieved from https://www.worldprivacyforum.org/2013/10/report-data-brokers-and-the-federal-government-a-new-front-in-the-battle-for-privacy-opens/

Yanes, A. (2014). Privacy and Anonymity. *arXiv preprint arXiv:1407.0423*.

Yin, R. (1984). *Case study research: Design and methods*. Beverly Hills, CA: Sage Publishing.

Yin, R. K. (1989). *Case study research: Design and Methods*. Newbury Park, CA: Sage

Zadek, S. (2007). The path to corporate responsibility. In *Corporate ethics and corporate governance* (pp. 159-172). Springer Berlin Heidelberg.