AM I WHO I SAY I AM? THE ILLUSION OF CHOICE: BIOMETRIC IDENTIFICATION IN HEALTHCARE

By

Morgan Catherine Banville

May 2023

Director of Dissertation: Dr. Nicole Caswell

Major Department: English

ABSTRACT

Grounded in surveillance studies and technical communication, this study defines biometric identification technologies as personal identifiers of the body, focusing specifically on how neonatal nurses use and perceive such technologies within the context of the United States healthcare system. As biometric identification and authentication becomes more commonplace within various sectors such as healthcare and medical-adjacent, it is crucial for technical communicators to return to the origins of biometric implementation to inform current interventions, and to question the reasons behind the urgency of implementing such technologies for efficiency, security, and compliance. Drawing from a corpus of communication materials from biometric companies, questionnaires, and ten interviews with neonatal nurses, this study explores the justification of implementing biometric technologies, including how biometric technologies are defined. Data analysis was conducted using interlocking surveillance, a framework that addresses sites of surveillance and their levels of awareness, advocacy, and

transparency of normalized surveillant practices. This study contributes to understandings and perceptions that neonatal nurses have of biometric technologies in healthcare and extends far past the scope of privacy. Even so, privacy in this study is situated as both a tradeoff and illusion of choice: you can change your password, but you can't change your fingerprint. Because the U.S. has a preoccupation with security and surveillance technologies, this study can better inform technical communicators how to intervene in and implement decision-making practices. In particular, this study argues that neonatal nurses are technical communicators: they communicate and negotiate specialized information. The findings contribute to redefining what it means to be a technical communicator, re-rhetoricizing how technical communication is represented in the medical sector. Further takeaways from the study influence future coalitional work, questioning and revising normalized surveillance including ethics of biometric use, and localization of community input and participatory approaches for design of and intervention in communication materials.

Am I Who I Say I Am? The Illusion of Choice: Biometric Identification in Healthcare

A Dissertation

Presented to the Faculty of the Department of English

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Doctor of Philosophy in Rhetoric, Writing, and Professional Communication

By

Morgan Catherine Banville

May 2023

Director of Dissertation: Nicole Caswell, Ph.D.

Dissertation Committee Members:

Erin Frost, Ph.D.

William Banks, Ph.D.

Emma Rose, Ph.D.

© 2023, Morgan Catherine Banville

DEDICATION

I dedicate this dissertation to all the first-generation college students. I see you. I know you. I'm proud of you. You can do it.

ACKNOWLEDGEMENTS

Out of the entire dissertation study, this section was the most difficult to write. How do you even begin to acknowledge all the people — family, friends, mentors, scholars, the neonatal nurses I interviewed for this study, and so on who have influenced and supported not just your scholarship, but your life? I could write an entire book about all the people over the last four years who have supported me through this degree (and the COVID-19 pandemic). By the time this dissertation is published, I'm sure I'll read this back and say, "oh shit, I forgot someone." Know that this is unintentional, and I appreciate you. Allegedly, it takes quite some time to come down from the wave of dissertation burnout.

When I was 12 years old, a sixth grader living in a SouthCoast town in Massachusetts, I proudly wrote that I wanted to be a Professor of English when I "grew up." The dream has become a reality 14 years later. I want to acknowledge that ambitious little middle schooler. I think she'd be really proud.

I also want to thank my advisor, Nicole Caswell. Nikki, I literally could not have done this without you. I needed the approval, obviously. But in all seriousness, you are the exemplar of what it means to be a mentor. I can't thank you enough nor put into words the number of texts, emails, calls, and thankless hours you dedicate to me, and all of your students. I'm lucky to now call you a friend.

I want to thank Erin Frost, Will Banks, and Emma Rose for *all* their guidance and feedback on this lengthy document. You three have made me a more curious thinker, critical analyzer, and have fueled (and supported) my passion for enacting change. Like Nikki, it's tough to put into words what your mentorship means to me. I'm excited to co-author chapters and organize professional events with you in the years to come. You're all models of what intentional research, instruction, and mentorship looks like.

I couldn't get through this dissertation without the music that inspired my writing, in the place where I did it all. Beyonce's *Renaissance*, Kendrick Lamar's *Mr. Morale and the Big Steppers*, and the 1975's *Being Funny in a Foreign Language* played on repeat as I wrote about surveillance in healthcare. I spent hours upon hours in a local coffee shop in Greenville, NC called Coastal Fog. I'm waiting for the shop to offer me some shares, or at least a bed in the back. I appreciate my favorite baristas, who always gave me refills of black iced coffee. They knew it was the next best thing to an IV drip of caffeine.

Of course, I can't forget to thank my therapist. Bless that woman. I'll never stop advocating for mental health care, and I'm fortunate and privileged that ECU covered this care for graduate students. I also found my care and outlet through Orangetheory, which I'm sure if you know anything about the studio, you won't be surprised that an article might be forthcoming. I can't thank my 5:30 p.m. crew enough, especially Xavier and Melissa, for their constant dedication, love, and support.

Though I might not be able to list every single influential person and scholar, I do want to note a few support groups. To Elena and Ashley, I'll cherish our Gather nightclub, and weekly writing. The DRPC, especially Gavin and Charles. My CPTSC graduate student committee, Rachael, Emily, Allison, and so many more; my cohortians, Bess and Jason; Hannah, for all the laughs; and sarah, for her inspirational radical activism. Quinn, you've quite literally been here from the beginning (2019); I'm so lucky to see this through with you by my side. I owe so many thanks to my brothers, Cameron and Connor—love you doots, my friends, classmates, colleagues, supervisors/mentors, and organizations who have been a source of continuous love and support. I see you. I appreciate you. And last, but certainly not least. To my mom—I know I've made you proud. Thank you for believing in me, and my dream. What's up, doc?

TABLE OF CONTENTS

LIST OF TABLES x

LIST OF FIGURES xi

CHAPTER 1: INTRODUCTION 1

1.1 Introducing Biometric Identification and the Research Questions 6

1.2 Historical and Definitional Overview 18

1.3 Elaborating on Research Goals: The Exigency 21

1.4 Chapter Summary 23

References 27

CHAPTER 2: LITERATURE REVIEW: SITUATING BIOMETRIC IDENTIFICATION IN TECHNICAL COMMUNICATION AND SURVEILLANCE STUDIES 31

2.1 Defining Surveillance 32

2.2 Defining Technical and Professional Communication 35

2.3 Bridging Surveillance Studies, Technical Communication, and Feminist Rhetoric 40

2.4 Technological Infrastructure, Power, and Data Collection 43

2.5 History of Biometric Identification 46

2.6 Authentication and Privacy 59

2.7 The Digital Cyborg and Layered Literacies 64

2.8 Rhetoric of Health and Medicine: Biometrics are not the End All 72

2.9 Chapter Summary 78

References 80

CHAPTER 3: METHODS AND INTRODUCING INTERLOCKING SURVEILLANCE 90

3.1 Introduction to Methodology: Interlocking Surveillance 90

3.2 Further Situating Feminism in Interlocking Surveillance 96

3.3 Implications of Interlocking Surveillance as a Methodological 98

a. Awareness 100

b. Advocacy 102

c. Transparency 103

3.4 Methods: Corpus Analysis, Questionnaire, and Interviews 106

a. The Challenges with Community-Engagement 110

b. Corpus Analysis 113

c. Defining the Corpus Genre 115

i. Voice Recognition 122

ii. Facial Recognition 124

iii. Fingerprinting 125

c. Questionnaire: I want the Snowball, not the Avalanche 127

c. Interviews 135

3.5 Coding 138

3.6 Chapter Summary 145

References 147

CHAPTER 4: THE TENSION BETWEEN PROFESSIONAL AND PERSONAL, AND THE AGE OF MEASUREMENT 151

4.1 Summary of Interlocking Surveillance 151

4.2 Corpus Analysis 154

4.3 Questionnaire (Screening Surveys) 158

a. Report 1: Accessing Nurses through Social Media 159

a. Report 2: Responses from a Nonprofit 166

4.4 How Compliance, Security, and Efficiency Manifest in the Questionnaire 169

4.5 Compliance and Introducing Biometric Solutions 184

a. Voice Recognition: Something you are, to something you have 188

b. Facial Recognition: Authenticating Your Face 197

c. Fingerprinting: Success is at your fingertips 202

4.6 Security 206

a. Voice Recognition and Security 210

b. Facial Recognition and Security 213

b. Fingerprinting and Security 216

4.7 Efficiency and Convenience 221

a. Voice Recognition: Efficiency and Convenience 223

b. Facial Recognition: Efficiency and Convenience 227

b. Fingerprinting: Efficiency and Convenience 231

4.8 Chapter Summary 236

References 238

CHAPTER 5: CONCLUDING TAKEAWAYS: A MOVE TOWARDS ADVOCACY, AWARENESS, AND TRANSPARENCY 243

5.1 Security, Efficiency, Compliance: Localizing Efforts 244

5.2 Questioning and Revising Norms: Patient Advocacy 249

5.3 Coalitional Work 258

5.4 Usability, Design, and Ethics 265

5.5 Advocacy, Transparency, Awareness: Calling in and Future Research 271

5.6 Chapter Summary 280

References 281

CHAPTER 6: PEDAGOGICAL AND PROGRAMMATIC IMPLEMENTATION 288

6.1 Problem Statement: Introducing Biometrics to TPC 288

6.2 In the Classroom 293

a. Design and Disability Justice as Advocacy for a Socially Just Classroom 295

b. Example Course Overview, Assignments, and Case Study 299
c. Case Study Example 305
6.3 Surveillance Pedagogy: Across TPC Programs 310
6.4 Chapter Summary 313
References 314
APPENDIX A: IRB APPROVAL LETTER 318
APPENDIX B: PATIENT CONSENT PHOTO (Edwards, 2022) 319
APPENDIX C: INTERVIEW SCRIPT 320
APPENDIX D: CONSENT PARAGRAPH AND QUESTIONNAIRE QUESTIONS 322

LIST OF TABLES

1. Table 1: Biometric Solution, Company, and Example Texts Collected 120
2. Table 2: List of Organizations Emailed with Questionnaire 134
3. Table 3: List of Neonatal Nurse Interviewees 137
4. Table 4: Methodological Framework and Coding Language 141
5. Table 5: Methodological Framework and Coding Language 156
6. Table 6: Report 1, Question 4 Themes 161
7. Table 7: Questionnaire Report 1, Question 4 Quotes 162
8. Table 8: Questionnaire Report 2, Question 4 Quotes 168
9. Table 9: Compliance, Security, Efficiency, and Interlocking Surveillance 171
10. Table 10: Nurses Referring to Themes (Q3, Report 1) 173
11. Table 11: Compliance, Nurse Engagement with Biometrics (Q6) 177
12. Table 12: Efficiency, Nurse Engagement with Biometrics (Q6) 179
13. Table 13: Security, Nurse Engagement with Biometrics (Q6) 181

LIST OF FIGURES

1. Figure 1: Biometric Timeline 49
2. Figure 2: uAttend Cloud Software Page 117
3. Figure 3: uAttend Shop, Touch Tablet Time Clock 118
4. Figure 4: Workwell (uAttend) Privacy Policy 119
5. Figure 5: Testimonials (uAttend) 120
6. Figure 6: Interlocking Surveillance Framework Visual 153
7. Figure 7: Report 1, Biometric Usage in Healthcare (Q5) 160
8. Figure 8: Report 2, Biometric Usage in Healthcare (Q5) 167

Chapter 1

Introduction

Time to move your body! Did you grab your nearest wearable device? Perhaps it's an Apple Watch or a Fitbit device, or some other device that tracks your calories, pulse, heart rate, sleep patterns, and so on. Has the device told you to breathe yet? Or even drink more water? Devices such as Apple Watches[1], collect personal bodily identifiers such as pulse, heart rate, oxygen level, and blood pressure. Most recently, these wearables have been poised as a method for COVID-19 detection in the self or environment (Wan, 2020).

My dissertation seeks to introduce a new definition of biometric identification (and related technologies) and addresses the tensions between personal/professional ethics (McKee & Porter, 2009) and obligations. This study contributes to redefining the role of a technical communicator, situated in rhetorics of health and medicine and surveillance studies scholarship. As biometric identification and authentication becomes more commonplace within various sectors such as that of healthcare, it is crucial for technical communicators to return to the origins of biometric implementation to inform current interventions, and to question the reasons behind the urgency of implementing such technologies for efficiency, security, and compliance. Though the site of surveillance is specific to healthcare and explores neonatal nurses' usages and perceptions of biometric technologies, the definition and impacts/consequences are easily transferable across sites of surveillance (such as that of education; borders and travel; and much more). With the current political turmoil in the United States[2] such as with reproductive rights/justice (in the wake of overturning Roe v. Wade) and threats of social media bans such as

[1] Apple Watch tracks metrics like blood oxygen, heart rate, time asleep, respiratory rate, and on Apple Watch Series 8, wrist temperature. The Watch also tracks ovulation (not available in all regions, allegedly), medications, and heart health (AFib) (Apple Watch, 2023).

[2] Currently writing this dissertation in the 2022-2023 academic year.

TikTok, this study is situated at a moment where technical communicators may better equip themselves to intervene in [communication] design and decision-making protocols. This intervention also extends to those technical communicators negotiate and communicate with, such as students. For example, privacy scholars have warned against the use of menstrual applications due to the potential ramifications of applications selling data to third parties, including governmental agencies and law enforcement (Novotny & Hutchinson Campos, 2019). The concerns have become an example of risk vs. convenience. Popular sources such as National Public Radio (NPR) have discussed the lengths to which data privacy has become of utmost importance (Torchinsky, 2022):

> Evan Greer, director of the digital rights advocacy group Fight for the Future, stated that period apps aren't the only ways technology can be used to connect someone to an abortion. If someone is sitting in the waiting room of a clinic that offers abortion services and is playing a game on their phone, that app might be collecting location data, she says.

The concern with data privacy has recently extended to focus on biometric usage in social media, as well. For example, TikTok's CEO Shou Zi Chew explained that the social media application determines the age of its users by scanning videos (Perez, 2023). However, follow-up questions such as what specific facial recognition or other technologies TikTok uses, and whether those technologies were "built in-house" or if the company relies on "facial recognition tech built by third parties," were not asked (Perez, 2023). Further, recent research published in Health Affairs claimed that 98.6% of hospital websites "leverage third-party tracking code that routinely transfers patient data to large technology companies, social media giants, advertising firms, and data brokers" (Davis, 2023). Functionality, whether through web browsing or use of biometric technologies, should not have to come at the cost of privacy. We as educators, scholars, and participants in society must unpack the purpose of implementing biometric technologies, how they are defined, and the ethical implications, such as who they protect and

harm. Healthcare is increasingly difficult to navigate, in addition to the layers of privacy concerns, precarity, understanding highly technical language, and navigating consent. More of "why" neonatal nurses and "why" healthcare as a site of study will be discussed in section 1.3.

One example of biometrics situated in healthcare is from researchers at UC San Diego who have developed a technology (ION) that fingerprints newborns. This technology collects "temperature, pulse, breathing and oxygen, and identifies the infant through their fingerprint" (Carr, 2018). Researchers state that the ION is a non-contact optical scanning technology that can image fingers and the palm of the hand. Now, let's imagine you have been told either technology, the wearable device to detect COVID-19 or the fingerprinting device for the newborn, would be implemented as standardized hospital practice in a month. For those who this directly impacts (such as neonatal nurses or parents), perhaps you might view the implementation as an efficient means of tracking. Maybe you feel more at ease, knowing that you can now quickly detect whether or not you have COVID-19 rather than swab your nostrils. Maybe, like the neonatal nurses interviewed in this study, you'll wonder about how the fingerprinting for newborns would work: newborn fingerprints change quickly and aren't fully developed. These scenarios are discussed in more detail in Chapter 4. With some of the positive aspects of the technology determined by neonatal nurse interviews, it can be difficult to think past the sometimes-invisible implications of such technologies. Often, these shiny, new technologies are poised as a means for additional "safety" or "protection," or even "efficiency." These themes of safety and efficiency will be discussed in further detail in Chapter 4; however, to elaborate on this example, a quick Google search asking "why use biometric authentication" provides a long list of webpages advocating for verification of identity, their convenience, added security measures, and an emphasis on faster authentication (or efficiency). One doesn't need to

look too far to witness numerous examples of biometric usage paraded as secure and efficient in the consumer arena[3]: a study from 2017, for example, suggested that "70 percent of consumers believe that biometrics are easier, and 46 percent think they are more secure than using passwords or PINs[4]" (Visa, 2017). This understanding, of course, extends into many sectors and has additional concerns when applied to the precarious site of healthcare. Even so, questions of concern include:

- who has access to this health data,
- how does this data may impact insurance (including life insurance) policies, and
- what and which bodies are considered the "norm" that the data is "measured" up against?

The problem with the concept of "health" is that it functions as a set of normative standards for how bodyminds are "supposed" to work in order to be productive under capitalism. Introducing new technologies into healthcare can be distilled to efficiency in terms of optimization; or, as mentioned, patients and neonatal nurses being "productive" under capitalism. There are increasingly more and more introductions to biometrics into the consumer arena; however, we must consider the implications of who the technology is identifying, protecting, harming, and how such are implemented, especially in a place as precarious as healthcare[5].

Even more recent in the surveillance and health arena is artificial intelligence (AI) and facial identification (an example of biometric identification). Maybe, like the California-based AI artist Lapine, your image recorded by your doctor was used to train AI data sets (Edwards,

[3] There are predictions documenting different percentages of biometric implementation growth; however, the consensus is the same that the industry is set to expand exponentially in the next 5 years. This will lead to more opportunities for research and preparing students for their careers in this industry.
[4] Research conducted by AYTM Market Research, September 12-19, 2017, among 1,000 U.S. adult consumers who use at least one credit card, debit card, and/or mobile pay (Visa, 2017).
[5] For this study, the focus is on hospitals where neonatal nurses work.

2022). According to Benj Edwards (2022), an AI and Machine Learning Reporter for *Ars Technica*, Large-scale Artificial Intelligence Open Network (LAION) is "a nonprofit organization with members worldwide, 'aiming to make large-scale machine learning models, datasets and related code available to the general public.' Its data can be used in various projects, from facial recognition to computer vision to image synthesis." Edwards (2022) includes a tweet from one "victim" of LAION:

> My face is in the #LAION dataset. In 2013 a doctor photographed my face as part of clinical documentation. He died in 2018 and somehow that image ended up somewhere online and then ended up in the dataset- the image that I signed a consent form for my doctor- not for a dataset.[6]

Aside from the issues (and violation) of consent, such as distribution of personal imagery, in this news story, the article poses questions about responsibility and ethical considerations regarding data privacy and *true* informed consent. Who, if anyone, is "at fault" for distribution of data? What protocols or opt out procedures are implemented if users do not want their information distributed? How can communication more accurately account for all the potential "agreements" the user, or patient, is consenting to? Such an example displays the very real implications and consequences of usage of biometric technologies without proper informed consent, regulation, and accountability measures to protect people.

Within this introduction to my dissertation study, I introduce my definition of biometric technologies including their aim and reference within and outside of rhetoric and composition.[7] I also give current examples of biometric technologies, which further establishes my definition and research trajectory. I pose some questions that help guide this study, as well as general questions for technical communicators to consider at the intersection of surveillance studies and

[6] See Appendix B for consent photo (ironic, isn't it?).

[7] I view technical communication as under the "umbrella" of rhetoric and composition, where technical communication may be defined as negotiating and/or communicating specialized information.

technical communication[8]. The chapter also includes a brief mention of the history of biometric use within the United States (though this will be discussed more in-depth in Chapter 2).

1.1 Introducing Biometric Identification and the Research Questions

For the purpose of this study, I define biometric identification as any identifier of the body that is collected and used for personal identification (and authentication). That is, the data being collected is an example of biometric technologies, whereas the device used to collect biometric information is a tool to collect such data. What is considered "personal" identification has been determined by capitalist societies for over a hundred years; however, the element of collection is integral to my definition. The goal of collecting personal identifiers of the body is to prove or legitimize the self, which are *huge* constructs that will be further referenced and discussed throughout Chapter 2. Collection is often, if not always, used as a means to prove you are who you say you are against the state system's repository (or contracted third-party's repository) of personal identification. My definition builds off a rich history of biometric technologies as established prior to the emergence of the digital era and includes more recent innovations during the digital age. Biometric identification may include, but is not limited to, facial and iris recognition (Gates, 2011), fingerprinting, voice recognition, driver's licenses, and passports. Though considered "identifiable" technologies, mental health and wellness surveillance (Skaik, 2020) and health communication on online platforms (Roundtree, 2017) may not be considered biometrics (there are exceptions[9]). Furthermore, an interviewee from this study[10] mentioned that a computerized tomography (CT) scanner is a popular technology used

[8] Technical and professional communication: communicating and/or negotiating specialized information.
[9] Characteristics (mental health) and subsequent language communication in forums and through health records is and can be identifiable to a specific person but is not a *physical* characteristic that can be taken from the body, thus why such attributes are not biometrics.
[10] Redacted (Interviewee C)

within Neonatal Care, but is it biometrics? Probably not. According to Mayo Clinic, CTs are scans that combine a series of X-ray images taken from different angles around the body and use computer processing to create cross-sectional images (slices) of the bones, blood vessels and soft tissues inside your body. CT scan images provide more-detailed information than plain X-rays do. CTs are collecting identifiers, such as bone imaging (arguably, skeletal biometrics); however, the scans do not collect unique, identifiable information from the body. Since bones are very similar (almost too similar) in adults, an example of a unique identifier or biometric information collected in this instance would be the DNA *from* the bone, rather than the image itself[11].

Such biometric data is collected and accumulated over time in databases, so individuals' personal identifiers are checked through a system(s); this has become a societal "norm." Technical communicators are well-positioned to focus on how "the bodies and behaviors of the inhabitants of these spaces [or sites]—are special areas of experimentation for new surveillance technologies" (Gates, 2011, p. 3). Of course, this is because "contemporary U.S. culture exhibits an intense preoccupation with the combined priorities of security and technology" (Gates, 2011, p. 3). Because the U.S. has such a preoccupation with security and surveillance technologies, such a study can better inform technical communicators how to intervene in and implement decision-making practices (Campbell, 2013). Considering the United States' current social and political climate, it isn't a surprise that healthcare is one of the leading industries for utilizing biometric technologies. Since the preoccupation with technologies is often under the illusion of safety and security, bodily control and surveillance happens more insidiously in a site such as healthcare. For example, Lupton & Michael (2017) write how "post-Snowden[12] several highly

[11] The CT does not contain unique enough data to distinguish individuals.
[12] Edward Snowden is an American former computer intelligence consultant who leaked highly classified information from the National Security Agency in 2013, when he was an employee and subcontractor.

publicized events and scandals have drawn attention to the use of people's personal data by other actors and agencies, both legally and illicitly" (p. 1). Lupton & Michael (2017) noted that the participants in their study recognize the value of both personal data and the big, aggregated data sets that their own data may be part of, particularly for their own convenience. However, participants expressed concern about "how these data may be used by others, often founded on a lack of knowledge about what happens to their data" (Lupton & Michael, 2017, p. 1). Understanding how data is used and what happens to the data gives technical communicators an opportunity to design best practices in the U.S., especially since security, privacy, and surveillance technologies and practices are implemented differently in other countries (see Kerr et al., 2009). The end goal? Determining: *are you who you say you are?*

As technical communicators have argued, technologies are neither neutral nor objective, nor always accurate (see Benjamin, 2019; Noble, 2018). One such technology that is not neutral are biometric technologies, which have been defined and/or referenced in technical communication most often by rhetorics of health and medicine scholars and compositionists who critique objects such as wearable devices, haptic technology[13], and health-related applications and tools (see Tham, 2016, 2017; Walters, 2014; Hansen, 2015; Novotny & Hutchinson Campos, 2019; Stambler, 2022). Isabel Pedersen defines wearable technology as a third medium that "sits midway between media you carry (e.g., laptops, BlackBerrys, memory sticks) and media you become[14] (e.g., devices implanted in the body, future nanotechnological manipulation, prostheses)" (Tham, 2016, p. 4).

[13] Haptic technology: As it relates to haptic vision, fusing the senses (vision and touch) (Hanson, 2015, p. 15), or relating to the perception and manipulation of objects.

[14] A gesture toward posthumanism, undermining the traditional boundaries between the human, the animal, and the technological; and cybernetics, the study of control and communication in machines and animals (see Bolter, 2016; Haraway, 1991; Hayles, 1999).

In my research and teaching, I refer to wearable technologies as the devices and/or tools that carry biometric identification, but the device itself is not biometric. Though wearable devices such as the "media you carry" and "media you become" (though this is not an extensive list) may be considered biometric technologies, biometrics have also been defined in rhetoric and composition, and communication/media studies through their aim. The aim of biometric identification technologies (such as fingerprinting, iris scanning, and voice recognition), according to Gates (2011), is "to bind identity to the body using digital representations of unique body parts, or, in the case of voice printing, by capturing, digitizing, and analyzing the sounds that the body produces" (p. 14). For example, wearable devices/technologies relate to biometric technologies because they are the devices responsible for collecting the biometric information (personal identifiers such as fingerprints, facial and voice recognition, and so on). The wearable technology is merely a tool, rather than an identifier.

According to the long history of biometric technology usage in the United States, biometric identifiers are necessary for federal and state identification. Because there are not currently measures or sanctions in place to regulate the government under ideologies such as (but certainly not limited to) neoliberalism, these state and federal governing bodies are able to collect biometric data without any repercussions for lack of transparency, or mediating visibility of opt-out procedures. Digitizing the body also looks different depending on culture and context. For example, as Haas (2007) writes, "'digital' refers to our fingers, our digits, one of the primary ways (along with our ears and eyes) through which we make sense of the world and with which we write into the world" (p. 84). When we think about biometric identification, fingerprinting is a popular technology to identify or "verify" the person is who they say they are. It's crucial to consider the ways fingers were used prior to the mainstream co-opting of identification for

"security" and "efficiency" purposes. Haas (2007) writes, "American Indians have a long-standing intellectual tradition of multimediated, digital rhetoric theories and practices—or theories and practices of communicating via the encoding of information with our fingers and toes using a variety of media" (p. 94). For example, Haas (2007) references wampum as hypertext, which extends "human memories of inherited knowledges through interconnected, nonlinear designs and associative storage and retrieval methods" (p. 77). Interconnected design extends to hands, too, which have been referenced in terms of being an "embodied instrument" (Haas & McGrath, 2017). As Haas & McGrath (2017) write, "the body (as phenomenologically experienced and embodied) serves as both a metaphoric and functional interface between the mind and the material world" (p. 127). Gates further explains how digitization, or "translating images and other analog texts into binary code," is a technique that is often regarded as a "definitive, accurate, and objective means of binding identity to the body" (2011, p. 14). Regardless, the bodies and minds behind the creation of the systems and technologies for biometric identification claim that by "digitizing visual representations of the body, the body itself will be laid bare and tied directly into information networks" (Gates, 2011, p. 14). Because of this longstanding, and ignored, history of technological influence, perhaps we should consider the "technologies" we use, for what purpose, and their intended (and consequential) impacts on users.

The reference to digital fingerprinting is not just used in determining a unique identifier of the body, but also is becoming an extension of the body through attempts to identify a person's work submitted against a repository. For example, the popular plagiarism detection company Turnitin writes:

> A document submission is converted into what we refer to as a digital fingerprint that our system then uses to search against our content databases using our proprietary algorithm.

> Our system then paints the document with highlights for each section of text that matches a source within our repositories. What our system deems to be the best matches to the sections of text are listed in the report sidebar. Although the best matches are listed there may be hundreds to thousands of other sources that match the document's text. These underlying sources are listed in the Content Tracking mode (iThenticate User, 2022).

This example suggests that what it means to be a "unique identifier of the body," is now being appropriated to refer to any documentation that would or could be used to identify you, your work, and so on. This digital fingerprint may contribute to redefining biometrics in the future; however, I do not consider the documents uploaded to a repository to be a unique identifier of the body.

Your digital fingerprint is now much more than your fingertips. As Haas (2007) reminds us, "All writing is digital—digitalis in Latin, which typically denotes 'of or relating to the fingers or toes' or a 'coding of information'" (p. 84). Browne (2015) writes how biometrics may be understood through their automation, as well. Some examples that Browne (2015) refers to are computer webcams that make use of motion-tracking software or touchless faucets, toilets, and hand dryers that "employ infrared or capacitive sensing to detect a user's presence and gestures" (p. 109). Browne (2015) writes that for biometric automation, it is not for "recognition or verification of a user's identity that the biometric is put to use, but rather for an acknowledgment of the user's presence or an awareness that someone, or at least a part of someone, is there, ideally" (p. 109). This differs from my own definition of biometrics by adding a layer of complexity that suggests biometrics as acknowledgement; however, I do *not* consider automation as biometrics *unless* there are identifiers such as fingerprints or iris scans that are gathered with the intent to identify and authenticate the body. Though devices such as movement trackers collect information, such as steps, distance traveled, calories burned, weight, heart rate, sleep

stages, active minutes, and location[15], the information is not a unique identifier of the body. The devices collect biometric information; to reiterate, though, wearable devices are merely tools, rather than identifiers.

Authentication and privacy will be discussed more in Chapter 2; but for the purposes of defining the parameters of my definition of biometrics, I want to note that biometrics are a *form* of authentication, but are not, as some popular sources report, the *same* as two factor authentication. Biometrics are occasionally part of two-factor authentication—used to confirm your physical body is who they claim to be against a repository or system. Two-factor authentication was initially a form of multi-factor authentication where only a second device was required for "authenticating" or identifying. Two-factor authentication has grown to include biometrics. In fact, Microsoft's Authenticator application claims "You need to confirm your sign-in with biometrics or a passcode" when logging into a Microsoft account. The reason that biometrics are not the *same* as two-factor authentication is because they are solely a *component* of the system. Two-factor authentication requires a combination of *two* of the following: "Something you know (your password); Something you have (such as a text with a code sent to your smartphone or other device, or a smartphone authenticator app); Something you are (biometrics using your fingerprint, face, or retina)" (Simon, 2019). Despite the glaring issue that nearly anyone with your password could "claim" to authenticate your body against the system, this further contributes to our understanding(s) of biometric technology and their role in "legitimizing" the self. What follows are some popular cultural examples to further our understanding and definition(s) of biometrics.

[15] According to Fitbit's Privacy Policy.

As stated, I define and view biometric identification and technologies as unique identifiers of the body used for personal identification (and authentication). One of the most common forms of identification and verification on the retail market and for corporate entities, are facial recognition devices. Because faces are, in theory, an identifier of the body, I consider documents such as passports and driver's licenses biometric identification. And the United States Customs and Border Patrol (CBP) does too. As of September 2022, the CBP's website has boasted how they are "leading the way in creating a more seamless, secure – and safer – travel experience" through increased use of facial recognition (Customs and Border Protection, 2023). This language, "seamless, secure, and safe," are terms I will be discussing further in Chapter 4 to explain how neonatal nurses perceive and use biometric technologies.

What you'll notice reading through the website is that the CBP, like other times during United States history, is implementing the technology during a time of crisis. For example, biometric implementation became more apparent and normalized in discourse post September 11, 2001 (9/11), when biometrics (such as facial recognition) circulated as the solution to prevent "another 9/11." What was once introduced as a safety and security measure has become normalized as a means to surveil and control bodies within the state. In this specific example, biometric technology has been around for decades prior, but the increased presence is due to the COVID-19 pandemic. The CBP states that this technology is "hands-free" and therefore "it helps to prevent the spread of germs. So, it's also a better public health option" (Customs and Border Protection, 2023). While the technology is "hands-free," this is a classic example of biometrics being implemented during times of fear (fear of health/safety from COVID-19), and further, it helps guide my definition of what biometrics *are*. Since facial recognition is used instead of presentation of a passport, and then further compared against an existing passport or visa photo,

this suggests that the CBP believes facial identification is sufficient verification. There are substantial issues with this line of thinking, which are further discussed below and in Chapter 4's analysis of facial recognition solutions; however, the parameters (employed by CBP at present) are helpful for the purposes of defining biometrics.

Interestingly enough, the CBP claims that "All traveler photos of U.S. citizens are deleted, and no photos are ever shared with industry partners" (Customs and Border Protection, 2023). A few thoughts arise here:

- When are the photos deleted ("CBP retains U.S. citizen photos for no more than 12 hours after identity verification, and only for continuity of operations purposes").
- Where are they stored ("Hosted within a secure cloud-based environment").
- And what if you are not a "U.S. citizen"?

What is fascinating is how the CBP frames biometrics as technologies that are *not* for surveillance. *I explicitly label biometrics as surveillance technologies*. Because the CBP associates the term surveillance with "hidden" or "out of sight" they frame the technology as not surveilling. What's interesting is how the CBP mentions that passengers and travelers are "informed about the process and technology" (Customs and Border Protection, 2023). The truth is, the signage in the airports isn't always clear, accessible, nor available. In fact, CBP does offer travelers a "choice" in opting out; but this is in fine print at the bottom of a sign off to the side of the biometric identification line. And for international travelers? CBP agents walk up to you, ask for your boarding pass, and then take a picture. No notification of ability to opt out. CBP mentions that "Surveillance programs, on the other hand, involve cameras that are hidden and out of sight, capturing video of people when they are in public spaces and completely unaware or informed" (Customs and Border Protection, 2023). Biometric identification certainly is prevalent

in public spaces, and the large majority of people are very uninformed as to the extent of the privacy they are swapping in return for "security."

As mentioned, biometric identifiers are positioned as a necessity for federal and state identification and there are not currently measures in place to regulate the government under neoliberalism. According to Welch (2008), neoliberalism is a "reassertion of classical economic liberalism's central tenet that major political and social decisions are best decided by the market" (p. 7). Because of this "free market" idealization, corporate and state forces (including police and military forces) collude "to privatize public resources and services, raise taxes on the poor, cut taxes on wealth and profit, and liberalize capital flows while holding increasingly impoverished and desperate populations in place with tightened immigration and border restrictions" (Welch, 2008, p. 7). Under neoliberalism, anti-poverty and equal opportunity programs have marked the leading edge of services to be defunded. According to Welch (2008), this disinvestment has been assisted by a "reworking and reclassifying of racism, sexism, homophobia, and other forms of discrimination as simply and rightly a private employer's or privatized community's prerogative" (p. 8). In this instance, the government's role is synonymous with the watchtower; that is, "the state serving to protect private property and private privilege from public demands" (Collins, 2003; Welch, 2008, p. 8). The United States' preoccupation with "safety" and "security," alongside their allegiance to protecting their own (private) interests, creates a tension (and barrier) to oversight and regulation of corporations.

A familiar example to most audiences of biometric identification under neoliberalism is ID.me. This following example displays the consequences of a lack of regulation of government entities. ID.me is a website catered towards providing discounts for teachers, students, military personnel, and others. During a controversy in 2022, the United States government gained public

scrutiny from privacy and surveillance activists such as the Algorithmic Justice League, for the government's intent to use ID.me for tax-related verification. Some of the problems include, but certainly are not limited to, how ID.me poses a larger issue for people of color; like many other aspects of biometric identification, other oppressed groups will be affected as well. Since facial recognition devices have been found to be racist (Grother et al., 2019), the government's insistence on using facial recognition to confirm identities for tax purposes is not only discriminatory, but also sets the expectation that many Black and people of color will not be able to access tax documents, further subjecting them to potential (violent) repercussions. The process to sign-up for ID.me also poses a problem for transgender and gender-nonconforming people because it requires users to match an image from a government-issued ID to a selfie. Not everyone has access to a driver's license or passport with photos that reflect their current gender presentation (Buolamwini, 2022). Nor does everyone have a birth certificate that reflects their accurate personal identifiers (Moore & Currah, 2015). According to Sullivan (2022), ID.me stated that they are also used by the Department of Veterans Affairs and the Social Security Administration, as well as several other federal agencies. It's important to consider: How will facial identification impact Veterans, those receiving social security, and so on? Technical communicators are advocates (Jones, 2016), which means in order to advocate and intervene in biometric communication and design, technical communicators need to reflect upon prior implications and consequences of federal agencies using biometric identification for services. This reflection helps to situate understandings of the patterns and problems associated with biometrics to assist in addressing the current issues with biometric identification today, such as the returning to the historical implementation in the United States, for example, with surveilling welfare recipients (such as EBT/SNAP) that began in the 1990s.

These examples will be discussed further in this dissertation in Chapter 2, documenting some of the history of biometrics. Many of the examples of biometric identification listed have been normalized by our society within the United States. Justification from governing bodies of such identification practices have been for "security," and are often regarded as "necessary" for "privacy." To address such justifications, Lyon (2007) mentions that despite the ubiquity of surveillance technologies, it is important to study specific "sites of surveillance" in order to understand their nuances (p. 25). For the purpose of this dissertation, I am specifically focusing on the "site" of the United States healthcare system, with a specific focus on where neonatal nurses work (hospitals, private practices, and so forth); though in understanding the workplace as a professional context, it is necessary to also unpack the history of biometric use prior to its commercialization in the workplace.

This study therefore contributes to the field of technical communication by exploring the following *general* research questions:

- How may technical communicators intervene in decision-making and advocacy work in relation to biometric technology implementation in healthcare?
- How do technical communicators[16] communicate complex language (like HIPAA, though it currently doesn't apply to digital tech) so that patients are aware of their rights?
- How can protocols and procedures apply to digital applications, technologies, and platforms?

This leads to my specific research question, which asks:

[16] I view technical communication as under the "umbrella" of rhetoric and composition, where technical communication may be defined as negotiating and/or communicating specialized information.

- What are neonatal nurses[17]' usages and perceptions of biometric technology in healthcare?

This research "answer" is determined through analyzing the connection (or tension) between neonatal nurses' perceptions and usage of biometric technology in healthcare, and the communication materials developed by biometric solution companies. To answer my research question, this study engages in three steps: first, I compiled a corpus of information directly from biometric technology company websites; then, I distributed a screening questionnaire through Twitter and through the Association of Women's Health, Obstetric, and Neonatal Nurses which asked neonatal nurses in the United States about their roles, and usage/perceptions of biometric technologies; lastly, I chose 10 participants from the screening questionnaire to be interviewed. This process will be further explored in my "Methods" section in Chapter 3.

1.2 Historical and Definitional Overview

My main focus of this study is the United States, though it would be a mistake to view biometric technologies as unique to the U.S. As Gates (2011) writes in relation to facial recognition technology, a biometric identifier, "research and development has occurred in other countries as well, and the technologies are finding applications beyond U.S. borders" (p. 3). Throughout history, biometric technologies have gathered data and/or been implemented for research purposes anywhere from airports, to borders, cities, and homes; sites of surveillance exist all around us. In fact, biometrics have been utilized in many different sites, including but not limited to:

> law enforcement and public security (criminal/suspect identification), the United States military (enemy/ally identification), Border, travel, and migration control (traveler/migrant/passenger identification), Civil identification (citizen/resident/voter

[17] Though neonatal nurses generally care for newborns, they communicate most with patients to discuss parent/infant rights and procedures.

> identification), Healthcare and subsidies (patient/beneficiary/healthcare professional identification), Physical and logical access (owner/user/employee/ contractor/partner identification), and Commercial applications (consumer/customer identification) (Thales Group, 2022).

Further contributing to the definition of biometric technologies and their subsequent impacts, Shoshana Amielle Magnet refers to bodies that are rendered biometric as a particular kind of capital (2011, p. 5). Magnet cites a specific example where "biometric maps of the body help to spin the bodies of prisoners, welfare recipients, and travelers into valuable data" (2011, p. 5). As Johnson et al. (2015) note, "the physical body carries meaning through discourse about or by a body." Embodiment theories, however, suggest that meaning can be "articulated beyond language…by recognizing the inherent relationship between embodiment and rhetoric, we can make all bodies and the power dynamics invested in their (in)visibility visible" (Johnson et al., 2015, p. 39). Surveillance and thus biometrics may be understood as an assemblage (Haggerty & Ericson, 2000) and fluid; that is, surveillance relies on both the physical presence of the body and its experiences both visible and not. One way to think about biometric maps of the body may be through Haggerty and Ericson's (2000) concept of surveillance assemblages, or data collection over time. Surveillance assemblages operate by "abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention" (Haggerty & Ericson, 2000, p. 605). Haggerty and Ericson (2000) note that during this process of reassembling, there is a "rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored" (p. 606). As Magnet argues, biometric representations of the body are able to "produce new forms of identity, including unbiometrifiable bodies that cannot be recognized by these new identification technologies, a subject identity that has profound implications for individuals'

ability to work, to collect benefits, and to travel across borders" (2011, p. 5). It is important to clarify that the surveillance assemblage does not approach the body in the first instance as a single entity to be molded, punished, or controlled; though ultimately biometric technologies can and are used for surveillant control. In fact, Haggerty and Ericson (2000) cite a study by Norris and Armstrong (1999) of British CCTV which demonstrates how the "unitary technology is actually an assemblage that aligns cameras, computers, people and telecommunications in order to survey the public streets" (p. 614). To bridge this study to a potential current implication of such assemblages, one example could be the triangulation of information with cell towers. Cell phones and other mobile devices are often used to "find" or contact a person. This triangulation of information, from cameras, to towers, public streets, people, and more, could lead to identifying the physical location of the body. Thus, all data collected within this negotiation of information may be considered a personal identifier, which of course has further implications about how such identifiers may not accurately identify the "correct" body.

As I mentioned, for the purpose of this study, I define biometric technologies as any identifier of the body that is collected and used for personal identification (and authentication). Biometric technologies may be viewed as a surveillant assemblage, a means to map the physical body and the in/visible experiences that accompany the body. Due to recent shifts in biometric identification and authentication, scholars and instructors in technical communication must call attention to and advocate for biometric corporations to focus on technological ethics including describing how data and information are collected, who has a right to privacy and why, and communication exchanges between company materials and the consumer. In the following section, I document my intended research goals and questions that are guiding this study. I will then shift to Chapter 2, where I dive deeper into the literature from the subfields that support my

dissertation research, including surveillance studies, technical communication, and the rhetoric of health and medicine.

1.3 Elaborating on Research Goals: The Exigency

Technical communicators are knowledge makers and designers of technologies; therefore, they are well-positioned to influence how biometric technologies are utilized within the workplace. In this study, I examine our growing surveillance society by analyzing a specific group of people, neonatal nurses, who work in healthcare (broadly defined). This specific group is important to study because of the added layer of precarity and tension when children are introduced to privacy concerns. For example, attitudes surrounding privacy tend to shift once children, especially infants, are involved. Many of the acts introduced by legislation, such as the Child Internet Protection Act/Children's Online Privacy Protection Act are introduced to "protect" *our* children. Oftentimes this concern with privacy does not extend to adults. Further, such acts are introduced because of the heteronormative values in the United States surrounding reproduction, also referred to as reproductive futurism (Edelman, 2004). Focusing on neonatal nurses in the United States provides an added layer of complexity: how do nurses in their role understand their relationship with privacy, and how does this discussion extend to their patients (and infants)? Neonatal nurses occupy and function in a particularly tense role, where healthcare concerns and protocols intertwine with responsibility for patients (infants) who cannot speak or make decisions for themselves. Ironically, despite the increase in privacy protection for children, parents and healthcare systems continue to opt into usage of surveillance technologies such as biometrics because they are perceived to be "safe." What would healthcare look like as a site of surveillance, if patients and nurses alike viewed biometrics as part of the "harm to minors" argument (Heins, 2007)? Because healthcare is the leading user of biometric technologies, this is

a fitting "professional workplace" and "site" of surveillance to study. And further, understanding the complexities of the usage of these technologies between neonatal nurse, parent, and infant, contributes to suggestions that technical communicators and surveillance activists alike may advocate for transparency and privacy protection. In 2019, research from Gartner Inc. projected that 40% of healthcare institutions will use biometrics by 2022 (Gormley, 2019). And well, it's past 2022[18].

To study this specific site of surveillance, I crafted the study to incorporate a corpus of documents focusing on the communication materials of specific biometric technologies, neonatal nurse understandings of such technologies, and subsequent interviews to receive a holistic view of the role the technologies play (or could play through given scenarios) in the day-to-day of neonatal nurses. Identity verification systems were designed with privileged users in mind. Other than the issues with privacy and the inability to opt out (or perceived inability), there are design flaws. Ultimately, the many surveillance systems (through biometrics) are designed toward capturing fraud rather than delivering benefits to those in need. How can we create more transparent documents and technologies? What perspectives are valued in the design process, who are the key players, and what is considered "legitimate"?

For the purpose of this study, the collected documents for the corpus are not all of the same genre, but instead are carefully selected based on their purposes. My corpus analysis of biometric corporations' data collection/distribution statements contributes to my focus on how the biometric corporations refer to and communicate about biometric identification and corresponding technologies to consumers. The corpus of communication materials is used to analyze the language used by biometric corporations to communicate to consumers, such as

[18] This study was conducted and written throughout 2022-2023.

healthcare institutions. For example, data collection and distribution are/may be located in the Terms of Service, or it may be advertised on the company homepage. Corpus materials were screen captured, compiled in a folder, and further organized into a Microsoft Word document with the date of capture and contents. The methods and means through which I analyzed the collected corpus is based on my methodological framework, interlocking surveillance, which is discussed in Chapter 3. Recent biometric identification features are positioned as a necessity and for effectiveness, but who is asking for such? What is the apparent need? For safety? From whom? Employees, such as neonatal nurses, often must make a choice between being employed or violating their privacy; just as patients often must make a choice between receiving care or violating their privacy. What does privacy or personal information mean to neonatal nurses utilizing biometric technologies for authentication?

1.4 Chapter Summary

All people have both in/visible identities (Beck, 2015) and it is our role as technical communicators to engage in ways to inform not only ourselves of the digital and physical ways we are monitored, but also those we encounter. Our goal as decision-makers is to empower ourselves and users to be well-informed citizens. Users are defined as an individual or the local community (Agboka, 2013). We navigate our day-to-day lives as consumers and users. This study more *broadly* contributes to questions technical and professional communication as a field should consider: How, as digital users and technical communicators, does surveillance impact professional contexts? What are the implications of surveillance, in particular biometric technologies, for historically excluded groups such as those who are marginalized due to race, class, gender, sexuality, and dis/ability in the workplace? These questions help to guide my thinking in this dissertation, and further contribute to my research trajectory, which asks:

- How may technical communicators intervene in decision-making and advocacy work in relation to biometric technology implementation in healthcare?

To answer this broader question, I am focusing on the following more specific research questions:

- How do neonatal nurses define biometric technologies? What are neonatal nurses' perceptions of biometric technologies? What is the connection (or tension) between neonatal nurses' perceptions and usage of biometric technology in healthcare, and the communication materials developed by biometric solution companies?

In the following Chapter, I explore the literature from the subfields that support my dissertation research, including surveillance studies, technical communication, and the rhetoric of health and medicine.

Chapter 1 introduces the history of biometric identification and subsequent technologies in the United States. This definitional backgrounding creates a foundation for the subsequent chapters and study to further contribute to the field of technical communication's understanding of biometrics. This chapter also introduces the research goals including research questions and a brief outline of the study.

Chapter 2 focuses on the literature that supports the study, assisting in understanding how surveillance, in particular, biometric technologies impact people disproportionately. This includes surveillance studies broadly defined, technical communication, and the rhetoric of health and medicine. Through my review of the literature, I define surveillance in relation to technical and professional communication in order to bridge the two fields through feminist rhetoric. This move allows me to chart the history of biometric technologies, explore

authentication (and identification), highlight ethical implications and privacy practices, and connect that work to rhetorics of health and medicine.

Chapter 3 explores the methods and methodologies underlying the study. The chapter is organized by first introducing my methods, which includes documentation of a questionnaire, interviews, and a corpus analysis. The chapter also includes my methodological framework, interlocking surveillance, which is situated at the intersection of surveillance studies and feminist rhetoric. The framework combines elements of new surveillance and intersectionality to develop a heuristic that addresses sites of surveillance and their levels of awareness, advocacy, and transparency of normalized surveillant practices.

Chapter 4 applies my theory of interlocking surveillance to the data collected based on a multiple-methods approach (questionnaire, interviews, corpus), and provides some insights for technical communicators. My analysis identifies themes and trends (security, efficiency, compliance) that link the initial communication of biometrics to consumers and institutions, to those who use the technology in healthcare (neonatal nurses), and individual accounts (those interviewed). The chapter is organized by summarizing interlocking surveillance, overviewing the corpus and questionnaire, discussion of how the emerging themes of compliance, security, and efficiency manifested in the questionnaire, and then a section bridging the themes to further explore how the interviews with nurses connect to the corpus.

Chapter 5 outlines future research trajectories and concluding thoughts. The chapter argues that neonatal nurses can (and do) have a role in the design of communication materials, particularly with patient choice in opting in/out. The chapter discusses implications of security, efficiency, and compliance in healthcare and how technical communicators may intervene. The chapter is organized by several takeaways for technical communicators to consider such as

coalitional work, questioning and revising normalized surveillance including ethics of biometric use, and further localization of community input with impacts to privacy and design including opting out procedures.

Chapter 6 describes pedagogical and programmatic impacts of this study for technical communication classes and programs. This study has implications for exploring digital literacy and ethical implications of emerging technologies. Such topics such as digital literacy, including privacy and surveillance, are relevant and applicable to all courses. The pedagogical and programmatic impact of this dissertation study guides technical communicators in implementing concepts, ideas, and themes (such as privacy, surveillance, efficiency, security, and compliance) into the technical communication classroom.

REFERENCES

Agboka, G.Y. (2013). Participatory localization: A social justice approach to navigating unenfranchised/disenfranchised cultural sites. *Technical Communication Quarterly, 22*(1), 28-49.

Apple. (2023). Apple watch user guide. Accessed April 6, 2023, https://support.apple.com/guide/watch/track-important-health-information-apple-apdc2bf82d90/watchos#:~:text=While%20you%20sleep%2C%20Apple%20Watch,Watch%20Series%208%2C%20wrist%20temperature.

Beck, E.N. (2015). The invisible digital identity: Assemblages in digital networks. *Computers and Composition, 35*, 125-140.

Beck, E., & Hutchinson Campos, L. (Eds). (2021). *Privacy matters: Conversations about surveillance within and beyond the classroom*. Utah State University Press.

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new jim code.* Cambridge, UK; MA: Polity Press.

Bolter, J.D. (2016). Posthumanism. *The International Encyclopedia of Communication Theory and Philosophy.* https://doi.org/10.1002/9781118766804.wbiect220

Buolamwini, J. (2022, January 27). The IRS should stop using facial recognition. *The Atlantic.* https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386/

Campbell, B. (2013, November 1). Ten talking points the NSA uses to justify its spying. *The World*. http://www.pri.org/stories/2013-11-01/ten-talking-points-nsa-uses-justify-its-spying

Carr, J. (2018, September 12). Researchers develop biometric tool for newborn fingerprinting. *UC San Diego Health.* https://health.ucsd.edu/news/releases/Pages/2018-09-12-researchers-develop-biometric-tool-for-newborn-fingerprinting.aspx

Customs and Border Protection (CBP). (n.d.). Introducing biometric facial comparison. *United States Customs and Border Protection*. Accessed January 15, 2023, https://biometrics.cbp.gov/

Collins, C. (2003). Shrink, shift, and shaft. www.tompaine.com/Archive/scontent/8608.html[19]

Davis, J. (2023, April 23). Most hospital websites routinely transfer patient data via tracking tools. *SC Media: A Cyber Risk Alliance Resource.* https://www.scmagazine.com/analysis/privacy/most-hospital-websites-routinely-transfer-patient-data-via-tracking-tools

[19] Link was inaccessible from Welch's (2008) citation. Potential citation url: https://sojo.net/magazine/april-2004/shrink-shift-shaft

Edelman, L. (2004). *No future: Queer theory and the death drive.* Duke University Press.

Edwards, B. (2022, September 21). Artist finds private medical record photos in popular AI training data set. *Ars Technica*. https://arstechnica.com/information-technology/2022/09/artist-finds-private-medical-record-photos-in-popular-ai-training-data-set/

Epstein, J., Donnan, S., & Bass, D. (2022, January 28). Treasury weighing alternatives to ID.me over privacy concerns. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-01-28/treasury-weighing-id-me-alternatives-over-privacy-concerns

Fitbit. (2023). Legal: Privacy Policy. Accessed April 6, 2023, https://www.fitbit.com/global/us/legal/privacy-summary#:~:text=When%20you%20use%20a%20Fitbit,%2C%20active%20minutes%2C%20and%20location.

Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Gormley, B. (2019, February 6). Hospitals turn to biometrics to identify patients. *The Wall Street Journal.* https://www.wsj.com/articles/hospitals-turn-to-biometrics-to-identify-patients-11549508640

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *NISTIR.* https://doi.org/10.6028/NIST.IR.8280

Haas, A.M. (2007). Wampum as hypertext: An american indian intellectual tradition of multimedia theory and practice. *Studies in American Indian Literatures 19*(4), 77-100. https://doi.org/10.1353/ail.2008.0005.

Haas, C., & McGrath, M. (2017). Embodiment and literacy in a digital age: The case of handwriting. In K.A. Mills, A. Stornaiuolo, A. Smith, & J. Zacher Pandya (Eds.), *Handbook of Writing, Literacies, and Education in Digital Cultures* (1st ed.) (pp.125-135). Routledge.

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605-622. https://doi.org/10.1080/00071310020015280

Haraway, D. (1991). *Simians, cyborgs, and women: The reinvention of nature*. New York, NY: Routledge.

Hayles, N.K. (1999). *How we became posthuman*. Chicago, IL: Chicago University Press

Heins, M. (2007). *Not in front of the children: 'Indecency,' censorship, and the innocence of youth*. Rutgers University Press.

Kerr, I., Lucock, C., & Steeves, V. (2009). *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. Oxford: Oxford University Press.

Ketch. (2022). The person behind the data. *Ketch*. https://content.ketch.com/consumer-privacy-perspectives-study

Lupton, D., & Michael, M. (2017). Depends on who's got the data: Public understandings of personal digital surveillance. *Surveillance & Society, 15*(2), 254-268. https://doi.org/10.24908/ss.v15i2.6332

Lyon, D. (2007). *Surveillance studies: An overview*. Malden, MA: Polity Press.

Magnet, S. (2011). *When biometrics fail: Gender, race, and the technology of identity.* Duke University Press.

Mayo Clinic. (2022). CT Scan. Retrieved from https://www.mayoclinic.org/tests-procedures/ct-scan/about/pac-20393675#:~:text=A%20computerized%20tomography%20(CT)%20scan,than%20plain%20X%2Drays%20do.

McKee, H.A., & Porter, J.E. (2009). *The ethics of internet research: A rhetorical, case-based process.* Peter Lang, New York.

Moore, L.J., & Currah, P. (2015). Legally sexed, birth certificates and transgender citizens. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 58-79). Durham and London: Duke University Press.

Noble, S.U. (2018). *Algorithms of Oppression*. New York: New York University Press.

Novotny, M., & Hutchinson, L. (2019). Data our bodies tell: towards critical feminist action in fertility and period tracking applications. *Technical Communication Quarterly, 28*(4), 332-360, https://doi.org/10.1080/10572252.2019.1607907

Perez, S. (2023, March 23). TikTok CEO says company scans public videos to determine users' ages. *TechCrunch*. https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/

Reilly, C. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition, 61*. https://doi.org/10.1016/j.compcom.2021.102652

Roundtree, A. (2017). Social health content and activity on facebook: A survey study. *Journal of Technical Writing and Communication, 47*(3), 300–329.

Simon, M. (2019, April 10). Two-factor authentication explained: How to choose the right level of security for every account. *PCWorld.* https://www.pcworld.com/article/403535/two-factor-authentication-faq-sms-authenticator-security-key-icloud.html

Skaik, R., & Inkpen, D. (2020). Using social media for mental health surveillance: A review. *ACM Computing Surveys (CSUR), 53*(6), 1-31.

Stambler, D.M. (2022). Eat well to work well: Oppression, risk, power, and the rhetorics of employee wellness. Retrieved from the University of Minnesota Digital Conservancy, https://hdl.handle.net/11299/241317.

Sullivan, M. (2022, January 21). IRS login makes you take a selfie for this security company you've never heard of. *FastCompany*. https://www.fastcompany.com/90714538/irs-login-makes-you-take-a-selfie-for-this-security-company-youve-never-heard-of

Tham, J. (2016). Globally fit: Attending to international users and advancing a sociotechnological design agenda for wearable technologies. *Proceedings of the 34th ACM International Conference the Design of Communication.* http://dl.acm.org/citation.cfm?id=2987599

Tham, J. (2017). Wearable writing: Enriching student peer review with point-of-view video feedback using Google Glass. *Journal of Technical Writing and Communication, 47*(1), 22-55.

Thales Group. (2022, January 27). Biometrics: definition, use cases, latest news. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Torchinsky, R. (2022, June 24). How period tracking apps and data privacy fit into a post-Roe v. Wade climate. *NPR*. https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

Turnitin. (2022). iThenticate user report FAQ. Retrieved January 2023 https://help.turnitin.com/ithenticate/ithenticate-user/the-similarity-report/report-faq.htm

Visa. (2017). Consumers ready to switch from passwords to biometrics, study shows. Accessed March 26, 2023, https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html

Walters, S. (2014). *Rhetorical touch: Disability, identification, haptics*. University of South Carolina Press. https://doi.org/10.2307/j.ctv6wgmmq

Wan, C. (2020, May 27). How smart fitness trackers can help detect covid-19. *Ambiq*. https://ambiq.com/how-smart-fitness-trackers-can-help-detect-covid-19/

Welch, N. (2008). *Living room: Teaching public writing in a privatized world.* Portsmouth: Boyton-Cook.

Youngblood, S.A. (2012). Balancing the rhetorical tension between right-to-know and security in risk communication: Ambiguity and avoidance. *Journal of Business and Technical Communication, 26*(1), 33-62.

Zuboff, S. (2019). *Age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

Chapter 2

Literature Review: Situating Biometric Identification in Technical Communication and Surveillance Studies

In the previous chapter (Chapter 1), I introduced a study that illustrates my definition of biometric technologies including their aim and reference within and outside of rhetoric and composition.[20] In Chapter 1, I give a few current examples of biometric technologies, which further establishes my definition and research trajectory. For example, I refer to biometrics as personal identifiers of the body; examples of identification systems include facial recognition, fingerprinting, iris scanning, voice recognition, and more. I also posed some questions that help guide my future research within the intersections of surveillance studies and technical communication, including a brief mention of the definitional history of biometric use within the United States.

In this chapter, I argue that biometric technologies are a form of surveillance that technical communicators can take care to intervene in. Through my review of the literature, I define surveillance in relation to technical and professional communication in order to bridge the two fields through a feminist rhetoric. This move allows me to chart the history of biometric technologies, explore authentication (and identification), highlight ethical implications and privacy practices, and connect that work to rhetorics of health and medicine. This chapter builds off the previous by providing grounding, history, and context for the exigency of my study. This literature review assists in understanding how biometric technologies impact people

[20] I view technical communication as under the "umbrella" of rhetoric and composition, where technical communication may be defined as negotiating and/or communicating specialized information.

disproportionately, and further grounds this study by providing context and situating scholarship in the intersecting fields.

2.1 Defining Surveillance

As I will discuss in the following sections, there are many definitions of surveillance from which my definition builds on. Clarke (1988) defines surveillance as the "systematic investigation or monitoring of the actions or communications of one or more persons. Its primary purpose is generally to collect information about them, their activities, or their associates" (p. 499). Rule uses the term for "any form of systematic attention to whether rules are obeyed, to who obeys and who does not, and how those who deviate can be located and sanctioned" (Clarke, 1988, p. 499). David Lyon (2007) defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction. Surveillance directs its attention in the end to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture)" (Smith, 2015, p. 22). These definitions provide a thorough overview of how surveillance studies refers to and defines "surveillance." I define surveillance as the collection of both visible and invisible data/information derived from those being observed, suggesting an application of power over the observed audience, who are often not informed of such collection. In the following section, I will further discuss the scholars who are informing my definition of surveillance and why (in)visibility is a crucial component to my understanding and contribution of/to surveillance.

As noted, there are various implications of my definition of surveillance; however, it is important to note that this definition focuses on power relations and ways of seeing that are both apparent, and not. One implication of defining surveillance as the "application of power over the

observed audience" may be viewed through what Andrejevic refers to as "mass culture," which, "like the mass market that produces it, has long been criticized for being top down, homogeneous, and non-participatory" (2007, p. 28). The term "top-down" is important to emphasize because of the connotations of power/dominance over (which could refer to both living/non-living actors). My definition of surveillance involves different types of surveillance enacted in our society: it isn't just a top-down panoptic approach, but also counterveillance (or sousveillance), and lateral surveillance are ways of unpacking the systems that we participate in our daily lives. Mann, Nolan, & Wellman (2003) coined the term "sousveillance," from the French words "sous" (below) and "veiller" (to watch) (Beck, 2015, p. 137). Sousveillance may be referred to as the opposite of Panopticism, where Panopticism as developed by Jeremy Bentham refers to the prison architecture: "invisible to prison inmates, the inspector in the watchtower had the capacity to see into any cell at any given time" (Nemorin, 2017, p. 242). As Foucault theorizes, this surveillance leads to disciplinary power and behavioral regulation (Hoffman, 2014). Sousveillance is "us watching the watchers," where invisible digital identities "start to become visible" (Beck, 2015, p. 137). Lateral surveillance (Andrejevic, 2007; Gates, 2011, p. 147) focuses on peer-to-peer monitoring; however, as Andrejevic notes "if everyone is a potential suspect, surveillance must become ubiquitous and comprehensive, and thus distributed" (2007, p. 43). I include this specific quote because it demonstrates researchers' role to question the need to turn people into both a suspect and a watcher. Further, my definition seeks to bring awareness to how the United States has been slowly turning into a hyper-suspicious assemblage based on the assumed necessity of safety and security, often introduced by state powers through times of trauma or fear.

Society turning into a hyper-suspicious surveillant assemblage (Haggerty & Ericson, 2000) contributes to my understanding of surveillance through applications of control and power. William Bogard coined the idea of "the imaginary of surveillant control," arguing that it is not crucial to know "what surveillance is and does" but rather "how the image of totalizing surveillance itself informs the logic of system development and functions as a form of social control" (Gates, 2011, p. 6). I see this statement as informing my definition of surveillance: in fact, I argue that it is *also* important to know the intricacies of how surveillance functions in our society to understand whose interests are being served, what information/data is being collected, how (visibly/invisibly), to what end, and how the power of surveillance forwards the aims of creating ubiquitous surveillance systems. Most notable new examples of surveillance systems are "smart surveillance," which Gates (2011) defines as "monitoring systems that perform the labor of surveillance with less human input and less need to rely on the perceptual capacities and analytical skills of human beings" (p. 3). Smart surveillance has the potential to create new divisions of perceptual labor between humans and computers, as exemplified through the Internet of Things (IOT) items (Ring doorbell, smoke detectors, thermostats, Alexa, Google Home, refrigerators, etc).

My definition of surveillance also focuses on public, and stakeholder, levels of informed-ness, which is often complicated by those who are gatekeepers of such knowledge. There are colonialist implications to the history of the definition of surveillance, and the connotations of surveillance are largely nefarious, complicated by the ways in which surveillance is poised as a "necessity" for "security" and "safety" (Kerr et al., 2009). Surveillance is, as Lyon (2007) writes, "systematic or deliberate and depends on certain protocols and techniques. Beyond this, surveillance is routine; it occurs as a 'normal' part of everyday life in all societies" (Smith, 2015,

p. 22). Surveillance often occurs through biometric use, though this is not the only form of monitoring and control. A social theory of surveillance centers those who are not just surveilled by the state and domineering institutions, but also those who laterally surveil. The public response is often to dismiss issues of surveillance, security, and privacy; however, my end goal is to inform users and push for policy to be implemented as a form of sousveillance (or counterveillance as Welch, 2008 notes). Who is responsible for being informed of surveillance practices? How do people become more empowered citizens?

Clarke (1988) defines personal surveillance as the surveillance of an identified person and argues that a specific reason exists for the investigation or monitoring. This understanding of personal surveillance assists in defining mass surveillance, which is the surveillance of groups of people, usually large groups. Clarke (1988) writes that the reason for investigation or monitoring is to identify individuals who belong to some "particular class of interest to the surveillance organization" (p. 499). This is an example of mass surveillance occurring through biometric identification: identifying large groups of people through technologies in order to categorize. Clarke (1988) furthers our understanding of biometric identification through dataveillance, which is the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (p. 499). In general, mass dataveillance tends to subvert "individualism" and the "meaningfulness of human decisions and actions" and asserts the "primacy of the state" (Clarke, 1988, p. 503).

2.2 Defining Technical and Professional Communication

Central to my definition of technical and professional communication is how I build directly from Frost and Eble (2015) where they coin the term "technical rhetorics," referring to the rhetorical assemblages that convey specialized information to a specific audience in a

persuasive way (p. 2). This informs my thinking of technical communication because of the way Frost and Eble (2015) define technical, as "specialized," and further cite Haas (2018) as referring to technical from the Greek term "techne" or the art of knowing (p. 2). Technical rhetorics includes Haas' (2012) definition of rhetoric as "a negotiation of cultural information and its political, social, economic, historical, etc. influences on social action" (p. 287). I define technical and professional communication as communicating and/or negotiating specialized information.

Because rhetoric is cultural, but not all rhetoric is cultural rhetoric, I see the role of the technical communicator as always already cultural (Haas, 2018; Blake, Longo, & Wills, 2006). Blake, Longo, & Wills (2006) explore technical communication as needing to include cultural knowledge and/or studies. Cultural rhetoric, to me, also focuses on specific aspects of intersectionality. Intersectionality, coined by Crenshaw (1989), was enacted as a response to the feminist movement because of the lack of Black representation in the very white feminist movement (generally speaking, this will be discussed more in Chapter 3). Intersectionality focuses on both the visible and invisible identities that are subject to social injustices and often violence. Cultural rhetoric's emphasis on exploration of communities relates to issues of power, access, and language because of the ways that we make meaning. For example, Overman Smith (2000) discusses how two ideas, rhetoric of communities and document design, are what "legitimize" the field of technical communication (p. 438). Even so, if we were to base our legitimacy on those two specific ideas, then what we need to focus on is where/how technologies (digital and not) contribute to knowledge legitimization; as stated, technologies are not neutral nor objective entities. In fact, Overman Smith (2000) references scholarship that discusses technologies as being an extension of human displays of the production of material goods and services. Because there are people behind the technology, and if we view technologies as

extensions of people, then they too are always already cultural and embedded with language structures that imbue specific meaning. Further, technical communication scholars reinforce conversations that technology use can become a tool that is complicit in racial discrimination; or, in other words, technologies are not neutral and are shaped by the ideologies that are embedded into their design (Haas, 2012; Benjamin, 2019; Jones, 2016a; Katz, 1992; Walton, 2016; Winner, 1980). In its most distilled version, technologies are referred to as extensions of people because *people* (and everything that makes them, them) are creating the technologies. Technical communicators have referred to the notion that technologies are value-laden with ideologies in their design through examples such as, but *certainly* not limited to, the connection between the digital divide and race (Banks, 2006); changes to policies that impact vulnerable populations (Rose, 2016); perceptions of diversity in technical communication courses (Savage & Mattson, 2011); and data discrimination through search engine results and algorithms (Noble, 2018).

Miller (1979) advocates for the role of technical communicators to be humanistic. Miller (1979) marks one of the first articles to emphasize technical communicators as involved in the knowledge-making and design process, rather than as an end point or part of the production end. That is, power is especially central to the history of the field, not just the role of technical communicators now and moving forward. Power may be exerted throughout the knowledge making process through the influence that technical communicators have in ensuring that those within the process are heard, but mostly those who are affected are privileged. This attention to power is what Frost and Eble (2015) advocate for in asking technical communicators to "resist, subvert, and intervene" (p. 6). I also see these calls as defining attributes to the role of a technical communicator and how they may wield the power the field has sought to legitimize for decades. The edited collection by Kynell-Hunt & Savage (2004) overviews ways to reimagine legitimacy,

especially in technical and professional communication. For example, legitimacy can be obtained through empowerment–that is, groups coming together to "advocate, relate, and/or interrupt" (Ryan et al., 2016) dominant ideologies to create change. This is different from what societal expectations are, which is that legitimacy would occur through relation to dominant societal and systemic values of approval.

Individually technical communicators must unpack our own roles and how we ethically engage in the creation and dissemination of information. This is especially important when addressing issues with biometric identification and unpacking the cultural and social implications of authentication systems. Katz (1992) helps us to define the role of a technical communicator in how we consider means to ends–that is, do we involve ethics in our teachings and productions of knowledge? I see a direct relation to ideas of efficiency, which Frost (2018) discusses, where efficiency is not what technical communicators usually think it is by centering time and speed/accuracy, but more importantly centering the needs of people. People or users are often viewed as objects or numbers to be mined rather than bodies especially in the context of technological use (Frost, 2018); and to be efficient, technical communicators must center and privilege user experience and knowledge as designers in the product/agreement/problem rather than as receivers of whatever the end goal is. This example argues for access as being important to efficiency–if technical communicators are to be agents of social change, then access to communities who are going to be affected by such change and involving their input only makes sense. Access, in this description, refers to the literal connecting and collaborating with community members. How do technical communicators collaborate, network, and involve people outside of their immediate space as agents in decision-making? This is a complex, contextual, and localized question; I discuss some of the ways this very project grapples with this

question in 3.4a. Further, some of the corporate/organization-community relationships may be positioned as transactional in situations where there is a move *towards* participatory approaches. Technical communicators must take care to balance the needs and expectations of all stakeholders in a way that *sustains* and grows relationships, rather than treats them as a transaction. The balance, in this instance, is an example of efficiency. As practitioners and instructors, we must be aware of power relations; surveillance studies offer a means to identify patterns of those who expect to be monitored, oppressed, and silenced due to the history of surveillance systems and biometric identification.

An essential component of this study is the move towards understanding "what can technical communicators *do*?" Because surveillance is embedded into our systems and structures, individual advocacy or accountability only extends so far. Agboka and Dorpenyo (2022) write that confronting injustice, such as surveillance systems, requires much more than "pledges, vain statements, and roundtable discussions and commitments" (p. 6). In fact, when we think through the ways technical communicators may intervene in and resist surveillance systems, we can take a page out of Agboka and Dorpenyo's book by acknowledging the ways in which we are all complicit in and affected by injustice: "coalition building and allyship are very necessary to respond to the dynamic and complex set of challenges involved in addressing issues of injustice" (2022, p. 6). Since "technical communicators are uniquely poised to function as public intellectuals" (Bowdon, 2004, p. 325), this places a sense of responsibility to create collaborative efforts in calling attention to the ways in which we are surveilled and the consequences of such data collection, mining, and distribution. Technical and professional communicators have extensive influence and practice in the classroom, sites of research, workplace contexts, scholarly platforms and so on. With the influence and reach communicators have, these sites

(and subsequent sites of surveillance) may be "potential sites of various unjust practices", or such sites could "present opportunities for analyzing, critiquing, and enacting social justice" (Agboka & Dorpenyo, 2022, p. 7). Change is necessary, and technical communicators are able to demonstrate such action within and outside of the classroom.

2.3 Bridging Surveillance Studies, Technical Communication, and Feminist Rhetoric

Grounding surveillance studies in technical communication allows researchers the opportunity to analyze and provide suggestions to dismantle systems that seek to discriminate based on categories such as privilege, access, and risk (Dubrofsky & Magnet, 2015). As Young (2023) notes, technical communicators (broadly defined) are well apt to contribute to surveillance studies through their expertise and future research trajectories. Technical communicators have the expertise that allows them to "do" surveillance work, especially due to their role as "information workers[21] and their technology expertise" (Young, 2023, p. 49). In surveillance practices, privacy is stripped away the moment the user agrees to policies (i.e., technical documents, wearable devices, etc.) to use the application and/or device of their choosing; this is a generalization, and I argue that bodies are surveilled without ever "agreeing" to use a device (in this example). Surveillance occurs through, for example, tools such as wearable devices and invasive technologies, Learning Management Systems (LMS) and other software/lockdown browsers, surveillance through a gaze (lateral) of communities, and beyond. The important intersection between technical communication and surveillance studies, however, resides in how situations are contextual. Surveillance *and* technical communication are part of

[21] Information workers: those essentially paid to create knowledge, communicate ideas, process information in one way or another transform symbols from one form to another, and whose jobs are primarily to manipulate information for either the purpose of intensive mental work creating new knowledge or the more routine tasks like inputting information into a computer (Porat, 1977, p. 3; Young, 2023, p. 49).

larger systems and circumstances, and impact people disproportionately. Young (2023) notes that technical communicators are experts on contributing to lines of reasoning and evoking kairotic appeals; because of this, technical communicators in positions to analyze and critique the "argument, or rhetoric, of surveillance itself," as well as to critique "the deployment and fitness of that rhetoric" (p. 54). For this study, surveillance will be explored through biometric technologies and identification in healthcare.

Walton, Moore, & Jones (2019) argue that when "we examine power as it exists in the interpersonal, we are invited to acknowledge the ways TPC [technical and professional communication] affects and is affected by lived experiences and bodies" (p. 124). This provides an additional site of knowledge making between technical communication and surveillance studies; if technical communicators are "knowledge makers" (Slack, Miller, & Doak, 1993) then we must consider our own "individual positions within the matrix of domination, oppression, and injustice in addition to institutional, structural, and cultural power relations" (Walton, Moore, Jones, & 2019, p. 126). Issues of power and dissemination/collection of information must "resist, subvert, and intervene" (Frost & Eble, 2015, p 6) in the ways biometric technologies, for example, include forms of oppression that should be addressed and corrected. For example, while biometric technology "mediates the human body and identity, between technology and biology," (Ajana, 2013, p. 3), technical communication mediates between users and technology (Dorpenyo, 2019, p. 364).

Implications for surveillance in technical communication may be analyzed through its in/visible applications. Jiwani (2015) demonstrates in their contribution how surveillance technologies work to "discipline certain bodies in particular ways, making some bodies hyper-visible and others invisible crafting regimes of intelligibility wherein what is rendered invisible

is legitimized and taken for granted as an inherent part of the social fabric" (p. 11). Feminist and social justice methodologies may better inform the intersection of surveillance and technical communication to explore how bodies are put on visual display. For example, Banks (2006) has argued that "racism is enforced and maintained through our technologies and the assumption we design and program into them–and into our uses of them" (p. 10). A feminist approach to surveillance studies also highlights the ways that surveillance is integral to many of our foundational structural systems, ones that breed disenfranchisement, and that continue to be institutionalized. Further, social justice research in technical communication investigates how "communication broadly defined can amplify the agency of oppressed people—those who are materially, socially, politically, and/or economically under-resourced" (Jones, 2016, p. 347). It is important to study the role biometric technologies play in technical communication, especially because biometric technologies serve to "categorize bodies with a dangerous discriminatory logic that cannot be touted as 'true' or 'objective'" (Murray, 2007, p. 359). The discriminatory logic embedded in the design of biometric technology, for example, raises social justice concerns in which technical and professional communicators have important roles to play (Dorpenyo, 2019).

It is important to center feminist and social justice methodologies as approaches to reorienting the lens of how surveillance pervades our lives; though surveillance is not solely understood as digital, many of the technologies that put bodies on visual display are not new and are rather associated with longstanding forms of oppression. For example, Jiwani argues that "visibility serves to heighten the focus on particular bodies by foregrounding their difference" (Dubrofsky & Magnet, 2015, p. 11). Many technical communicators have taken up centering feminist and social justice methodologies such as work intersecting gender and technical

communication (Takayoshi & Van Ittersum, 2018; Petersen & Moeller, 2016), urgency, power, and social justice (Angeli, 2019; Walton, Moore, & Jones, 2019), cultural rhetoric(s) and technology (Haas, 2012), and ethics of efficiency (expediency) (Katz, 1992). Because many technical communicators play a role in developing integral parts of products, such as user interfaces and technological design, feminist methodologies are crucial to the creation and collaboration needed for designing biometrics (see Gurak & Bayer, 1994). Feminist methodologies will be further discussed in the methodology section (Chapter 3).

2.4 Technological Infrastructure, Power, and Data Collection

Writing infrastructures may be better understood through feminist and technical rhetorics, and surveillance studies which critically engage the relationship between power and information collection (Dubrofsky & Magnet, 2015). Many risk/health scholars have written about the impact of technologies on health (focusing on women's reproductive health in particular). Unacknowledged biases and norms that contribute to dominant power structures work their way into a number of forms of monitoring and documentation. Beck (2015) writes about how digital users and writers of the Internet "cannot simply ignore the globalized political economy that so heavily relies upon computer code and architecture, and thereby shapes online discourse and design patterns" (p. 137). As Andrejevic writes in the foreword, "Even without the high-tech interface, the physical world is already overlaid with the information the viewer brings to it" (Dubrofsky & Magnet, 2015, p. xvi). Andrejevic argues that our gaze is never "unmediated, innocent, or free of preconceptions, background knowledge, and information" (Dubrofsky & Magnet, 2015, p. xvi). The physical world is overlaid with the information the viewer brings to it, which helps technical communicators better understand the role biometric identification plays within our networks. With or without digital technologies, systems still incorporate forms of

surveillance that categorize individuals. Andrejevic mentions that the result of such surveillance is the automation of shared "knowledge" and preconceptions (Dubrofsky & Magnet, 2015, p. xvi).

Digital rhetoric is especially pertinent to understanding systems and infrastructures utilizing biometric technologies as surveillance tools because of the overlapping issues of agency and authorship. There is a direct correlation between power and data mining, especially with who is collecting information as well as who has agency over their information. Haas (2012) defines technology as informed by cultural and rhetorical theories as these theories "interrogate how inequalities of power are produced, maintained, and transformed through culture and its rhetorics" (p. 288). Haas (2012) refers to technology as both integral to culture and always already cultural. When referring to technologies, especially that of biometric technologies, I am not defining technology as "things." The reason for this is that to position a technology as a thing suggests it as something "discrete and isolatable from culture—and thus observable and knowable" (Haas, 2012, p. 289). Likewise, as Slack and Wise (2005) demonstrate, "the formulation of technology as things that are useful deflects vision toward the tool-like use of these things, and away from the work or role of these things beyond matters of usefulness" (p. 97). Thus, by intersecting technical communication (as a subfield of rhetoric and composition) and surveillance studies, scholars are able to better theorize the "interdependent relationships between living and nonliving actors" as well as the "rhetorical and cultural work that technologies do in our everyday lives (in the discipline, our classrooms, popular media, workplaces, and beyond)" (Haas, 2012, p. 289).

As Beck and Hutchinson Campos (2021) note, "scholars of computers and writing have addressed issues of surveillance and privacy within writing infrastructures through course

management systems, plagiarism detection software, and social media used in classrooms" (p. 3). This study does have implications for classroom use, however; it can further contribute to writing infrastructures, defined as the role language, through writing and identification, plays in shaping our understanding of objects and bodies (Boyle, 2018; Ching, 2018). This study helps to build a narrative that explores biometric technology use in healthcare and amplifies the historically silenced to better understand how such infrastructures impact our ways of knowing and being.

As many scholars have noted, technologies and bodies are codependent and always acting upon each other (Frost & Haas, 2017; Nakamura, 2008). Infrastructures are not neutral, and "exert agency over everything from how we communicate to how bodies move" (Frith, 2020, p. 406). Munster (2006) argued that digital histories "have limited the present and future possibilities for bodies in culture" (p. 9). Haas (2018) highlights the interface as a possible means through disrupting and fostering power structures since, "digital rhetoric requires a negotiation–an interfacing–between bodies, identities, rhetoric, and technology" (p. 412). Interfacing involves having disparate objects communicating or meeting together; just as identities and bodies are not neutral, technology also is not passive. Interfacing is "always already political" and rhetorical studies that consider this negotiation reveal what communities benefit from certain relationships, especially within digital writing infrastructures (Haas, 2018, p. 412).

Thus far, this literature review has defined surveillance, technical and professional communication, and provided examples of ways the two distinct fields (surveillance studies and technical communication) may be bridged through a feminist lens. This helps situate the connection between technological infrastructures, data collection, and power dynamics. One

aspect of surveillance studies that is important to study in relation to infrastructure, data, and power are biometric technologies. The following sections overview the history of biometric identification as a surveillance tool, including implications of biometrics as they manifest in authentication and privacy practices, ethical concerns and terms of service, and the rhetoric of health and medicine. This review thus far, and what will continue, helps to provide backgrounding for my research questions: How do healthcare professionals (specifically neonatal nurses) define biometric technologies? What are neonatal nurses' perceptions of biometric technologies? Providing context about components of biometric technology (infrastructure, history, and data, for example), and the intersection between surveillance studies and technical communication not only contributes to the exigency of this study, but also situates (and integrates) neonatal nurses within the conversations surrounding biometrics.

2.5 History of Biometric Identification

This section discusses the history of biometric technologies (identification/authentication) within the United States. This study is situated within the United States, and exploring the manifestation and implementation of biometric technologies assists in understanding the urgency and exigency for its usage in healthcare as a site of surveillance.

One tool (or technology) of surveillance are biometric technologies. In their interview, Ajana refers to biometrics as "a technology of identification that relies on physical characteristics or behavioural traits to identify or verify the identity of a person" (Beer, 2014). For the purpose of this study, I define biometric identification as any identifier of the body that is collected and used for personal identification (and authentication). That is, the data being collected is an example of biometric technologies, whereas the device used to collect biometric information is a tool to collect such data. To further define the parameters, Ajana explains that biometrics can be

defined as a form of "biomediation." In this way, the body is "doubly mediated by being at once the object and the subject of measurement, i.e., that which is being measured as well as what enables the process of identification" (Beer, 2014). This therefore suggests that though biometric technologies are used as "fixed" identification methods, technical communicators should address the ways in which control and management of our bodies, identities, and movements are manipulated.

As Foucault (1979) infamously notes in his definition of biopolitics[22], the same techniques that are used to protect and enhance certain lives can be used to endanger and obstruct others. Gates (2011) writes how "the assumption that biometrics are derived from and link directly to physical bodies conceals a complex technological process of mediation, as well as a whole set of historical relationships that create the very conditions of possibility for biometric identification" (p. 15). Biometric identification as a personal identifier occurs in varying contexts. Surveillance studies scholars note that the history of biometric technologies in the United States is most "widely understood" as beginning with law enforcement and military use in the 1960s, and gradually became utilized for "public consumption" through surveillance of welfare recipients in the 1990s (Magnet, 2011, p. 9). This study does focus on biometrics within the United States, and though implementation and historical significance of biometric technologies has certainly developed and/or informed the United States, this study seeks to contribute to the history and implementation of biometric technologies within the country. To provide some context for usage within the United States, I will only briefly refer to other countries. For example, though biometric identification may be traced to the end of the 19th century, where a French police officer introduced the concept of scientific policing, biometrics

[22] Biopolitics: the management of life in various sectors such as the government, healthcare, border patrol (Foucault, 1979).

were not used in the United States for law enforcement until the 1960s. This French officer used "body measurements taken of specific anatomical characteristics to identify reoffending criminals, which often proved successful" (Thales Group, 2022). In Paris, France, the Forensic Identification Unit began in 1888, where mugshots and anthropometry (measurements of a body) were collected; four prints were instituted in 1894, and ten prints were added in 1904 (Thales Group, 2022). According to Thales Group (2022), the Metropolitan Police in the United Kingdom started the use of biometrics for identification in 1901. In the United States, it was initiated by the New York police in 1902 and by the FBI in 1924.

It is rhetorically important to trace how the United States has taken advantage of times of crisis and/or fear to introduce innovative technologies. For example, Angeli (2019) explores writing and communication in the Emergency Medical Services (EMS) field. Angeli's insights provide rhetorical insights into the ways in which professionals working in high-stakes environments manage communication. Similar to the EMS professionals, the neonatal nurses in my study communicate in unpredictable and arguably high-stakes workplaces. Furthermore, many of the concerns that Angeli (2019) cites, also overlap greatly with the concerns neonatal nurses may encounter with their own communication; whether that is improper documentation as it relates to insurance claims, patient records, healthcare/provider communication, and more. Biometric technologies and their usages also fall under concerns with communication. As I will discuss in Chapters 4 and 5, neonatal nurses *are* technical communicators, and as such, have a responsibility to communicate with patients. Angeli (2019) also argues similarly regarding EMS professionals: despite a "compliance" with protocol, technologies such as biometrics, can create more harm than their expected usage for compliance, safety, and efficiency. Though Angeli argues for "accurate and clear written communication," I foresee neonatal nurses engaging in

efficient healthcare communication as defined by engaging in communication practices that are both convenient for the nurse, while also effectively reaching the patient's background and knowledge base. This may look like a mixture of communication materials, including, but not limited to written communication as well as audio and/or visual genres and documents. Those working in healthcare should communicate "for specific audiences in specific contexts for specific purposes" (Andersen, 2014, p. 118). The following figure is a timeline that refers to the major (popularized) events that historicize biometric usage, globally and in the United States.



Figure 1: Biometric Timeline

Both within and outside of the healthcare context, women, people of color, Black, Indigenous, disabled, LGBTQIA+, amongst many more groups of people experience hyper-surveillance of their bodies, movements, and societal engagement. For example, technical communicators engaging in social justice work such as McIlwain (2019) discuss the history of

building a technological society, and the impact on who is/isn't included. McIlwain writes that when information societies were beginning to be created, people failed to consider "what kind of society they were building. Who was included and who was deliberately excluded from that society?" (2019, p. 19). Further, when we consider the history of hyper-surveillance in the United States, it's crucial to consider the consequences of building a new technological society. Unfortunately, those consequences were not and still are not considered in the ways emerging and previous technologies are created. Such technologies still uphold systemic oppression, and McIlwain (2019) argues that the technological society certainly did not account for the ways "in which Negroes were [and still are] educationally and technologically both separate and unequal" (p. 19). Biometric technologies reinforce this technological divide, and may be viewed as disciplinary power in action, a concept coined by Foucault (1977). An example of biometric technologies as disciplinary power is displayed by Browne (2015) who explores how surveillance studies "has been primarily concerned with how and why populations are tracked, profiled, policed, and governed at state borders, in cities, at airports, in public and private spaces, through biometrics, telecommunications technology, CCTV, identification documents, and more recently by way of Internet-based social network sites" (2015, p. 13). Browne writes about practices such as body measurements and the branding of slaves, arguing that such practices persist in modern-day biometric data collection or automated facial recognition (2015). Bodies who tend to be hyper-surveilled are subject to endless screenings—they may be considered "a risky" body rather than a body "at risk" (Scott, 2003, p. 10). Hyper-surveillance of bodies, however, is not a new concept. For example, though the "information superhighway" was "paved with good intentions," as McIlwain (2019) notes about Bill Clinton's 1994 State of the Union address, Clinton neglected to note the potential "detours and dead-ends that could lead the have-

nots of today to become the know-nots of tomorrow" (p. 111). The information superhighway was paved, but it certainly was paved over by colonial powers: once a community, the Afronet quickly became a space appropriated and taken without attribution or collaboration by white designers and developers. Afronet, according to McIlwain (2019), was essentially an online space created for "Africans and African Americans" to network through exchanging "messages, emails, electronic bulletin boards" and general topics (p. 94). I include the example of the Afronet as a way to connect to biometric technologies because of the way both technological advances have had significant harmful impacts due to hyper-surveillance. Biometric technologies have impacted people disproportionately, especially those who are Black, Indigenous, and people of color; the technologies have been trained *on* the very people they also oppress. The same goes for Afronet: a space of networking and activism became a model that eventually was used to harm and punish the very people who created the space. This sentiment, of co-opting and appropriating technology only to turn the advances onto the people who created them, has occurred time and time again; in this study, focusing specifically on biometric technologies and how they hyper-surveil.

Another example of modern-day surveillance through biometric identification is omnipresent racial profiling, especially of Muslims and refugees, at national borders and on the street; surveillance scholars argue that this racial profiling would be barely conceivable without the "colonial, orientalist, and racist logic" that facilitates it in the first place (Dubrofsky & Magnet, 2015; Browne, 2015; Gates, 2011). For example, Al-Khateeb refers to biometric screening as a means to dismantle the "physical borders and boundaries that once deemed the refugee body unencounterable"; however, the very same screening systems also serve to thicken "borders and boundaries between bodies, determining who is dangerous and who is endangered,

thus who must be violated and who can violate" (2021, p. 23). According to Dubrofsky and Magnet (2015), biometric technologies render "the body in binary code," and industry manufacturers of these technologies claim this code "reveals nothing about race, gender, class, or sexuality, instead representing bodies as anesthetized strands of ones and zeroes" (p. 15). However, when tracing the history of biometric identification and its implementation, it becomes increasingly clear that biometric technologies are a "high-tech form of racial and gender profiling" that categorize people by using criteria that often explicitly include race and gender (Dubrofsky & Magnet, 2015, p 15). For many biometric technologies, "like characteristics" include race and gender identities, which is why it would be much easier to scan a database searching for "like characteristics" to identify, rather than scanning an entire system without categories. Despite the appearance of and communication to consumers of "efficiency," technical communicators should note that this sorting and categorization only serves to contribute to existing forms of biological racialism and sexism, in which "race and gender are imagined as stable biological properties that can be reliably read off the body" (Dubrofsky & Magnet, 2015, p. 15).

Further, biometric technologies have only more recently been introduced into rhetorical studies and technical communication. For example, Al-Khateeb (2021) writes about the intersection of biometrics and disability studies that examines the (re)emergence and (re)circulation of biometric screening technologies. Dingo (2012) posits, "[Rhetoricians] must examine how rhetorics travel—how rhetorics might be picked up, how rhetorics might become networked with new and different arguments, and how rhetorical meaning might shift and change as a result of these movements" (p. 2). Considering the history and ethical implications of introducing biometrics to different sites of surveillance, such as that of healthcare, is an

important aspect of rhetorical theory and meaning. Rhetoricians and technical communicators alike are well-poised to analyze, intervene in, and reimagine the impact of emerging technologies in various sites. Al-Khateeb (2021) specifically focuses on tracing biometrics, and notes that their "discursive, material, and technological practices" reveal how "such discourses and their promises materialize on bodies of refugees and shape their encounters as 'others and other-others'" (p. 15). Ahmed writes that "others" are those who are marked as different and live within the national body; while "other-others" are those who are different but "may yet be expelled from the national body" (2000, p. 106). This biopolitical control is only one of many ways biometric technologies may be referred to or considered dark or deceptive design (see 4.6). Biometric technology's introduction through state sanctioned use, often, as we've seen, on multiply marginalized people during times of fear and disguised as a necessity for safety, is part of understanding the means through which rhetorics travel.

Surveillance is integral to the United States' (and many global) foundational structural systems, "ones that breed disenfranchisement, and that continue to be institutionalized" (Dubrofsky & Magnet, 2015, p. 7). Surveillance practices and technologies normalize and maintain whiteness, able-bodiedness, capitalism, and heterosexuality (see hooks, 1994). In/visible ways marginalization occurs may be exemplified in Ramos' chapter which explores surveillance as the "tracking and identification of Latinx migrant communities by state entities such as the Department of Homeland Security" (2021, p. 150). To further discuss the ways surveillance practices and biometric technologies maintain whiteness, Smith writes about how though the modern bureaucratic state is often the focus of surveillance studies, "the surveillance of native peoples is a key foundational strategy of colonialism: technologies of surveillance were integral to settler colonialism" (2015, p. 7). Surveillance through biometric technologies often

does not question the state itself, but rather seeks to modify the extent to which and the way the state surveils. For example, Al-Khateeb (2021) writes how biometric screening technologies function not only as technologies that "promise safety for the US American public through the identification of suspicious refugees," but also as "technologies of mobility that promise resettlement for refugees in the United States" (p. 15). This positions biometric technologies as allegedly humane and transparent; however, their deceptive design creates a barrier to intervention in the ways in which the technologies, despite their affordances, exacerbate conditions of violence and control for refugees. In other words, as Al-Khateeb (2021) argues, "what gets overlooked by such rhetorical framings are questions about the ways technologies of biometrics have also functioned as technologies of immobility and debility for refugees;" though this notion certainly extends much further than refugee populations (p. 16). To reiterate, surveillance is integral to the United States system. For example, a focus on gendered settler colonialism foregrounds how surveillance is not simply about "seeing" but about "not-seeing" the settler state (Smith, 2015). Smith recounts how the "violence of surveillance through organized settler colonial practices transformed First Peoples into racialized communities, thus facilitating the bureaucratically managed rape of indigenous people, making them 'rapeable'" (2015, p. 7). This example illustrates how surveillance has been foundational to the structure of the United States, from the beginning. The systems that inform the state were built on disenfranchisement and continue to be oppressive in their nature often in seemingly invisible ways due to their normalization within society.

It is important to note that biometric data was collected prior to the "digital era" emerging. Shephard (2019) charts the historical intersections of surveillance and feminism, taking note that to govern during colonial rule (17th to 18th century), colonial rulers gathered as

much data on their local population as possible. Shephard (2019) notes that this included "not just acquiring knowledge of the geographical regions and political structures but also the meticulous categorization and description of people and their social forms." This categorization is what Lyon (2003) refers to as a form of social sorting. Lyon (2003) posits that surveillance is used to sort people into categories to establish demographics such as a person's gender, socio-economic status, ethnicity or religion. Categorization also assigns values and risks and seeks to establish trends for future "terrorist" movements, crimes, and/or consumer behavior (Lyon, 2003, p. 79). Based on these categorizations, the colonies ultimately served as an initial form of testing and refining surveillance technologies before they were implemented and used in and across Europe. For example, according to Ahmad H. Sa'di (2012), a colonial officer in British India named William J. Herschel was the first to introduce fingerprinting as a biometric identification feature in a commercial setting in the 19th century.

As Dorpenyo (2019) notes, although biometric technologies are touted to be "credible, value-neutral, objective, and accurate," they are inherently discriminatory (p. 361). Though this chapter focuses on some of the history of biometrics and examples of their usage through time, it's important to note that this study focuses on biometric usage in healthcare, a site of surveillance. Biometrics, especially with their implementation in healthcare settings, reproduce "existing inequalities into their designs and risk further disenfranchising already vulnerable populations" (Rose, 2016, p. 428). For example, Magnet (2011), discusses how biometric fingerprint scanners struggle to scan the hands of Asian women, and worn-down or sticky fingerprints are rejected by fingerprint biometric scanners. Magnet writes how the mass failures that characterize the use of the biometrics indicate that the biometric "suffer[s] from 'demographic failures'" (p. 5), or it cannot account for "bodily deviance" (2011, p. 30), meaning

that any type of body that falls outside the limit of the biometric lens cannot be accurately read or is read as "deviant" or "not compliant." Essentially, those with "careers that require manual labor have abused hands" (Murray, 2007, p. 358) and are rejected by biometric technology; those in "particular trades that use their hands often," such as health-care workers (p. 351) also suffer rejection. The notion of compliance, especially as it relates to patients and healthcare workers, will be further discussed in section 2.8.

The ways in which biometric technologies surveil occur in multiple ways. Initially, some surveillance scholars might argue that the surveillance occurred (and still does) in a top-down way. Cultural anthropologist Martha Kaplan posits that Jeremy Bentham's Panopticon design, which has been popularized by Michel Foucault and often used by surveillance scholars as a metaphor for ubiquitous surveillance, was not constructed in Europe but instead in India under British colonial rule (Kaplan, 1995). Described by Foucault (1977) from a centralized point of view, the body within the Panopticon can see the surrounding prison cells and occupants, but the prisoners cannot see inside the panoptic tower. As I have previously written (Banville & Sugg, 2021), because prisoners cannot see inside the tower, they are left to assume that their behavior and activities are constantly being observed by the Panopticon. Speaking broadly, the basic tenet of Panopticism is the power of control—control over norms—wherever they may be found. A control over norms may be exemplified through biometrics—how they're designed and deployed. For example, since Panopticism emphasizes control, Foucault posits that power or control becomes *biopower* because of the way people shift their physical (and mental) state to modify their behaviors. Biometric technology is a means of behavioral control: the body, under constraints, tries to remain compliant and not deviant, despite the powers watching (like the Panopticon or biometric technology) that decide whether or not the body matches a norm.

According to Murray (2007), biometric technology is "gauged to the idealized bodies in a given culture, producing as 'abnormal' those who do not correspond to the idealized model…Biometric technology has been made therefore, with a normative notion of 'body' in mind; a culturally constructed notion of embodied identity…" (p. 351). Because of the ways the Panopticon and biometric technologies are designed, the systems give those with power—actual and assumed—the expected norm to measure "non-conformity" to, thus contributing to the everyday[23] form of surveillance.

An example of biometric usage in the United States occurred in 2011, when the FBI signed a contract with the military developer Lockheed Martin to launch a pilot program called "Next Generation Identification" (NGI). This program, according to Head and Stroud (2018) was designed to "utilize biometric data to assist the investigations of local and federal law enforcement agencies as part of anti-terrorism, anti-fraud, and national security programs." Head and Stroud (2018) cite that by late 2014, the program's facial recognition sector became fully operational and was used regularly by the FBI and other law enforcement agencies to aid in the identification of persons of interest in open investigations. A major issue with the usage of the identification system is that when the program was first introduced, the FBI used biometric data from known and convicted criminals to compile the database (Head & Stroud, 2018). The database has since been expanded through a program run by the FBI's Criminal Justice Information Services (CJIS) called FACE (facial analysis, comparison, and evaluation), and now includes driver license photos from individuals that have been issued a photo ID from participating states (Head & Stroud, 2018). Alongside the issues of opting in/out procedures, is the problematic nature of the FBI choosing to uphold systemic oppression through training facial

[23] Everyday surveillance: transcends institutional spaces and is brought to formerly private places such as web browsers in one's own home (Lyon, 2001, p. 2).

recognition systems on convicted criminals. As we know in the United States, many convicted "criminals" are subjected to wrongful suits and are often targeted due to their race, gender, age, disability, and sexuality. For example, Pew Research Center (2020) has published research suggesting that large numbers of incarcerated Black and Hispanic populations make up more than the United States population for the specific race. This leads to not just surveillance concerns, but also concerns with the array of technologies such as biometrics that are being developed to hyper-surveil such groups of people for "criminal" activity.

Biometric technologies are one approach to the problem of "disembodied identities," also known as "the existence of visual and textual representations of individuals that circulate independent of their physical bodies" (Gates, 2011, p. 12). Examples range from early technologies such as the phonograph, to photography, and more. Gates (2011) states that biometrics are a "solution" to the "disembodied" problem because of the ways they *include* bodies in mediation with communication. In this way, emphasizing and designing a more *embodied* approach to mediating communication, supplements identification and even replaces, in some cases, what Robertson (2009) calls a "documentary regime of verification" (p. 331). The aim of a documentary regime of verification is to assign each individual an "official" identity that could be verified in repeated transactions with the state and other institutions (Robertson, 2009, p. 331). These official forms of bureaucratic identification combine a "set of existing and already mediated markers of identity—such as names, addresses, signatures, and photographs—to create a more stable and standardized form of identity that could be verified via the very bureaucratic apparatus that constitutes that identity" (Gates, 2011, p. 13). These official forms of bureaucratic identification contribute to our understanding(s) of authentication procedures and subsequent historical usage of biometrics for identification.

2.6 Authentication and Privacy: The Paradox

It would not be possible to discuss biometric technologies without mentioning their purposes of identifying and authenticating. Dorpenyo (2019) questions: Why will a technology which has the sole purpose of verifying and authenticating users reject specific groups of people? Focusing on biometric use, for instance, helps social justice advocates to discuss "how humans are affected by technology design and use, and how technologies define what it means to be a human" (Dorpenyo, 2019, p. 370). Authentication is a component, or second layer to the biometric technologies utilized in our neoliberal society. Authentication practices are slightly different from biometric identification technologies in their layered history. For example, two-factor authentication may be considered a second layer of biometric identification due to the expectation that the body on the receiving end of the technology is indeed the body confirming their identity. Authentication may be thought of as an extension of the foundational biometric technologies; the goal of authentication is to, as biometric technologies aim to do, confirm that the user is who they say they are. This newly added protection, for example when logging into a Google account, is intended to add "security" for the individual who owns the account and the data associated with that account. Authentication in this context is often referred to by cybersecurity professionals; it is defined as "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system" (NIST, 2022). Authentication in this sense may be viewed as a digital panopticon: rather than building a "secure" system from the start, the responsibility for safety/security and compliance falls on the user. The individual responsibility is an example of the way user behavior is manipulated to *opt in* to being verified by an invisible database that decides if we *are who we say we are*. Johnson-Eilola (2004) argues that we should see such an accumulation of texts, images, and ideas that

comprise a database, through which users are verified against, composed "intertextually from bits and pieces already out there" (p. 200). Alongside the notion of individual responsibility and behavioral control to be "confirmed" by a database, there are also issues of security and privacy.

Herein lies the "Privacy Paradox." The privacy paradox refers to the "conflict between individuals express[ing] concern over privacy and their apparent willingness to surrender that privacy in online spaces in exchange for very little of value"[24] (Reilly, 2021, p. 33). A popular claim is that people do not care about privacy. Everything is already out there! In reality, people do care about their privacy. According to a new study by MAGNA Media Trials and Ketch, 74% of people now rank data privacy as one of their top values (Ketch, 2022). Privacy becomes important to people when linked to other things that matter to them. For example, privacy concerns in relation to infant and mother safety, as well as job security (such as with neonatal nurses) are crucial components to exploring healthcare as a site of surveillance.

Adorjan and Ricciardelli (2019) describe in their study the privacy paradox, which identifies a "disjuncture" between what is said about privacy and what is done in practice (p. 8). Content, referred to as any digital information, is, after all, searchable. Content can also be replicated outside of its original context, and as boyd (2014) notes, invisible audiences make it difficult or impossible to anticipate those who ultimately receive the content posted in networked publics, outside of intended audiences. When technical communicators discuss the privacy paradox, or even notice this with certain groups (such as in my study, neonatal nurses), we should consider the delineation between perceptions of privacy based on assumptions regarding specific affordances of technology. While many youths, for example, are aware of privacy risks

[24] Privacy Paradox: refers to the "conflict between individuals express[ing] concern over privacy and their apparent willingness to surrender that privacy in online spaces in exchange for very little of value" (Reilly, 2021, p. 33 as cited in Beck & Hutchinson Campos, 2021).

related to their online activities, "they see the compromise of their privacy as unavoidable, even imperative, in order to connect with peers online and acquire social and personal benefits through accessing" social media sites (Regan & Steeves, 2010 as cited in Adorjan & Ricciardelli, 2019, p. 10). The privacy paradox, as I will discuss more in Chapter 4, explains the tension between personal and professional, and the perceived ability to self-manage. There's a specific notion of personal responsibility for managing risk (akin to James's (2014) privacy mindset "privacy in your own hands"). As Adorjan and Ricciardelli (2019) argue, what is fundamentally absent is understanding of the personal troubles tied to privacy management. When people declare that they have nothing to hide, it suggests that if they *did* have something to hide, it would be illicit. It also suggests that one is indifferent to monitoring and "sidelines consideration of situations where one's digital profile can be usurped and privacy breached" (Adorjan & Ricciardelli, 2019, p. 23). This indifference also neglects other ways of engagement, especially digitally, such as digital activism (Wilson & Hayhurst, 2009), consenting digital sexual expression (Koskela, 2006), and corporate surveillance and targeted advertising (Marx & Steeves, 2010; Steeves, 2012; Anthony et al., 2017).

Though written over two decades ago, Haggerty and Ericson's discussion of privacy remains relevant: "privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation" (2000, p. 616). They compare the space of negotiating privacy to the emergence of the wage economy; in this way, there was an exigence for the fixing of monetary prices to labor, power, citizens, and economists. Further negotiating privacy, Kerr et al. (2009) argues that "new methods of authentication, verification and surveillance have increasingly allowed persons and things to be digitally or biometrically identified, tagged, tracked, and monitored in real time and in formats that can be captured,

archived, and retrieved indefinitely" (p. xxiv). Therefore, newer surveillance technologies do have implications for "informational privacy[25]" defined as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Kerr et al., 2009, p. xxvii). Even though I believe privacy is a human right, Gates (2011) has argued that in surveillance studies advocating for privacy rights can be viewed as problematic. Hall points to how "welfare recipients, people living in poverty, and queers have never been entitled to privacy," as well as the fact that privacy has not always kept people, especially women and children, safe because violence "often occurs in the home" (2015, p. 149). Solely focusing on privacy as the only concern related to surveillance and biometrics is a narrow scope that often obscures other pressing concerns. Technical communicators should care about privacy, but not *just* privacy. In a report conducted by the Annenberg School for Communication, the survey revealed that 56% of American adults don't understand the term "privacy policy," often believing it means that a company won't share their data with third parties without permission (Reissman, 2023). As previously discussed, this is quite the opposite. Reissman (2023) posits that because so many Americans feel that internet privacy feels impossible to comprehend—with "opting-out" or "opting-in," biometrics, and VPNs—they don't trust what is being done with their digital data. For example, opting in/out presupposes three claims: that people are informed; that they understand what is happening to their data; and that they've provided consent for it to happen (Reissman, 2023). Of course, since biometric technologies are surveillance tools, data protection and access are major concerns (which are privacy concerns). For example, more than 8 in 10 Americans believe, incorrectly, that the federal Health Insurance Portability and Accountability Act (HIPAA) stops apps from selling

[25] Informational privacy: defined as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Kerr et al., 2009, xxvii).

data collected about app users' health to marketers (Reissman, 2023). Along with privacy concerns, an even larger feminist concern is based on how biometric technologies are impacting people disproportionately. Why do we need to identify, or authenticate our bodies in the first place? Is this not control? Why do we need technologies for ease of use, when we know they are fallible and discriminatory? Why don't we put people first?

Expanding upon the idea of informational privacy and advocacy, according to Haggerty and Ericson (2000), the general public is slowly beginning to understand and notice the profits that are being made from the sale of their data doubles. Data doubles[26] are, as Edwards writes, "vast archives of personalized information [that] circulate absent the territorialized body, traveling via infrastructures subject to sorting, categorization, and other surveillance techniques. In other words, a multiplicity of circulatory flows is always being produced through everyday acts of composing, flows that can be aggregated, duplicated, sorted, and recirculated" (2021, p. 79). One consequence of this recognition, writes Haggerty and Ericson, has been the further commodification of the self (2000, p. 616). In the assemblage process, groups which were previously exempt from routine surveillance are now increasingly being monitored (Haggerty & Ericson, 2000). Now the question is what, if any, compensation individuals should receive for the sale of their personal information (Haggerty & Ericson, 2000, p. 616).

Data doubling happens as an assemblage network, where information collected from the body through biometrics is sorted and categorized based on characteristics, which then circulates and is shared among healthcare providers, other third parties, and governing bodies. If the body is commodified through data doubling, this raises concerns about the impact of selling patient

[26] Data doubles: "vast archives of personalized information circulate absent the territorialized body, traveling via infrastructures subject to sorting, categorization, and other surveillance techniques" (Beck & Hutchinson Campos, 2021, p. 79).

data and information in healthcare (broadly defined), but also in biomedicine. Biomedicine[27] is the study and practice of applying biological and physiological principles to health and medical care settings (Foucault, 1975) with the ultimate goal of "correct[ing] disease and restor[ing] normal functioning" (Fuller, 2017, p. E640). Biomedicine stresses standardized, evidence-based interventions validated through biological research, with treatment administered via licensed practitioners, such as doctors, nurses, technicians, and other specialists, and has been the dominant healthcare system across the United States and in much of the Western world for over a century. Furthermore, because biomedicine determines which conditions and what types of interventions are "approved," biomedicine also structures how other stakeholders across the medical-industrial complex, like pharmaceutical companies and insurance providers, are implicated in patient care. As such, understanding how biomedicine operates is imperative in understanding how other facets of our healthcare system—such as the deployment of biometric technology—may be used, when, and most importantly, why.

2.7 The Digital Cyborg and Layered Literacies

Biometric technologies and their usage (and impact) in healthcare can be better understood through how stakeholders relate to concepts discussed thus far such as authentication, privacy, and biomedicine; such concepts are part of what may be referred to as "health literacy." People engage in a plurality of literacies, especially when it comes to healthcare. Though there are a multitude of definitions both of literacy and health literacy, for the purposes of this study I adopt Ratzan & Parker's (2000) definition of health literacy[28] as, "the degree to which

[27] Biomedicine: the study and practice of applying biological and physiological principles to health and medical care settings (Foucault, 1975) with the ultimate goal of "correct[ing] disease and restor[ing] normal functioning" (Fuller 2017, p. E640).

[28] Health literacy: "the degree to which individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions" (Ratzan & Parker, 2000).

individuals have the capacity to obtain, process, and understand basic health information and services needed to make appropriate health decisions" (p. vi). When considering the ways patients interact with biometric technologies, for example, this is an added layer of "health literacy." Questions related to the "literacy" of biometrics may be: What is the technology, how is it used, where is information distributed, who has access, and so on. Not only is this information crucial for patients to know, but also the healthcare practitioners they are working with. This is a question that Lupton (2012) posits: whose responsibility is it (patient or provider) to disclose and communicate health information? Biomarkers may be used to locate patient records and share them with stakeholders across the medical-industrial complex, such as pharmaceutical companies, insurers, providers, and government entities, often without patient knowledge and explicit consent.

Cargile Cook's (2002) concept of "layered literacies" in technical communication may bridge to healthcare to discuss how health literacy is an embodied, multisensory experience that is mediated by healthcare technologies, such as biometrics. In Western cultures, healthcare technologies use biometrics such as voice recognition, facial recognition, and fingerprinting to identify and surveil the body to better explain and understand the person. Part of understanding health literacy as embodiment is also highlighting the ways in which data is collected and/or distributed digitally. Who has access to the information that technologies mediate? For example, Reyman (2013) highlights the many ways that user data is collected and appropriated by corporations in the absence of widespread online literacy. Reyman's (2013) work explores how users subject their data to surveillance and collection, which has ownership implications (see Amidon et al., 2019). Agreements (such as Terms of Service and End-User License Agreements) often protect the company providing services, rather than the individual user. Kulak further

contributes to the data collection conversation by arguing that technical communicators, researchers, and instructors should consider principles of "transparency and security, considering (so as to counter) the potentially pernicious effects and reuses of the data we gather and the stories the data can tell" (2021, p. 15). Ruti (2017) writes how neoliberal capitalism uses biopolitical forms of control disguised as good, necessary, and for safety/security. Bivens et al., (2018) propose that understanding health literacy practices entails "attending to the interconnectedness of our senses and sensibilities, which pushes back against the mind/body divide often invoked in Western cultures" (n.p., see also Segal, 2005).

When we consider the ways, neoliberal capitalism uses biopolitical control disguised as potentially "positive" deliverables such as safety and security, it's also important to note how neoliberalism itself is a disguise. Queer theorists such as Ruti (2017) question and critique the ideals of success from scholars such as Jack Halberstam: for example, how neoliberal capitalism promotes a route to happiness, when arguably, it is those ideals that "blind us to structural inequalities such as poverty, racism, sexism, and homophobia which make it impossible for some people to succeed no matter how hard they try" (2017, p. 16). This is important to know because of the ways in which structural inequalities have been normalized and deeply rooted within the surveillance systems and biometric technologies within our society. Further, Ahmed notes that in the place that heteronormative society has determined as 'right': the price of being acceptable is to "*become* acceptable to a world that has already decided what is acceptable" (2010, p. 106). Opting out then, in this capacity, is the ability to defeat cruel optimism which "exists when something you desire is actually an obstacle to your flourishing" (Berlant, 2011, p. 1). Cruel optimism entails the hope that our efforts to fit into neoliberal society will bring us the "love, intimacy, success, security" and so forth that people crave even when they are extremely unlikely

to do so (Ruti, 2017, p. 16). So perhaps instead of continuing our desires and fantasies as established by the dominant norm, we must "opt out[29]" of such; this may lead to our "seeing" the norms that we have been persuaded to conform to and defy such structures. Further, rhetoricians of health and medicine and technical communicators alike are able to lend insight into the ways that "discourse is created, used, disseminated, and also critiqued" (Meloncon & Frost, 2015, p. 9). Therefore, we are able to determine not just *how* health literacy is layered, but also *how* we determine such "norms" and means of communication. This idea of opting out is currently, just that, an idea. There is an illusion of choice associated with opting out, which adds to our layered literacies. Illusion of choice has been normalized, and is deeply rooted in surveillance systems, and yet individuals are *told* and therefore *perceive* that they have choice (to opt out). Because of these deeply rooted social norms, there's a pressure to not question or resist (another layer of literacy). Technical communicators can engage in decision-making that contributes to the layers of health literacy, while also communicating the very "norms" that users *should* be able to opt out of, instead of taking them at face value. Such contributions will be discussed in more detail in Chapter 5.

Ethical approaches to technological decision making must also engage in queer and feminist principles of critical analysis, collaboration, and care, since decision-making often only focuses on economic/management concerns, or on technique and innovation (Pacey, 1983, p. 101). Layered (health) literacies include ethical implications of biometric technology usage; amongst the examples and concerns already raised, it's also crucial to consider the ways biometrics may queer the body. Queering data or the body is a means to critically question pre-

[29] In this instance, opting out may not be literal (this largely isn't an option in healthcare). Opting out, in this context, could mean resistance or challenging (depending on the user position). Resistance will be discussed in more detail in Chapter 5.

fixed categories, as well as the values granted to "some identities above others" along with questioning who actually benefits "from the collection, analysis, and use of data about LGBTQ people" (Guyan, 2022, p. 1). Queer data is a tension, often critically questioning fixed categories which are subsequently used to create decisions. For example, Mauro and Schellmann (2023) write about artificial intelligence (AI) tools developed by large technology companies, including Google and Microsoft, meant to protect users by identifying "violent or pornographic visuals so that social media companies can block it before anyone sees it." According to Mauro and Schellmann (2023), the companies claim that their AI tools can also detect "raciness" or how sexually suggestive an image is. For example, the AI rated pictures of "women" as more "racy" or sexually suggestive than comparable pictures of "men" working out. Further, medical tests with partial nudity suggested that the AI tags photos of "women" in everyday situations as sexually suggestive. The gender bias and objectification is deeply embedded within AI. With this establishing of fixed categories of what "is or isn't sexually suggestive," should be queered to critically examine why images are suppressed or labeled as contentious imagery.

Biometric technology design, if approached through a queer perspective that is fluid (critically questioning pre-fixed categories and characterizations), may be one step towards dismantling the discriminatory nature of the technologies. The first step is to "see" the norms: what categories are created? Why? Who do they help and harm? The onus, of course, relies on those creating the technologies in the first place. For example, current biometric identification design is based on determining a "match;" that is, determining that the body is precisely who they claim to be. This suggests that there is a "norm," something measurable that determines if the characteristics are close enough, in "compliance," or "non-deviant"—concepts that would not exist when queering data.

The idea of a "norm" reminds me of Lupton's (2012) piece, where they argue that mHealth technologies produce a digital cyborg body. A cyborg[30] is a creature "simultaneously animal and machine," which Haraway uses to discuss the idea that feminist thinking should "[take] pleasure in the confusion of boundaries" that results in part from digital technologies (1985, p. 66). Though biometrics are not mHealth technologies, such tools and technologies are used to collect biometrics. The Global Observatory for eHealth of the World Health Organization defines mHealth as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices" (Park, 2016, p. 253). Lupton (2012) describes the mHealth technologies as not only acting as "prostheses, but also as interpreters of the body" (p. 229). Similarly, we might consider biometrics as a digital cyborg body: the subject produced through the use of biometric technologies is constructed as an "object" of surveillance, and as a "responsible citizen who is willing and able to act on the health imperatives issuing forth from the technologies" (Lupton, 2012, p. 229). Bodies are not only subject to the hyper-surveillance, but it is also expected that such bodies comply. Queering biometric design would mean a dismantling of a "norm" to be measured against, and further, a critical questioning of what it means to be in compliance as an "object" or "cyborg" subject to state surveillance. Can a world even be imagined?

Bodies are "non-compliant" if deciding not to opt into usage of biometric technologies and are also non-compliant if they do not match collected data in a repository. In fact, as Lupton (2012) writes, "Technologies bestow meaning and subjectivity upon their users, just as users shape the technologies and give them meaning as they incorporate them into their everyday practices" (p. 232). Technologies assume embodiments just as much as they also construct and

[30] Cyborg: a creature "simultaneously animal and machine" (Haraway, 1985).

configure them. In fact, those who identify as LGBTQIA+ for example, "risk engaging with technologies [such as biometrics] that might normalize categories and practices that hamper rather than help the wider" population (Guyan, 2022, p. 3). For example, because current biometric design categorizes in pre-fixed ways, historical assumptions based on the United States' white heteropatriarchal capitalist society informs such preconceived notions. Therefore, any research that suggests the practices of "x" community, may end up *hampering* said community from any change or progression because the black box is determined by the labels and/or characteristics. All this to say: instead of surveillance technologies potentially helping vulnerable communities, engaging with technologies that normalize categorizing ultimately harm them. Such "normalization" of categorizing may lead researchers to question the "gendered and sexualized identities and emotions," which operate across different populations as individuals "interact with, manipulate and appropriate surveillance practices" (Ball, Haggerty, & Lyon, 2012, p. 8). Another example exemplifying the ways categorization may cause harm is the constraint on identity change. The power to change identity is situated in institution(s). For example, in the case of gender reassignment, the endorsement and approval of someone "authorized" as an "identifier" is required before identity change can be affected legally: this may include a medical doctor or a panel of doctors (Jenkins, 2012, p. 160). Further, in this study, we could extend this line of thinking to the sex of a newborn infant: the sex is "officially assigned and registered by an authorized medical professional" (Jenkins, 2012, p. 160). The predetermined categorization from birth only serves to hamper rather than help those who wish to choose their identity.

As aforementioned, technologies such as biometrics have been employed to render the body more visible, to exert a biopolitical gaze and disciplinary control upon bodily structure and

function (Foucault, 1975; Armstrong, 1995; Casper & Morrison, 2010). In this way, patients are surveilling themselves: their bodies are more visible, more "empowered" and thus they are being "more responsible" and active agents in participating in the monitoring of their own bodies (Mort et al., 2009). There is a societal urge to remain in compliance. Do what the doctor says, they're the professional, the expert. Yet for historically excluded groups of people such as those who are Black, Indigenous, people of color, disabled, and LGBTQIA+, the body is *never* in compliance with white heteropatriarchal capitalist norms. When biometrics are introduced into an always already vulnerable and precarious space such as healthcare, this creates a feedback loop: non-compliant bodies are rendered non-compliant despite attempts to *be* compliant with the given technology. Biometric technologies are ableist, racist, and often "out" bodies who are not verified against the predetermined set of data (this argument is detailed more in Chapter 4). For example, Haraway (1988) argued that individuals in contemporary Western societies become cyborgs in their interaction with technologies, blurring the distinction between human and machine. As Gates (2005) argues, biometrics are designed to transfer "some of the responsibility for the culturally conflicted process of identification from humans to computer systems" and in this way, biometrics are another example of how we have "always relied on technologies in the effort to fix identities and bind them to bodies" (p. 50). Racism is especially prominent in international security, where, for example, the "war on terror"[31] has embraced dataveillance, biometrics and surveillance cameras (Whitaker, 1999). Despite the potential to "out" people, such as those who identify as transgender, being visible is also a means of "pushing back against opponents who have (and continue to) work to silence and erase particular lives" (Guyan, 2022,

[31] Though the "war on terror" references the September 1, 2001, attacks in the United States, this war "ended" in 2021. The "face of terror" refers to the facial recognition technology trained to flag a person of color as a potential "terrorist" (see Gates, 2005 and 2011).

p. 7). Ultimately, visibility prompts "examination of whose data are seen by whom and with what effects," (Brighenti, 2007) because managing visibility is at the core of control (Ball, Haggerty, & Lyon, 2012, p. 6). While there are certainly safety, security, and categorical concerns related to biometrics, there are also ways the technologies help to shape data sets and individual perception of identity. Even so, biometrics are not the end all for identification.

2.8 Rhetoric of Health and Medicine: Biometrics are not the End All

The rhetoric of health and medicine has been "acutely concerned with, and responsive to, its relationships with health and medical areas and publics" (Scott & Meloncon, 2019, p. iv). When technical communicators think about the sub-field of health and medicine, we may adopt the view from Scott & Meloncon (2018) where:

> health and medicine encompasses rhetorical interactions across varied and overlapping cultural spheres, including those related to health and medical research, clinical medicine, health and medicine policymaking, consumer health and personal health management, health advocacy, and community-based health practices (p. 2).

Because "the rhetorics of health and medicine are comfortable navigating a myriad of sites and locations and texts" (Scott & Meloncon, 2018, p. 4), one surveillance site that is of relevance are healthcare institutions. Work that most obviously counts as rhetoric of health and medicine is "criticism of the texts, genres, and discourses of health and medicine, as performed by a rhetorical critic" (Segal, 2009, p. 228). The connections between surveillance, technical communication and the rhetorics of health and medicine (RHM) include topics concerning the regulation and identification of bodies, patient autonomy, personal/ethical concerns, privacy, and consent.

Within healthcare, amongst other larger institutions, biometrics are used to prove that the person is who they say they are. As we know, this is not necessarily the case. Bodies rendered static are unrealistic; in fact, bodies can and often do change. One example is the use of tattoos as

a form of biometric surveillance. For example, tattoos are often logged within prison systems to better identify people. Even so, tattoos are not only changeable, but they can also be removed. Another example is from personal experience: when I wanted to substitute teach in secondary education, I had to get fingerprinting done so that the school could run a background check. We also know that sometimes fingerprints may be altered and are not always a true indicator of a person (consider placing a bandage on a cut, missing fingers, burns, wounds, and so on). Therefore, any company that is outsourced for biometric authentication should be responsible for engaging in ethical decision-making, including engaging in transparent practices regarding the collection and dissemination of private information such as health information. Lewis, Gangadharan, Saba, and Petty (2018) argue that in order for us to understand and confront "the ways in which data-based technologies are being integrated into our everyday lives" we must first understand how our "communities—ones marginalized by race, class, gender, sexuality, immigration status, and other natural and imposed identities—are impacted by data-based technologies" (p. 3) Lewis et al., (2018) further that our data are our stories, and when "our data are manipulated, distorted, stolen, exploited, or misused, our communities are stifled, obstructed, or repressed, and our ability to self-determine and prosper is systematically controlled" (p. 3). Our data *are* our stories.

Though wearable devices are often referred to as biometric technologies, I argue that wearables may harbor and collect biometric data but are not necessarily personal identifiers. The reason for this is that wearables have the opportunity to collect information regarding breathing activity, heart rates, sleep patterns, and much more; yet the problem lies with that data collection may not confirm the person who is utilizing the wearable. Beck (2018) cites Brock and Shepard who note:

> [We] convince ourselves that we are actively making decisions about how to participate in a given system when, in reality, we accept options made apparently available to us from a set of constrained possibilities. In other words, we allow ourselves to be persuaded that we are the only agents involved in a particular situation when, in reality, there are networks of visible and invisible actors working to persuade us to specific ends—often including further participation in relevant persuasive computational systems (p. 21).

Rhetoricians and technical communicators have long critiqued wearable devices especially in terms of health intervention and reproductive justice. For example, Novotny and Hutchinson Campos (2019) focus on Glow, a fertility and period tracking application, and discuss the duality of self-empowerment and reduction of individual agency. Novotny and Hutchinson Campos (2019) call for technical communicators to be changemakers in redesigning how consent is obtained when collecting user's personal health information. This is an apt example for the ways technical communicators may intervene in consent protocols for patients when biometric technologies are utilized in healthcare.

Biometric identification and technologies have ethical concerns that should be negotiated and addressed. McKee and Porter (2017) define ethics as every day because ethics are "fundamental to all human interaction. Ethics pertains to character and credibility and to issues of trust, responsibility, honesty, and integrity" (p. 27). In taking this perspective on rhetoric and ethics, McKee and Porter view rhetoric and ethics as an "inextricably intertwined set of concerns fundamental to all communication interaction" (2017, p. 27). Especially in health and medicine, the usage of biometrics has serious ethical considerations. For example, if you are working in an Intensive Care Unit, biometrics such as facial identification and fingerprinting fail if/when the body has suffered from severe trauma. One problem with relying on emerging technologies such as biometrics are that they are fallible; Welhausen and Bivens (2021) allude to some of these concerns when referencing a case study of two civilian emergency response mHealth apps—PulsePoint and OD Help. mHealth apps are similar to wearable devices in that they are not

biometric technologies, yet they harbor biometric identification and information. The mHealth apps can (and are) fallible, and also raise concerns about user agency, data protection, and other vulnerabilities.

The inextricable tie of rhetoric and ethics is furthered by Boyd (2015), who writes about the problematic nature of informed consent to medical treatment and research, and its relationship to autonomy, trust, and clinical practice. Throughout this study, it is likely that such ethical concerns will arise in relation to informed consent. For example, Herman and Chomsky (1988) coin the term "manufacturing consent," which refers to creating the appearance of personal agency by leveraging public opinion through propaganda. This manufacturing of consent occurs when employers mandate biometric identification within the professional context. For example, as I will discuss in greater detail in Chapter 4, for many of the neonatal nurses interviewed, fingerprinting was not just used for patient identification, but also for employees (signing in/out, accessing certain areas, etc.). As mentioned, wearable devices and mHealth apps are not biometric technologies, despite their potential to collect biometric data. Such devices, like many other surveillance technologies, are introduced to the public (or consumers) through the illusion of empowerment, or agency. Employers often have "wellness" or "health" incentives for employees through the use of wearable devices. Beck (2018) writes, "The lure of using technology as a means of improving the quality of life has proven time and again a benefit (writing, the printing press, radios, televisions) for humanity, but often a tool ripe for exploitation and the consolidation of power by those who produce the technology" (p. 300). While employers, such as those who oversee neonatal nurses, assume (and likely believe) that they are contributing to creating a "safe" and "healthy" work environment by implementing new technologies, they are instead subjecting employees to increased surveillance that they are

(often) uninformed about. What biometric information is collected and distributed by the wearable devices/mHealth applications? Are employees in healthcare systems aware (and consenting) of the collection and dissemination (selling)? How is the concept of "health" and "wellness" situated for healthcare employees?

Ethical and consensual issues have always evolved with digital technologies, and McKee and Porter (2018) note that with their ever-increasing pace of change it is "essential that we acknowledge and address the ethical (and legal) issues shaping our communications. Ethics is integral to technology development, design, and usage" (p. 401). Of particular concern are issues of privacy, accessibility, compliance, and transparency. Tschider (2019) argues that consent "has an almost deferential power as a proxy for consumer choice, organizations increasingly use consent as a de facto standard for demonstrating privacy commitments" (p. 1505). Tschider (2019) documents that The Department of Health and Human Services and the Federal Trade Commission have integrated the concept of consent into health care, research, and general commercial activities. The health industry alone uses at least four different variants of consent: "traditional notice with explicit consent, express authorization, informed consent, and notice with recommended consent" (Tschider, 2019, p. 1506). The variants of consent directly correlate with the ethical issues that arise with personal information and identification, including doxing. Hutchinson Campos (2018) notes that "doxing enacts a rhetorical function of persuasion when a person attempts to wield power over another through the exploitation of personally identifying information" (p. 303). Doxing[32] is defined within hacker culture as "the pluralized nominal form of the action to 'drop documents' on a person" (Hutchinson Campos, 2018, p. 304). Doxing is important to mention in relation to the rhetoric of health and medicine, and biometric

[32] Doxing: defined within hacker culture as "the pluralized nominal form of the action to 'drop documents' on a person" (Hutchinson Campos, 2018, p. 304).

identification because of the ways in which Western culture has exploited personally identifying information; this may occur within the workplace and professional contexts such as a healthcare institution where employers wield power over employee information and/or patient information. Doxing plays only a "partial role in a collection of actions such as hacking, leaking, and whistleblowing that can be defined together as hacktivism" (Hutchinson Campos, 2018, p. 305). Technical communicators may view biometric technologies as a form of doxing, where in this study for example, neonatal nurses wield their influence in patient decision-making, often unknowingly exposing patients to exploitation of their personal information.

To the extent that a patient does not opt into usage of technologies such as biometrics, they are often referred to as "non-compliant." This notion of compliance will be explored more in Chapter 4: in the chapter, I explore a tension between patient and nurse expectations, and compliance is often referred to whether or not a patient follows a healthcare providers' advice (Stone, 1997). Yet a healthcare providers' advice often falls in the scope of immediate assistance: perhaps this comes in the form of testing; prescription; rest; and so much more. The immediacy or urgency of a solution for a patient comes at the expense of potential long-term impacts or [invisible] consequences. For example, healthcare providers will use the tools they need to operate or perform their expected responsibilities; however, healthcare providers do not consider topics such as data management, distribution of information (especially to third-parties), informed consent and opting out of technologies, and so on. This will be discussed further in Chapter 4. And if such concerns *are* discussed, it is often done verbally, which technical communicators are aware provides ample room for misunderstanding, clarity concerns, and overall localization and legitimacy concerns (Boyd et al., 1974). Compliance is often discussed in terms of safety, specific standards or procedures, and ultimately risk management.

Compliance therefore regulates; surveillance tools such as biometric technologies exacerbate compliance initiatives in the ways that the technology becomes an embodiment of the person. Are you who you say you are? If you do not consent to use the technology, are you non-compliant? Are healthcare providers to infer that you may not be who you claim to be? This embodiment suggests disciplinary and behavioral control and determines a "norm" where there is an expectation for always already engaging in acceptable and appropriate acts. Anything other than the acceptable and appropriate courses of action are considered risky (Sauer, 2003; Scott, 2003). As Stone (1979) mentions, technical communicators must address issues of responsibility; that is, questions such as "Is the patient able to comprehend the hazards of noncompliance?" or better yet, "Or, is the physician able to present the hazards in such a way that the patient will comprehend?" (p. 52). As Blackwell (1976) notes, it is best to regard every individual as a potentially "noncompliant client." This is based on an acknowledgment that human limitations apply to *all* of us. So why do we rely on non-human devices, which also have limitations, to assume and determine compliance?

2.9 Chapter Summary

The literature review helps to inform and provide a foundation for the methods discussed in Chapter 3 (textual corpus analysis, screening surveys, and interviews) by defining surveillance, technical and professional communication, bridging the two fields through feminist rhetoric, charting the history of biometric technologies and identification, authentication and privacy practices, ethical implications and terms of service, and the rhetoric of health and medicine. This literature review assists in understanding how surveillance, in particular, biometric technologies impact people disproportionately. What came from intersecting the two fields, surveillance studies and technical communication, was an obvious need for a

methodological framework that could analyze various sites of surveillance. What follows in Chapter 3 is an introduction to interlocking surveillance, a methodological framework that centers feminist principles in moving towards raising awareness, advocating, and intentionally pushing for more transparency of "normalized" surveillant practices.

By reviewing the ways surveillance studies can inform technical communication, this insight creates a foundation for the ways in which a specific group of people in healthcare who work with biometric technologies (a surveillance tool) define and perceive the technology. Because the site of surveillance is in healthcare, it is also necessary to include literature by rhetoricians of health and medicine to situate this study at a time where fields are overlapping in their desire for advocacy work, especially patient advocacy. Overall, this literature review explores interdisciplinary contributions and situates the current conversation surrounding authentication and privacy to shape an argument of necessity. That is, to fully be able to intervene in design protocols, communication materials, and defining biometric technologies, it is necessary to return to the history of usage which contributes to charting such surveillant usage of biometrics present day. This review helps to situate my research questions: How do neonatal nurses define biometric technologies? What are neonatal nurses' perceptions of biometric technologies? The next chapter will discuss the methods and methodologies utilized in this study.

REFERENCES

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide." *Canadian Review of Sociology, 56*(1), 8-29. https://doi.org/10.1111/cars.12227

Agboka, G.Y., & Dorpenyo, I.K. (2022). The role of technical communicators in confronting injustice—everywhere. *IEEE Transactions on Professional Communication, 65*(1), 5-10. https://doi.org/10.1109/TPC.2021.3133151.

Ahmed, S. (2010). *The promise of happiness.* Durham, NC: Duke University Press.

Ahmed, S. (2000). *Strange encounters: Embodied others in post-coloniality*. Taylor and Francis.

Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. Basingstoke, UK: Palgrave Macmillan.

Al-Khateeb, M.T. (2020). Toward a rhetoric account of refugee encounters: biometric screening technologies and failed promises of mobility. *Rhetoric Society Quarterly, 51*(1), 15-26. https://doi.org/10.1080/02773945.2020.1841276

Amidon, T.R., Hutchinson, L., Herrington, T., & Reyman, J. (2019). Copyright, content, and control: Student authorship across educational platforms. *Kairos, 24*(1). http://kairos.technorhetoric.net/24.1/topoi/amidon-et-al/index.html.

Andersen, R. (2014). Rhetorical work in the age of content management: Implications for the field of technical communication. *Journal of Business and Technical Communication, 28*(2), 115-157. https://doi.org/10.1177/1050651913513904

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era.* Lawrence: University Press of Kansas.

Angeli, E.L. (2019). *Rhetorical work in emergency medical services: Communicating in the unpredictable workplace*. Routledge.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a sociology of privacy. *Annual Review of Sociology, 43*, 249–69.

Armstrong, D. (1995). The rise of surveillance medicine. *Sociology of Health & Illness, 17*(3), 393-404.

Ball, K., Haggerty, K.D., & Lyon, D. (2012). *Routledge handbook of surveillance studies.* Routledge.

Banks, A.J. (2006). *Race, rhetoric, and technology: Searching for higher ground.* Mahwah, NJ; Urbana, IL: Lawrence Erlbaum; National Council of Teachers of English.

Banville, M., & Sugg, J. (2021). "Dataveillance" in the classroom: Advocating for transparency and accountability in college classrooms. *In The 39th ACM International Conference on*

Design of Communication (SIGDOC '21), October 12-14, 2021, Virtual Event, USA. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3472714.3473617

Beck, E., & Hutchinson Campos, L. (Eds). (2021). *Privacy matters: Conversations about surveillance within and beyond the classroom*. Utah State University Press.

Beck, E. (2018). Implications of persuasive computer algorithms. In Alexander, J. and Rhodes, J. (Eds.). *The Routledge handbook of digital writing and rhetoric* (pp. 291-303). Routledge.

Beck, E. (2016). Who is tracking you? A rhetorical framework for evaluating surveillance and privacy practices. In S. Apostel & M. Folk. (Eds.). *Establishing and Evaluating Digital Ethos and Online Credibility*, (pp. 66-84). Hershey, Pennsylvania: IGI Global.

Beck, E.N. (2015). The invisible digital identity: Assemblages in digital networks. *Computers and Composition, 35*, 125-140.

Beer, D. (2014). The biopolitics of biometrics: An interview with Btihaj Ajana. *Theory, Culture and Society, 31*, 329-336. https://doi.org/10.1177/0263276414546380

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new jim code*. Polity.

Berlant, L. (2011). *Cruel optimism*. Duke University Press.

Bivens, K.M., Arduser, L., Welhausen, C.A., & Faris, M.J. (2018). A multisensory literacy approach to biomedical healthcare technologies: Aural, tactile, and visual layered health literacies. *Kairos: A Journal of Rhetoric, Technology, and Pedagogy, 22*(2). http://kairos.technorhetoric.net/22.2/topoi/bivens-et-al/index.html

Blackwell, B. (1976). Treatment adherence. *British Journal of Psychiatry, 129,* 513-53.

Blake, S.J., Longo, B., & Wills, K.V., (Eds.). (2006). *Critical power tools: Technical communication and cultural studies.* Albany: State University of New York Press.

Bowdon, M. (2004). Technical communication and the role of the public intellectual: A community HIV-prevention case study. *Technical Communication Quarterly, 13*(3), 325–340.

Boyd, J.R., Covington, T.R., Stanaszek, W.F., & Coussons, R.T. (1974). Drug-defaulting analysis of noncompliance patterns. *American Journal of Hospital Pharmacy, 31,* 485-491.

Boyd, K. (2015). The impossibility of informed consent? *Journal of Medical Ethics, 41*(1), 44-47. Retrieved from www.jstor.org/stable/43283222.

boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication and Society 15*(5), 662-79. https://doi.org/10.1080/1369118X.2012.678878.

boyd, d. (2014). *It's complicated: The social lives of networked teens*. London: Yale University Press.

Boyle, C. (2018). *Rhetoric as a posthuman practice.* Ohio State University.

Brighenti, A. (2007). Visibility: A category for the social sciences. *Current Sociology, 55*(3), 323–442.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Cargile Cook, K. (2002). Layered literacies: A theoretical frame for technical communication pedagogy. *Technical Communication Quarterly, 11*(1), 5–29. https://doi.org/10.1207/s15427625tcq1101_1

Casper, M., & Morrison, D. (2010). Medical sociology and technology: Critical engagements. *Journal of Health and Social Behavior, 51*(1), S12–S32.

Ching, K.L. (2018). Tools matter: Mediated writing activity in alternative digital environments. *Written Communication, 35*(3), 344–375. https://doi.org/10.1177/0741088318773741

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498–512.

Dingo, R.A. (2012). *Networking arguments: Rhetoric, transnational feminism, and public policy writing*. University of Pittsburgh Press.

Dorpenyo, I. (2019). Risky election, vulnerable technology: Localizing biometric use in elections for the sake of justice. *Technical Communication Quarterly, 2*8(4), 361-375. https://doi.org/10.1080/10572252.2019.1610502

Dubrofsky, R.E. & Magnet, S.A. (2015). *Feminist surveillance studies*. Durham and London: Duke University Press.

Edwards, D. (2021). Deep circulation. In E. Beck & L. Hutchinson Campos, *Privacy Matters: Conversations about Surveillance Within and Beyond the Classroom,* (pp. 75-92). University Press of Colorado.

Frith, J. (2020). Technical standards and a theory of writing as infrastructure. *Written Communication, 37*(3), 401-427. https://doi.org/10.1177/0741088320916553

Frost, E.A. & Eble, M. (2015). Technical rhetorics: Making specialized persuasion apparent to public audiences. *Present Tense, 4*(2). Retrieved from http://www.presenttensejournal.org/wp-content/uploads/2015/04/FrostandEble.pdf

Frost, E.A., & Haas, A.M. (2017). Seeing and knowing the womb: A technofeminist reframing of fetal ultrasound toward a decolonization of our bodies. *Computers and Composition, 43*, 88-105. https://doi.org/10.1016/j.compcom.2016.11.004

Frost, E.A. (2018). Apparent feminism and risk communication: Hazard, outrage, environment, and embodiment. In M. Eble & A. Haas (Eds.)., *Key Theoretical Frameworks: Teaching Technical Communication in the Twenty-First Century* (pp. 23-45). Utah State University Press.

Foucault, M. (1975). *The birth of the clinic: An archaeology of medical perception.* New York: Vintage Books.

Foucault, M. (1977). *Discipline and punish: The birth of the prison.* New York: Vintage.

Foucault, M. (1979). *The birth of biopolitics: Lectures at the collège de France, 1978-1979.* Picador.

Fuller, J. (2017). The new medical model: A renewed challenge for biomedicine. *Canadian Medical Association Journal, 189*(17), E640-E641.

Gates, K. (2005). Biometrics and post-9/11 technostalgia. In R. Maxwell (Ed.)., *Surveillance: A Special Issue of Social Text* (pp. 35-55). Duke University Press.

Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Gurak, L.J., & Bayer, N.L. (1994). Making gender visible: Extending feminist critiques of technology to technical communication. *Technical Communication Quarterly, 3*(3), 257-270. https://doi.org/10.1080/10572259409364571

Guyan, K. (2022). *Queer data: Using gender, sex and sexuality data for action*. London: Bloomsbury Publishing

Haas, A. (2012). Race, rhetoric, and technology: A case study of decolonial technical communication theory, methodology, and pedagogy. *Journal of Business and Technical Communication, 26*(3), 277-310. https://doi.org/10.1177/1050651912439539

Haas, A.M. (2018). Toward a digital cultural rhetoric. In J. Alexander & J. Rhodes (Eds.), *The Routledge Handbook of Digital Writing and Rhetoric*, (pp. 412-422). Routledge.

Haas, A.M., & Eble, M.F. (Eds.). (2018). *Key theoretical frameworks: Teaching technical communication in the twenty-first century.* Logan, UT: Utah State University Press.

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Hall, R. (2015). Terror and the female grotesque, introducing full-body scanners to U.S. airports. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies,* (pp. 127-150). Durham and London: Duke University Press.

Haraway, D. (1985). A manifesto for cyborgs. *Socialist Review, 15*(2), 65-107.

Haraway, D. (1988) A manifesto for cyborgs: Science, technology and socialist feminism in the 1980s. In E. Weed (Ed.) *Coming to Terms: Feminism, Theory and Practice* (pp. 173–204). New York: Routledge.

Head, J., & Stroud, S. (2018, April 17). Biometrics, data, and privacy. *Center for Media Engagement.* https://mediaengagement.org/research/biometrics-data-and-privacy/

Hoffman, M. (2014). Chapter two: Disciplinary power. In D. Taylor (Ed.), *Michel Foucault: Key Concepts*, (pp. 27-39). New York, NY: Taylor and Frances. https://doi.org/10.4324/9781315711478

hooks, b. (1994). *Teaching to transgress: Education as the practice of freedom*. New York: Routledge.

Hutchinson, L. (2018). Wielding power and doxing data: How personal information regulates and controls our online selves. In J. Alexander & J. Rhodes (Eds.), *The Routledge Handbook of Digital Writing and Rhetoric* (pp. 303-317). Routledge.

James, C. (2014). *Disconnected: Youth, new media, and the ethics gap.* Cambridge: The MIT Press.

Jenkins, R. (2012). Sorting out who's who. In K. Ball, K.D. Haggerty, & D. Lyon (Eds.)., *Routledge Handbook of Surveillance Studies,* (pp. 159-166). Routledge.

Jiwani, Y. (2015). Violating in/visibilities, honor killings and interlocking surveillance(s). In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 79-93). Durham and London: Duke University Press.

Johnson-Eilola, J. (2004). The database and the essay: Understanding composition as articulation. In A.F. Wysocki, et al. (Eds)., *Writing New Media: Theory and Applications for Expanding the Teaching of Composition*, (pp. 199-226). Utah State University Press.

Jones, N.N. (2016). The technical communicator as advocate: Integrating a social justice approach in technical communication. *Journal of Technical Writing and Communication, 46*(3), 342–361. https://doi.org/10.1177/0047281616639472

Jones, N.N. (2016a). Narrative inquiry in human-centered design: Examining silence and voice to promote social justice in design scenarios. *Journal of Technical Writing and Communication, 46*(4), 471-492. https://doi.org/10.1177/0047281616653489

Kaplan, M. (1995). Panopticon in poona: An essay on foucault and colonialism. *Cultural Anthropology, 10*(1), 85-98. https://doi.org/10.1525/can.1995.10.1.02a00040

Katz, S.B. (1992). The ethic of expediency: Classical rhetoric, technology, and the holocaust. *College English, 54*(3), 255-275.

Kerr, I., Lucock, C., & Steeves, V. (2009). *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. Oxford: Oxford University Press.

Koskela, H. (2006). The other side of surveillance: Webcams, power and agency. In D. Lyon, *Theorizing surveillance: The panopticon and beyond*, (pp. 163–81). Collumpton, Devon, UK: Willan Publishing.

Kulak, A. (2021). Ethics in big data composition research: Cybersecurity and algorithmic accountability as best practices. In A. Licastro, & B. Miller (Eds.)., *Composition and Big Data.* University of Pittsburgh Press.

Kynell-Hunt, T., & Savage, G. (2004). *Power and legitimacy in technical communication: The historical and contemporary struggle for professional status*. Routledge.

Lewis, T., Gangadharan, S. P., Saba, M., & Petty, T. (2018). Digital defense playbook: Community power tools for reclaiming data. *Our Data Bodies.* https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Spreads.pdf

Licastro, A., & Miller, B. (2021). *Composition and big data.* University of Pittsburgh Press.

Lupton, D. (2012). M-health and health promotion: The digital cyborg and surveillance society. *Social Theory & Health, 10*, 229-244. https://doi.org/10.1057/sth.2012.6

Lyon, D. (2001). *Surveillance society: Monitoring everyday life.* Open University Press.

Lyon, D. (2003). *Surveillance as social sorting: Computer codes and mobile bodies.* Routledge.

Lyon, D. (2007). *Surveillance studies: An overview*. Malden, MA: Polity Press.

Magnet, S. (2011). *When biometrics fail: Gender, race, and the technology of identity.* Duke University Press.

Marx, G., & Steeves, V. (2010). From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society, 7*(3/4), 192–230

Mauro, G., & Schellmann, H. (2023, February 8). 'There is no standard': investigation finds AI algorithms objectify women's bodies. *The Guardian*. https://www.theguardian.com/technology/2023/feb/08/biased-ai-algorithms-racy-women-bodies

McKee, H.A., & Porter, J.E. (2017). *Professional communication and network interaction: A rhetorical and ethical approach*. New York, NY: Routledge.

McKee, H.A., & Porter, J.E. (2018). Digital media ethics and rhetoric. In J. Alexander & J. Rhodes (Eds.), *The Routledge Handbook of Digital Writing and Rhetoric*, (pp. 401-412). Routledge.

McIlwain, C. (2019). *Black software: The internet & racial justice, from the afronet to black lives matter illustrated edition.* Oxford University Press.

Miller, C.R. (1979). A humanistic rationale for technical writing. *College English, 40*(6), 610-617.

Meloncon, L., & Frost, E.A. (2015). Charting an emerging field: The rhetorics of health and medicine and its importance in communication design. *Communication Design Quarterly, 3*(4), 7-14. https://doi.org/10.1145/2826972.2826973

Moore, L.J., & Currah, P. (2015). Legally sexed, birth certificates and transgender citizens. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 58-79). Durham and London: Duke University Press.

Mort, M., Finch, T., & May, C. (2009). Making and unmaking telepatients: Identity and governance in new health technologies. *Science, Technology & Human Values, 34*(1), 9-33

Munster, A. (2006). *Materializing new media: Embodiment in information aesthetics.* Hanover, NH: Dartmouth College.

Murray, H. (2007). Monstrous play in negative spaces: Illegible bodies and the cultural construction of biometric technology. *The Communication Review, 10*, 347–365. https://doi.org/10.1080/10714420701715415

Nakamura, L. (2008). *Digitizing race: Visual cultures of the Internet*. Minneapolis: University of Minnesota Press.

National Institute of Standards and Technology (NIST). (2022). Authentication. *Computer Security Resource Center.* https://csrc.nist.gov/glossary/term/authentication#:~:text=Verifying%20the%20identity%20of%20a,resources%20in%20an%20information%20system.

Nemorin, S. (2017). Post-panoptic pedagogies: The changing nature of school surveillance in the digital age. *Surveillance & Society, 15*(2), 239-253. https://doi.org/10.24908/ss.v15i2.6033

Noble, S. (2018). *Algorithms of oppression: How search engines reinforce racism.* New York University Press.

Novotny, M., & Hutchinson, L. (2019). Data our bodies tell: towards critical feminist action in fertility and period tracking applications. *Technical Communication Quarterly, 28*(4), 332-360. https://doi.org/10.1080/10572252.2019.1607907

Pacey, A. (1983). *The culture of technology.* Cambridge: MIT.

Park, Y.T. (2016). Emerging new era of mobile health technologies. *Healthc Inform Res, 4*, 253-254. https://doi.org/10.4258/hir.2016.22.4.253. PMID: 27895955; PMCID: PMC5116535.

Petersen, E.J., & Moeller, R.M. (2016). Using antenarrative to uncover systems of power in mid-20th century policies on marriage and maternity at IBM. *Journal of Technical Writing and Communication, 46*(3), 362-386. https://doi.org/10.1177/0047281616639473

Pew Research Center. (2020, May 6). Blacks, Hispanics make up larger shares of prisoners than of U.S. population. https://www.pewresearch.org/fact-tank/2020/05/06/share-of-black-white-hispanic-americans-in-prison-2018-vs-2006/ft_20-05-05_imprisonmentrates_2a/

Porat, M.U. (1977). The information economy: Definition and measurement. *U.S. Government Printing Office.* https://eric.ed.gov/?id=ED142205

Ramos, S. (2021). Cultural political organizing: Rewriting the latinx "criminal/immigrant" narrative of surveillance. In E. Beck & L. Hutchinson Campos, *Privacy Matters:*

Conversations about Surveillance Within and Beyond the Classroom, (pp. 150-166). University Press of Colorado.

Ratzan, S.C., & Parker, R.M. (2000). Introduction. In C.R. Seldon, M. Zorn, S. Ratzan, & R.M. Parker (Eds.), *National Library of Medicine Current Bibliographies in Medicine: Health literacy* (pp. v–vii). NLM Pub. No. CBM 2000-1. Bethesda, MD: National Institutes of Health, U.S. Department of Health and Human Services. Retrieved January 16, 2023, from https://www.nlm.nih.gov/archive//20061214/pubs/cbm/hliteracy.pdf

Reilly, C. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition, 61*. https://doi.org/10.1016/j.compcom.2021.102652

Reissman, H. (2023, February 7). Americans don't understand what companies can do with their personal data—and that's a problem. *TechXplore*. https://techxplore.com/news/2023-02-americans-dont-companies-personal-dataand.html

Reyman, J. (2013). User data on the social web: Authorship, agency, and appropriation. *College English, 75*(5), 513–33.

Robertson, C. (2009). A documentary regime of verification: The emergence of the U.S. passport and the archival problematization of identity. *Cultural Studies, 23*(3), 329–354.

Rose, E.J. (2016). Design as advocacy: Using a human-centered approach to investigate the needs of vulnerable populations. *Journal of Technical Writing and Communication, 46*(4), 427-445. https://doi.org/10.1177/0047281616653494.

Ruti, M. (2017). *The ethics of opting out: Queer theory's defiant subjects.* NY: Columbia University Press.

Ryan, K.J., Meyers, N., & Jones, R. (2016). *Re-Thinking ethos: A feminist ecological approach to rhetoric.* Southern Illinois University Press.

Sa'di, A.H. (2012). Colonialism and surveillance. In K. Ball, K.D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies*, (p. 151). Routledge.

Sauer, B. (2003). *The rhetoric of risk: Technical communication in hazardous environments*. Routledge.

Savage, G., & Mattson, K. (2011). Perceptions of racial and ethnic diversity in technical communication programs. *Programmatic Perspectives, 3*(1), 5–57.

Scott, J.B. (2003). *Risky rhetoric: Aids and the cultural practices of HIV testing*. Southern Illinois University Press.

Scott, J.B., & Meloncon, L. (2018). Manifesting methodologies for the rhetoric of health & medicine. In L. Meloncon & J.B. Scott (Eds.), *Methodologies for the Rhetoric of Health & Medicine,* (pp. 1-23). New York: Routledge.

Scott, J.B., & Meloncon, L. (2019). RHM's relations and relationships. *Rhetoric of Health & Medicine, 2*(4), iii-x.

Segal, J.Z. (2005). *Heath and the rhetoric of medicine.* Carbondale, IL: Southern Illinois University Press.

Segal, J.Z. (2009). Rhetoric of health and medicine. In A. Lunsford et al. (Eds.), *The SAGE Handbook of Rhetorical Studies*, (pp. 227-246). Thousand Oaks, CA: SAGE.

Shephard, N. (2019, November 1). Surveillance intersectional: Historical continuities. *Feminism and Gender Democracy.* https://www.gwi-boell.de/en/2019/11/01/surveillance-intersectional-historical-continuities

Slack, J., Miller, D., & Doak, J. (1993). The technical communicator as author: Meaning, power, authority. *Journal of Business and Technical Communication, 7*(1), 12-36. https://doi.org/10.1177/1050651993007001002

Slack, J.D., & Wise, J.M. (2005). *Culture + technology: A primer.* New York, NY: Lang.

Smith, E.O. (2000). Points of reference in technical communication scholarship. *Technical Communication Quarterly, 9*(4), 427-453. https://doi.org/10.1080/10572250009364708

Smith, A. (2015). Not-seeing, state surveillance, settler colonialism, and gender violence. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 21-39). Durham and London: Duke University Press.

Steeves, V. (2012). Hide and seek: Surveillance of young people on the internet. In K. Ball, K.D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies,* (pp. 352–359). New York: Routledge.

Stone, G.C. (1979). Patient compliance and the role of the expert. *Journal of Social Issues, 35*, 34-59. https://doi.org/10.1111/j.1540-4560.1979.tb00788.x

Takayoshi, P., & Van Ittersum, D. (2018). The material, embodied practices of composing with technologies. In J. Alexander & J. Rhodes (Eds.) *The Routledge Handbook of Digital Writing and Rhetoric*, (pp. 84-94). Routledge.

Thales Group. (2022, January 27). Biometrics: definition, use cases, latest news. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Tschider, C. (2019). The consent myth: Improving choice for patients of the future. *Washington Law Review.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3171801.

Walby, K., & Anais, S. (2015). Research methods, institutional ethnography, and feminist surveillance studies. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 208-221). Durham and London: Duke University Press.

Walton, R. (2016). Supporting human dignity and human rights: A call to adopt the first principle of human-centered design. *Journal of Technical Writing and Communication, 46*(4), 402-426. doi:10.1177/0047281616653496

Walton, R., Moore, K., & Jones, N. (2019). *Technical communication after the social justice turn: Building coalitions for action.* Routledge.

Welch, N. (2008). *Living room: Teaching public writing in a privatized world.* Portsmouth: Boyton-Cook.

Welhausen, C.A., & Bivens, K.M. (2021). mHealth apps and usability: Using user-generated content to explore users' experiences with a civilian first responder app. *Technical Communication, 68*(3), 97–112.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality.* New York: The New Press.

Wilson, B., & Hayhurst, L. (2009). Digital activism: Neoliberalism, the internet, and sport for youth development. *Sociology of Sport Journal*, *26*(1), 155–81.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, *109*(1), 121–136.

Young, S. (2023). *Working through surveillance and technical communication: Concepts and connections.* SUNY Press.

Chapter 3

Methods and Introducing Interlocking Surveillance

In the previous chapter (Chapter 2), I introduced a literature review that focused on the intersection of surveillance studies and technical communication. Specifically, bridging these fields creates a foundation for situating how neonatal nurses define and perceive a specific surveillance technology, biometrics. Overall Chapter 2's review explores interdisciplinary contributions and situates the current conversation surrounding authentication and privacy to shape an argument of necessity. That is, to fully be able to intervene in design protocols, communication materials, and defining biometric technologies, it is *necessary* to return to the history of usage which contributes to charting such surveillant usage of biometrics present day.

The following sections discuss a methodology, interlocking surveillance, which bridges surveillance studies, technical communication, and feminist approaches to issues/sites of surveillance. This methodology is used to analyze data (in Chapter 4) from the methods: textual corpus analysis, screening survey (questionnaire), and interviews. The methods and methodological framework help to answer: What are neonatal nurses' experiences with biometric technology in healthcare? What is the tension between neonatal nurses' perceptions of biometric technology usage in healthcare institutions and the intention of creators of biometric technologies as deduced from the company language?

3.1 Introduction to Methodology: Interlocking Surveillance

Interlocking surveillance combines elements of the new surveillance and intersectionality to develop a framework that addresses sites of surveillance and their levels of awareness, advocacy, and transparency of normalized surveillant practices. This methodological framework

is useful in understanding surveillance tools and technologies through a feminist lens. Chapter 3.2 further states how the methodological framework grew out of explicitly feminist concerns.

The goal of the following methodological framework, interlocking surveillance, within rhetoric and composition, but more specifically the subfield of technical communication, is to make apparent and trace the history of surveillance. For example, tracing the history of surveillance "back to organized forms of state control such as slavery [and colonialism], the management of women's reproductive autonomy, the regulation of sexuality, and the institutionalized scrutiny of those living in poverty" (Dubrofsky & Magnet, 2015, p. 15). As outlined in Chapter 2, biometric technologies are a form of surveillance, and charting their histories is crucial to understanding how they are implemented in present day sites. The list of organized state control by Dubrofsky & Magnet (2015) are just a few of many examples of where interlocking surveillance incorporates principles of feminism to raise awareness, advocate, and push for more transparency of "normalized" surveillant practices. What follows is a breakdown of interlocking surveillance as a methodological framework, based on the literature compiled from feminist rhetoric, surveillance studies, and technical communication.

The framework of interlocking surveillance incorporates my definition of surveillance: the collection of both visible and invisible data/information derived from those being observed, suggesting an application of power over the observed audience, who are often not informed of such collection[33]; and an adopted definition of intersectionality originally coined by Kimberlé Crenshaw in 1989. Intersectionality[34] is defined by Crenshaw (1989) as, "a metaphor for

[33] Surveillance: the collection of both visible and invisible data/information derived from those being observed, suggesting an application of power over the observed audience, who are often not informed of such collection.
[34] Intersectionality: a metaphor for understanding the ways that multiple forms of inequality or disadvantage sometimes compound themselves and create obstacles that often are not understood among conventional ways of thinking (Crenshaw, 1989).

understanding the ways that multiple forms of inequality or disadvantage sometimes compound themselves and create obstacles that often are not understood among conventional ways of thinking" (p. 149). My definition of surveillance encompasses my understanding of biometric identification, or any identifier of the body that is collected and used for personal identification, by emphasizing that information collected from the body *can* be visible; however, oftentimes such parties involved are not informed of such collection. If bodies are informed, it is usually through agreeing of terms or "opting in" to usage without fully understanding (or choosing) what they are opting in to. Crenshaw (2013) wrote how one problem with identity politics is not that it "fails to transcend difference" but rather the "opposite-that it frequently conflates or ignores intragroup differences" (p. 93). Part of intersectionality informing interlocking surveillance is the complex combination of not just the violence enacted on Black women in particular, but also the ways in which new surveillance oppresses and imposes on *all* bodies including those historically excluded based on their surveilled identities. What's important here is that race and gender *do* intersect in shaping political, social, and structural aspects of being; however, interlocking surveillance as a methodology *also* considers disclosure (including politics of disclosure) of identities such as disability, sexuality, economic status, and so forth. Of course, Crenshaw does recognize class and sexuality as important in shaping experiences, especially for "women of color;" however, the takeaway is that there is a "need to account for multiple grounds of identity when considering how the social world is constructed" (2013, p. 95). Identity is and can be a site of resistance.

Scholars in technical communication have also positioned Crenshaw's work within their scholarship. For example, intersectionality is an understanding of oppressive structures as "intersecting, interlocking, and inseparable" (Walton, Moore, & Jones, 2019). Such structures

recognize situated and contextualized identities such as those influenced by race, gender, class, sexuality, and intersectionality is a response to feminist frameworks' failure to recognize "other seemingly discrete markers of identity that we can see societal injustice and violence enacted differently" (De Hertogh et al., 2019, p. 5). For example, Crenshaw's intersectionality focuses on the "differential imposition of power and state violence on" Black women (De Hertogh et al., 2019, p. 5). I see the intersection of principles of intersectionality and surveillance studies best described through what Crenshaw (2013) writes, "is not the existence of the categories, but rather the particular values attached to them, and the way those values foster and create social hierarchies" (p. 112). Surveillance tools and technologies reinforce categories and social hierarchies, and thus should be critically examined to understand how and why such surveillance tactics impact bodies based on characteristics.

Thus, to reiterate Dubrofsky and Magnet's (2015) call, the direction in which surveillance is headed will require resources that draw on an intersectional exploration of the ways in which forms of exclusion, discrimination, and sorting are built into the taken-for-granted norms that guide the monitoring process. Suppressed or overlooked histories of surveillance practices provide crucial guides for navigating this unfolding surveillance scape, in which all forms of monitoring are encompassed by the embrace of power. Calling attention to what has become "commonplace" or a "norm" within the United States helps shed light on what has become all too easy to overlook in the contemporary exercise of surveillance. Surveillance includes both invisible and visible forms, which often must be called attention to due to their increasing normalization.

I therefore categorize my methodological framework as an explicitly feminist framework of surveillance. Interlocking surveillance as a methodological framework emphasizes the

collection, coding, and analyzing of data in order to create units of information that "extrapolate themes" from the collected information (Blakeslee & Fleischer, 2019, p. 187). This study implements interlocking surveillance as a methodological framework that is applied to a multiple-method collection of qualitative information, helping to increase understanding (but not necessarily over-generalize discoveries to a larger population) (Glaser & Strauss, 1999). Such coding approaches will be discussed in detail in section 3.5.

The intention with utilizing aspects of intersectionality to contribute to the methodological framework of interlocking surveillance is to engage in critical analysis of interlocking as one component of intersectionality. Intersectionality has been appropriated by both popular media and white women scholars, neglecting to recognize that the origins of intersectionality began as a response to white women feminism (Flores Niemann, Gutiérrez y Muhs, & González, 2020). There has been a hegemonic "politeness" of academic culture that Flores Niemann, Gutiérrez y Muhs, and González (2020) call attention to. This politeness "serves to protect White fragility and perpetuate existing power relations" (Flores Niemann et al., 2020, p. 7). Because of the way academia cradles (and protects) White bodies, I especially want to be mindful of my utilization of *elements* of intersectionality due to my position as a white heterosexual cisgender woman. It's important to remember that our positionalities are not fixed. That is, "there are no single, fixed meanings, rather positionality is relational, historical, fluid, particular, situational, contradictory, intersectional" (Walton, Moore, & Jones, 2019, p. 65). Using the term *interlocking* as derived from Crenshaw's coinage of intersectionality shifts the focus on societal injustice and violence enacted differently on women of color, to further recognizing that our interlocking and situated identities based on race, class, disability, sexuality,

economic status, and so forth oppress people in ways that are furthered by state sanctioned surveillance and lateral surveillance.

This methodological framework also includes elements of Lyon's (2007) criteria for viewing sites of surveillance. Since healthcare is a site of surveillance, interlocking surveillance is a framework that may be applied to any site of surveillance. Surveillance is not always occurring through technological means; therefore, some aspects of the framework may not be applicable to every site. Adding to the feminist emphasis of amplification through awareness, advocacy, and transparency more generally speaking, these goals include analyzing sites for their justification for standardization, technology use, categorization of people, level of informedness, and urgency or efficiency (Lyon, 2007, p. 26-27). Interlocking surveillance, as it applies to situated sites of surveillance, certainly can recognize and discuss the ways societal injustices are enacted on women of color, while also calling attention to normalized societal injustices that are enacted on other bodies and are also insidious in nature, especially through the ways categorization exists as part of the heuristic. I do not want to appropriate intersectionality, and instead seek to borrow conceptually from it. This methodological framework thus centers the aspect of intersectionality that notices identities as interlocking; however, this framework specifically is used to call attention to the ways interlocking identities are disproportionately affected by surveillance. Scholars who use interlocking surveillance may approach understanding(s) through intersectional listening, for example. Walton, Moore, and Jones (2019) explain that intersectional listening "invites a multiplicity of marginalized perspectives and identities to be centered and acknowledged, without demanding that they coincide, match, or align" (p. 74). The following sections define what feminism means to me and this methodological framework, as well as further implications of the methodology.

3.2 Further Situating Feminism in Interlocking Surveillance

Central to exploring interlocking surveillance is also my definition of feminism[35], which emphasizes care and collaboration through seeking to eliminate the "oppression of *all* [emphasis added] people who are marginalized by the dominant culture including but not limited to people of color, people with disabilities, people of different ages and socioeconomic classes," and members of the LGBTQIA+ community (Foss, Foss, & Griffin, 1999, p. 2). My adopted definition of feminism is important because it centers on interlocking approaches to amplifying historically excluded voices; voices that are often ignored or devalued. This definition of feminism suggests the treatment of all humans in accordance with such feminist values as "respect, caring, reciprocity, self-determination, and interconnection" (Foss, Foss, & Griffin, 1999, p. 2). Further, my definition of surveillance and feminism combines to establish interlocking surveillance as a methodological framework that emphasizes awareness, transparency, and advocacy; that is, establishing an increased awareness of our invisible/visible identities that are surveilled, and creating more transparent efforts by collaborating with public audiences to understand how information/data is collected, stored, and distributed from those who engage in top-down surveillance. Awareness, advocacy, and transparency centers on feminist values of rhetorical listening (Glenn, 2018), coalition-building, and researching more deeply the models of protection that currently exist in our globalized world (Royster & Kirsch, 2012) such as the regulations implemented by the European Union (the General Data Protection Regulation) to advocate for similar (yet increased) protection in the United States. Further, this

[35] Feminism: eliminating the "oppression of all people who are marginalized by the dominant culture including but not limited to people of color, people with disabilities, people of different ages and socioeconomic classes," and members of the LGBTQIA+ community (Foss, Foss, & Griffin, 1999, p. 2).

general framework at the intersection of feminist and surveillance studies foregrounds concerns such as reciprocity, representation, and accessibility (see Garland-Thomson, 2011).

Through unpacking the ways our dominant ideologies have influenced systems in the United States, we can collaborate with the community in feminist ways (and localized, see Agboka, 2013). My methodological framework emphasizes principles of feminism as they relate to a "practice of listening deeply and actively;" setting aside assumptions or what Royster & Kirsch (2012) refer to as strategic contemplation; and amplifying voices by emphasizing inclusivity, participation, and recursion through deep listening, flexibility, and respect (p. 85-89). Since interlocking surveillance may be applied to different sites of surveillance, one current example is Novotny's (2015) article about legislation attempts to regulate health decisions of female bodies. Novotny (2015) calls for more explicit feminist methods to resist such anti-feminist legislation to be developed; in this way, interlocking surveillance as applied to healthcare responds to Novotny's (2015) call for explicitly feminist interventions in health regulation. Interlocking surveillance as a methodological framework that can explicitly address the regulation that continues to reinforce domination and oppress those through Young's (1990) five faces of oppression (marginalization, exploitation, powerlessness, violence, and cultural imperialism). As state and federal legislation continues to regulate reproductive health especially through biometric technologies, for example, the field of technical communication must continue to develop ways to facilitate stakeholder participation in policymaking practices to address normalized surveillance. As I'll discuss in Chapter 5, coalitional approaches are crucial to change, including policymaking practices. For example, as outlined in HIPAA and reaffirmed by the Department of Health and Human Services (DHHS), "any third-party tools installed should also have their privacy policies reviewed by a hospital's legal department **in conjunction with**

[emphasis added] a patient representative to ensure that the policies meet the hospital's legal and ethical obligations to protect patient privacy" (Davis, 2022). This example displays how in the context of healthcare, participatory approaches to legal and ethical guidelines *are* outlined, though there are questions about if such guidelines are *enforced* or interpreted in the same ways. For example, DHHS states that the third-party tools "should" be reviewed by the hospital's legal department, and "in conjunction with" a patient representative: what are the criteria for "ethical" *and* "legal" obligations? Is a patient representative always present? If we know that biometric technologies do not protect patient privacy, then how do legal departments "approve" or classify biometrics as a tool (and subsequent policy) that protects patients? One only needs to read the Privacy Policies and Terms and Conditions.

3.3 Implications of Interlocking Surveillance as a Methodological Framework

Though I am specifically focusing on the United States, there is of course influence from countries across the world on technological advances: both for surveillance and biometric measures. Modern-day surveillance, as well as historical implications of surveillance, have much to do with seeing and being seen. Critically examining who is visible and who is invisible is an excellent example of interlocking surveillance in practice. Based in feminist methodologies, it may be determined that since "Western" thought and societies have been created by white cisgender men, a male-dominated viewpoint shapes not only the top-down or lateral surveillance[36] and control of "other" bodies, but also the history behind every form of data collection. Because surveillance is locally contextualized—despite generalizations that are made across cultures about who surveils and is surveilled—interlocking surveillance assists with understanding and making visible what may be invisible. This approach centers sousveillance or

[36] Lateral surveillance: peer-to-peer surveillance.

watching the watchers; a shift from individual accountability and transparency to a deep interrogation of the surveillance practices and power relations executed by states or corporations (systemic surveillance).

A way to develop a critical consciousness of surveillance practices may be through what Marx (1998) calls "the new surveillance[37]." New surveillance is composed of technologies, practices, and forms of surveillance that have varying degrees of shared characteristics (Browne, 2015, p. 15). There are 10 characteristics of new surveillance according to Marx; however, in a later article (2002), Marx charts 28 dimensions that highlight the differences between the *new* and *traditional* surveillance and "offer a way to capture major sources of variation relevant to contemporary social, ethical and policy considerations" (p. 8). Some of the characteristics that Marx (1998) outlines as part of "new surveillance" inform considerations in the heuristic developed for interlocking surveillance: distance and physical barriers; how data is shared, stored, and aggregated; consent with data collection, especially with biometric tagging; types of surveillance, such as self-surveillance and justifications for use; and the interiority of surveillance and the body[38].

With these developments regarding the scope and scale of surveillance, Marx (1998) has suggested that perhaps we have become a "maximum-security society." Considering the origins of surveillance and biometric identification with "maximum-security" prisons and law enforcement, it is helpful to understand this type of surveillance as pervading our current everyday life. For example, Staples calls "participatory monitoring" a way of understanding how people, objects, and things come to be monitored in remote, routinized, and continuous ways

[37] Not to be confused with an "old" surveillance.

[38] Marx (1998) refers to technological innovations that have made for a more intensive and interiorizing surveillance where the body is concerned, for example, with voice analysis that is said to measure stress as a way to differentiate between lies and truths.

(Browne, 2015, p. 16). Staples gives an example of electronic "ankle bracelets as a requirement of house arrest or car ignitions fitted with breathalyzers that measure a driver's breath alcohol content before the engine can be started" (2014, p. 48; Browne, 2015, p. 16). Browne (2015) writes how people who are subject to such monitoring as described above are also tasked with "actively participating in their own confinement by partnering, in a way, with the overseeing body or agency in the check for violations and infractions" (p. 16). Though certain groups of people such as those who are Black, Indigenous, LGBTQIA+, and disabled tend to categorically be hyper-surveilled more than others, it is crucial to notice the interlocking identities of such individuals and how certain biometric identifiers are privileged for surveillance over others.

3.3a Awareness

When considering "awareness," I adopt Lyon's (2007) site of surveillance framework as an intersection between feminist methodologies to better inform interlocking surveillance. This means that part of the goal of company awareness is analyzing how the companies respond (or don't) to justification for standardization, technology use, categorization of people, level of informedness, and urgency or efficiency.

I argue that interlocking surveillance includes the interconnectedness of the ways in which bodies are surveilled in different contexts (Shivers-McNair, et al., 2019). This includes the hyper-surveillance of those who are historically excluded based on race, gender, sexuality, dis/ability, and so on. The intention with bringing awareness to bodies who are hyper-surveilled is because I am focusing on biometric technologies. Since biometric technologies are a personal identifier and/or extension of the body, some bodies are hyper-surveilled more than others. From my textual corpus and participant responses (the questionnaire and interviews), technical communicators should consider such impacts of hyper-surveillance. In this way, interlocking

surveillance does not just rely on how technology practices impact bodies, but primarily interlocking surveillance focuses on the contexts in which bodies are surveilled and their implications. For example, this may mean analyzing biometric technologies through digital technology such as facial recognition software or fingerprinting (Gates, 2011), but also through invisible means that have been normalized, e.g., surveillance that isn't solely digital, such as vaccination IDs, passports, driver's licenses, birth certificates, and social security cards.

As I've argued before (Banville & Sugg, 2021), part of recognizing roles, or positionality within a site of surveillance, comes from understanding/unpacking actions that are interpreted as privileged. For example, we (Banville & Sugg, 2021) focused specifically on instructors in higher education: some markings of privilege in instructor responses followed the assumption that surveillance, or monitoring in the classroom, "doesn't apply to me" or that instructors have "nothing to hide." This sentiment has been discussed in previous scholarship (Adorjan & Ricciardelli, 2019); however, it displays an example of privilege. A position of privilege means, "not just having power but having more power than certain other groups of people have" (Walton, Moore, & Jones, 2019). That is, practitioners or scholars may write that they have "nothing to hide" and are therefore unbothered by surveillance technologies because they are not part of marginalized groups who are often surveilled. My hypothesis is that the more people are aware of the ways in which they are becoming numbers to be mined and profited from, the less the opinion of "I have nothing to hide" will pervade throughout society. Research studies have shown that those who have "nothing to hide," truly are unaware of all the ways they are being observed; and technical communicators' roles as knowledge-makers, creators, and instructors is to communicate with audiences regarding how surveillance impacts their daily lives. However, it is also important to note that the "nothing to hide" conversation is much more complex than

simply “not knowing.” Another aspect of the “nothing to hide” argument is rooted in biopolitics: Beauchamp argues how state identification hinges on, for example, transgender individuals’ “performances of legibility” and legitimization through official documentation to prove that they are who they say they are, and also don’t have anything to hide (2019, p. 49). It is first and foremost the goal to communicate such information, as we utilize interlocking surveillance as a methodological framework to determine what bodies are impacted, how, and why. Further, in this study, rhetoric of health and medicine scholars are uniquely positioned to, “critically examine how our methodological choices affect how we gather and understand health data and—more important—the impact that process can have on the communities we study” (De Hertogh, 2018, p. 9). This is certainly part of determining awareness.

3.3b Advocacy

Awareness is linked to advocacy as another aspect of interlocking surveillance’s methodological framework. Rhetoric, writing, and professional communication is a growing field where programs, broadly speaking, explore writing and communication practices. Professional communication programs prepare students for careers as “writers, editors, document designers, presentation developers, and information managers in technology industries, other businesses, government, and nonprofit organizations” (Kynell-Hunt & Savage, 2004, p. 89). Due to the wide range of careers that students and technical communicators are involved in, interlocking surveillance may be applied as a framework in rhetoric and composition to show how surveillance is not “universally and uniformly applied to all human bodies and, furthermore, monitoring occurs with different degrees of specificity and intention” (Dubrofsky & Magnet, 2015, p. 59; see also Casper & Moore, 2009). Technical communicators are in unique positions to analyze and inform audiences of the varying degrees that surveillance is applied to bodies

using interlocking surveillance as a framework. Advocacy work is expanded in both Chapter 5, as a takeaway, and Chapter 6, within the classroom.

Colonialism and surveillance capitalism (Zuboff, 2019) play a large role in advocacy within the methodological framework because the United States is built off "white supremacist capitalist patriarchal" values (hooks, 1994, p. 26). Advocacy work means directly addressing the surveillance systems and technologies origins. Foucault (1995) emphasized how the state "produces the docile bodies essential to its functioning," and state scrutiny occurs through not just external forms such as policing, but also internal "systems of discipline by which people come to police themselves" (Dubrofsky & Magnet, 2015, p. 2). As Agboka (2013) clarified, "'current approaches' to both researching and designing technologies are [often] motivated by modernist ideologies…whose history is tied to the colonial project" (p. 298). This framing helps in considering surveillance capabilities and how they do not account for *who* created the technologies, *why,* and *how*. Reilly (2021) mentions Zuboff's (2019) description of the "asymmetrical power differential between data-collecting corporations and individuals as completely unprecedented and, as such, invisible to users by design: 'surveillance capitalists know everything about us, whereas their operations are designed to be unknowable to us'" (p. 4). Advocacy work is defined by the ways in which corporations surveil through my heuristic for determining their justification for standardization, technology use, categorization of people, level of informedness, and urgency or efficiency.

3.3c Transparency

Transparency certainly does not always lead to accountability or changes in laws or policies (see Brucato, 2015). And sure, increased transparency is often an initial impulse to want to make visible the "normalized" and "everyday" surveillance that is embedded in

systems/structures in order to create change. It would be amiss to state that transparency benefits everyone. Making visible the invisible doesn't always help the very people who are most impacted by surveillance technologies: I state this at the forefront because every example I mention of transparency, also includes the invisible weighing of impact. A feminist approach is concerned with getting away from neutral definitions of surveillance and putting critique first to continually point out "how ruling relations are enabled by the texts and classifications that make up surveillance" (Walby & Anais, 2015, p. 220). In this explicitly feminist framework, transparency may be understood through the level in which corporations and organizations are direct about their justification for standardization, technology use, categorization of people, level of informedness, and urgency or efficiency. As Monahan (2022) writes, "transparency serves as a master protocol, such that opacity is anathema," especially in the context of pervasive and ubiquitous surveillance systems predicated upon "datafication" and hyper-surveillance (p. 14). To build off transparency as a concern (and goal), interlocking surveillance seeks to challenge the current systems that the United States has been built on. Central to interlocking surveillance is a focus on what is often overlooked as an observation and/or monitoring practice. This can range from genetic screening, invasive body-monitoring technologies (Frost & Haas, 2017), birth certificates (Moore & Currah, 2015), security screening (Gates, 2011; Kerr et al., 2009), and the other seemingly "normal" or "everyday" forms of data collection, information collection, and observation, that are in/visible forms of surveillance.

Transparency in healthcare may manifest as informed consent (for all stakeholders), as well as through communication materials that are accessible to users. The complexities surrounding informed consent and communication tactics are unpacked in more depth throughout the data analysis in Chapter 4. To achieve transparency requires an acknowledgment

and reframing of the ways informed consent *is* surveillance. The illusion of choice extends to informed consent: in healthcare, there often isn't communication about ways to opt out, if there even are any. Because of the precarious nature of the healthcare system, and the unspoken trust that is placed in "expert" hands, informed consent documents an instance of patient acquiescence, especially at times when they may be uncertain about what they're agreeing to. Informed consent is part of this *level of informedness*, which shifts depending on the context. In this study, for example, levels of informedness would code neonatal nurses in interviews explaining that they verbally ask for consent from patients to use biometric technology as limited informed consent; this will be discussed further in section (4.4). In this example, nurses may be informed about how to *use* the biometric technology, but they may not be informed about the *implications* of use (such as data collection and distribution). Further, patients could be informed verbally by the nurse, but this is consenting to the likely limited or vague information shared by the nurse. There is also the added complexity of knowledge base: how do you ask a question, when you're unsure of what it is you really want to know? Trusting in experts to protect *and* inform is truly where intervention with informed consent needs to occur: healthcare providers need to overview precisely what patients are consenting to, and potential implications and ramifications (this is what transparency could look like).

Informed consent also quickly expands to include issues of design, usability, and agency/power, thus resulting in what Edbauer (2005) and more recently Jensen (2015) would refer to as an emergence of a rhetorical ecology[39]. Since the site of surveillance (healthcare) is fluid and differentiates based on context/location, my methodological framework is a heuristic used for guidance to critically examine the site. Increased awareness, advocacy, and transparency

[39] Rhetorical ecology: conceptualizes rhetoric as fluid and situational as texts circulate through publics, changing discourses, and contextual situation, considering factors beyond audience, exigence, and constraints.

are therefore goals, and overall takeaways vary depending on specific factors. The situatedness of the site does include generalizations about the healthcare system based on applying the heuristic to neonatal nurse responses and the textual corpus.

3.4 Methods: Corpus Analysis, Questionnaire, and Interviews

This section overviews the trajectory of the study, including some of the processes leading to the final implementation. I will first document preliminary and pilot study data that was involved in decision-making for the final study.

To better inform my methods section, I interviewed Consultant A[40]. Consultant A works for VHB a civil engineering corporation whose goal, according to their website, is to help

> improve mobility, enhance communities, build resilience, and contribute to economic vitality. Our holistic problem-solving philosophy is ingrained in all that we do, and each project considers environmental, social, and economic factors that result in sustainable solutions. VHB collaboratively applies technical skills anchored in this philosophy to deliver lasting results that help communities thrive for generations to come.

During this meeting with Consultant A, I asked them about their day-to-day role, and how the company keeps track of employee information. This meeting was in October of 2021, after I passed my comprehensive exams and was in the process of brainstorming a dissertation idea. I was specifically curious if the company educated or communicated with their employees about privacy. Consultant A claimed that employees were aware of what directors have access to; even so, Consultant A stated that 40% of employees (including directors) have access to managing the dashboard of employees. This means that most employees know that *directors* have access to their information, but not necessarily other parties at the company[41]. The dashboard includes access to employee business or personal cell phone numbers, when their last

[40] Name and title redacted for anonymity.
[41] Consultant A did note that employees are communicated with about who has access to employee information but did not elaborate on all stakeholders involved.

salary review was and salary changes over time, vacation time and sick time is available, collected vaccination and COVID-19 status from employees, and much more.

Consultant A discussed that within the company, in order to inform employees of the importance of security (let's not confuse this with privacy), there are mandatory phishing tests for security and training. Anyone who fails needs to do training and video, which then gets sent to the manager (who has access to a dashboard displaying all employees who are passing and failing). There is much more information that I learned from my meeting with Consultant A, including IT's ability to remove unused software, global map and travel access, collection of information for new employee hires, email scanning, and more. What I would like to focus on from this meeting is how the information presented informs my chosen methods and direction of study.

What I found out from Consultant A confirmed my suspicions: like most technology, nearly every amount of data about a person is logged, though companies claim that they do "not have access to all of it." Information is saved for efficiency; that is, saved chats and threads on Microsoft Teams for the purposes of projects and collaboration. If there is an issue with a client, or an employee, then records of data may be accessed. What I was *initially* curious about were the ethical implications of collecting employee information, and if employees are informed about such collection and/or if their employment is contingent on opting into collection of information (which, it's hard to say there's an opt in when there really isn't an opt out). The answer? The company was looking to host informational "lunch and learns" to talk through the company policies to better understand topics such as security, best practices, and implications for personal life (for example, not using the same password). Especially with the move from the office to

home during the COVID-19 pandemic, the lines have increasingly blurred between work and home.

The conversation with Consultant A, though early in my brainstorming phase, proved informative. I then began to wonder about the following questions: How is biometric identification discussed with employees? Are there increased "security" measures to confirm the identity of employees now that they are out of the office (re: COVID-19 pandemic)? How do biometric technologies influence disciplinary regulation within the workplace? Are there ways that employees are biometrically monitored or observed—how? What biometric information does IT have access to, and are employees aware that such information is collected? What about third-party usage? These questions, though they informed a "professional workplace" as a site of surveillance, have now transitioned to focusing on "healthcare" as the site of surveillance. Not only did my conversation with Consultant A remind me that healthcare *is* a professional workplace, but I decided that since there was a wider range of biometric technology being implemented in healthcare, this would be a prime site to study. Consultant A's conversation with me led to the realization that I would have access to few biometric solutions, such as fingerprinting, for data collection and analysis. Furthermore, healthcare is the leading sector of usage of biometric solutions. The list of questions and conversation with Consultant A quickly shifted from wondering about privacy in the professional workplace (broadly defined), to narrowing in on the healthcare sector. I was especially interested in localizing my efforts and takeaways. Because of this, I contacted the head of hiring at Vidant Medical Center (now ECU Health), located in Greenville, NC. The medical center serves most of eastern North Carolina, and I thought it would be beneficial considering the influence and increased usage of biometric technologies in healthcare to explore this site of surveillance (at the time of the study, up 40%

from the previous year). In particular, I wanted to focus on the people using the technologies in their day-to-day roles. I was still able to work with nurses in my study; neonatal nurses to be specific. I was not able to collaborate with Vidant Medical Center; herein lies the challenge with community-engagement, as outlined in 3.4a.

My research questions are best answered through textual corpus analysis (see 3.4b and 3.4c) of biometric company materials (geared towards corporations seeking biometric capabilities within their companies), screening surveys of neonatal nurses throughout the United States (see 3.4d), and interviews (see 3.4e) to expand upon survey data. The research question(s) are as follows: How do healthcare professionals (specifically neonatal nurses) define biometric technologies? What are neonatal nurses' perceptions of biometric technologies?

The methods were chosen specifically because of the ways in which they inform and build off one another:

- The textual corpus contextualized *how* companies are understanding and communicating their biometric solutions.
- The questionnaires were needed to collect a large amount of data showcasing *how* neonatal nurses understood (through defining) biometrics, as well as *what* technologies they were using.
- and lastly, the interviews build on the questionnaire and corpus to dive further into understanding the connections between how neonatal nurses understand their *role*, and how their role informs how they *communicate* about biometric technologies with their patients.

Further, I used my methodological framework of interlocking surveillance to analyze the collected data, determined by how the companies who build biometric technologies respond (or

don't) to justification for standardization, technology use, categorization of people, level of informedness, and urgency or efficiency. The questionnaire asks neonatal nurses their perceptions about biometrics, generally speaking, while my textual corpus looks at companies who build the tools and how they communicate to potential purchasers about such materials. I coded the corpus data by first categorizing the collected texts by biometric solutions: voice, facial, and fingerprinting. These solutions were determined by the popularity of technology used by neonatal nurses in the screening surveys. The questionnaire assisted in collecting information from neonatal nurses in the United States, further contributing to understandings of personal information, privacy, biometric technologies, health, and the role a technical communicator plays at the intersection of surveillance and decision-making protocols. The interviews provided an opportunity to further discuss takeaways and offer a chance to localize conclusions and analysis based on the participants and their roles. In total for the entire study, I collected:

- 15 websites for the corpus,
- 118 survey responses (Report 1),
- 28 survey responses (Report 2), and
- 10 interview participants.

It is important to note that the total number of responses per question varied on the questionnaire/screening survey (Report 1 and 2).

3.4a The Challenges with Community-Engagement

Initially, I planned the study to focus on and contribute to decision-making protocols for purchasers (healthcare institutions) who utilize biometrics within the workplace. My curiosity stemmed from my conversation with Consultant A, and so I was especially interested in encouraging professionals to think about the tools they are creating/designing and their

implications. I wanted to understand how employees who work for biometric technology companies understand the tools the company is communicating and building. How does this affect their role? Lives? Does the company implement the technologies they make on its employees? As Katz (2002) writes, after choosing a site of study, researchers then have to "convince the organization to grant permission for the study" (p. 27). And it sure was a hurdle to convince.

Herein lies my community-engagement problem: it is so difficult and time consuming. I "have" all of the resources and access in the world to people in higher education, but when it comes time to access the "alt-academic" community, it's challenging. I found that with the groups I was interested in contacting, such as the nurses at Vidant, there were either multiple channels of permissions that I needed to gather, or the sheer inability of finding contact information for the person who would give the approval. There was also a significant financial barrier. As a graduate student, I was faced with the hurdle of purchasing memberships and/or paying for screening survey distribution in order to access the participants that I wanted to gather information from. Fortunately, I had applied for and received a grant to pay my participants for their time; but this is a huge hurdle for students seeking to create meaningful and sustainable engagement with the local community. The department at ECU was willing to support any screening survey distribution, so this assisted in accessing populations outside of social media and word of mouth.

Academics engage in lots of really fantastic community research and engagement, but I still see a disconnect between the circles we write to and for, and the work we're doing. As Ceccarelli (2013) writes, "for the most part, we fail to creatively project ourselves onto horizons of possibility as forces of change at all. In articles written to each other, we find ourselves

preaching to the choir, with only passing mention of our obligation to reach out to the very audiences who are empowered to make the alterations to practice that our critical findings recommend" (p. 1). I believe that privacy and surveillance, especially in thinking about several sites of surveillance such as healthcare, is relevant to many people; however, accessing these people to survey or interview (or even send an email to) is a barrier. This is an area worth noting and exploring as academics: how can we collaborate *with* and research *with* the community, people who can be and are often the most impacted by the research done in higher education?

One idea I was considering was two discrete screening surveys, documenting variable changes. I didn't end up doing this for the survey distribution because I ended up receiving an influx of interested interview participants prior to the second-round distribution of the survey. I was contacted by the Association of Women's Health, Obstetric and Neonatal Nursing (AWHONN) who on October 21, 2022, determined that they needed more information prior to distributing my survey. AWHONN required the following: 1) a draft of my post; 2) copy of IRB approval or exemption; 3) a study summary; and 4) a link to my survey/questionnaire. These items were reviewed by an AWHONN supervisor for approval. Upon approval, AWHONN asked for criteria to focus on a select part of the membership: factors such as state, clinical focus, workplace setting, etc., to refine the number of members that meet these criteria. This organization required $375 per 1000 nurses contacted. The expected return rate was 3%, with my final count of 28 nurse questionnaire responses[42]. October 21 was the same day I reposted the survey on my personal Twitter. Once approved on November 16, 2022, AWHONN sent the screening survey to their networks on November 23 and December 7 of 2022. After both

[42] Responses did vary per question.

distributions, I contacted four interviewees to schedule an interview. No nurses from AWHONN responded for an interview.

3.4b Corpus Analysis

There are currently over 400 companies (websites) that identify as biometric companies in the United States; I used this repository to categorize the list of websites that identify as hosting biometric information into different themes focused on different components of biometric identification. This study utilizes textual corpus analysis as a means to analyze the language used by biometric corporations in communication materials for potential users. I have included a list of websites in the following section (3.4c Defining the Corpus Genre) that compiled a list of companies that create biometric solutions. Once I categorized the websites by their main focus (fingerprinting, facial recognition, and voice recognition), I chose five companies per category to apply my methodological framework to. Gathering five companies based in the United States per biometric solution offered 15 different textual corpi to analyze. This provided more of a holistic insight into, and representation of the ways biometric solutions are communicated to potential users and consumers. The five companies per category (three categories: voice, facial, fingerprinting) give insights into privacy, health, and wellness, as well as defining biometric identification/technology.

From the screening questionnaires, neonatal nurses cited biometrics solutions such as facial recognition, voice recognition, and fingerprinting as the tools most often used in their roles. This aligns with popular consumer data. For example, Spiceworks, a professional network for people in the IT industry, stated that nearly 90% of businesses will use biometric authentication by 2020, up from 62% in 2018 (Tsai, 2018). This figure has not been updated based on the original study. Fingerprint scanning is currently the most common type of biometric

authentication: 57% of organizations use it. Far fewer, just 14%, use facial recognition (Tsai, 2018). According to Statista, in 2022, the digital identity solutions market (of which biometric technology is a major component) was valued at 28 billion U.S. dollars with a forecast of exceeding 70 billion U.S. dollars by 2027 (Sava, 2022). Because of the data collected from the neonatal nurses, I created a corpus of text based on Biometric Update[43] that documents major biometric solutions.

For example, security firm BioCatch provides tools for companies to "learn employees' digital behavior and identify when an unauthorized person is trying to access information" (Larson, 2018). Companies can add BioCatch software to apps and websites. It runs in the background to build a 'behavior profile' of a user, and "learns activities like how someone holds the phone, whether they type with one or two hands, and how they scroll or toggle between screens" (Larson, 2018). To reiterate some of my general guiding questions, I've referred to how recent biometric identification technologies are positioned as a necessity and for effectiveness, but who is asking for such? What is the apparent need? For safety or security? From whom? Employees, such as neonatal nurses, must make a choice between being employed or violating their privacy and the privacy of their patients. What does privacy or personal information mean to those who are employed by companies utilizing biometric authentication?

I view all forms of biometric identification and subsequent collection as surveillance. The predetermined categories I focused on were voice recognition, facial recognition, and fingerprinting. To cross-check the companies for usage in the United States, I referred to Security Informed[44].

[43] https://www.biometricupdate.com/biometric-companies
[44] https://www.securityinformed.com/companies/biometrics-united-states-of-america/directory.html

For the purposes of this project, along with the screening survey, or questionnaire, and interview collection, I collected 15 websites focused on the three biometric solutions: voice, facial, and fingerprinting. By doing this, I found general thematic patterns that are further supported with the information from the screening surveys and interviews which are discussed in Chapter 4. I am aware that despite utilizing the same corpus for analysis, the patterns can provide an infinite number of models with varying numbers of topics. Pääkkönen writes how researchers tend to decide what version to report "based not on something inherent to the text or the model, but based on whether they have something to say about it" (Licastro & Miller, 2021, p. 15). So, it is likely that some potential results in Chapter 4 could be overstated.

3.4c Defining the Corpus Genre

The Terms of Service (TOS) and the End-User Licensing Agreement (EULA) are examples of the few "static" texts that were collected for my corpus and analysis. Part of my method of collecting a corpus of texts is redefining my own genre of materials biometric companies share with purchasers (in this case, the healthcare institutions). Another part of the corpus is listed in the coming pages, which includes genres such as the communication materials (on the website), social media posts, and privacy policies. TOS and EULAs are not only my static texts because of their boilerplate language, but because of their similarities no matter the company. The "corpus genre" that I created focuses on a combination of documents that showcase how biometric companies communicate information about their technologies. Who are they for, and who do they not include? How does the biometric technology benefit people? What's the intended use in the workplace? The corpus connects to the population surveyed and interviewed because the language included in guides and training materials for nurses is based on the communication materials from the biometric solution companies. Neonatal nurses elaborated

on the ways biometric technologies were *justified* to them through training materials in the healthcare settings, which further informed how nurses communicate about biometrics to their patients.

I specifically looked for materials that communicate what the biometric solution is, why purchasers (such as the hospital) would contract the company for the solution, and how the company discusses topics such as privacy, security, health, surveillance, and use in the workplace. In these documents, I've ascertained how biometric identification companies discuss their privacy and data collection for consumers or corporations that are interested in a third-party collecting identifiable information (such as the healthcare institution). This would contribute to understanding the "ethics of opting out" and informed consent, or rather the illusion of choice. In order to be employed, receive care/treatment, or even partake in society, you must "agree" to terms. There are ethical ramifications related to the illusion that choice and privacy are a given. There is often a moral, ethical, and political dilemma between choosing to be a part of society (or in my study, being employed or a patient) or submitting oneself to violation of privacy. This textual corpus will be analyzed in Chapter 4.

What follows after an example from the textual corpus is a table (Table 1: Biometric Solution, Company, and Example Texts Collected) with the type of biometric solution, the company name, and the texts collected from the website. After the table, there is a more in-depth discussion of "about" the company and how I chose or found the specific companies from BiometricUpdate. The texts were collected based on my framework of interlocking surveillance. I searched websites for what I considered the company to communicate intended purpose of technology, justification of standardization, categorizing of people (as they relate to demographics and predetermined social stereotyping and hierarchies), levels of informedness

(that users would determine from the ways the company was transparent about their practices), and discussions of efficiency/urgency.

To give an idea of what the textual corpus "looks" like, the following is an example from uAttend, a fingerprinting company.

Product Images/Descriptions: Photos Taken 2/22/2023.



Figure 2: uAttend Cloud Software Page

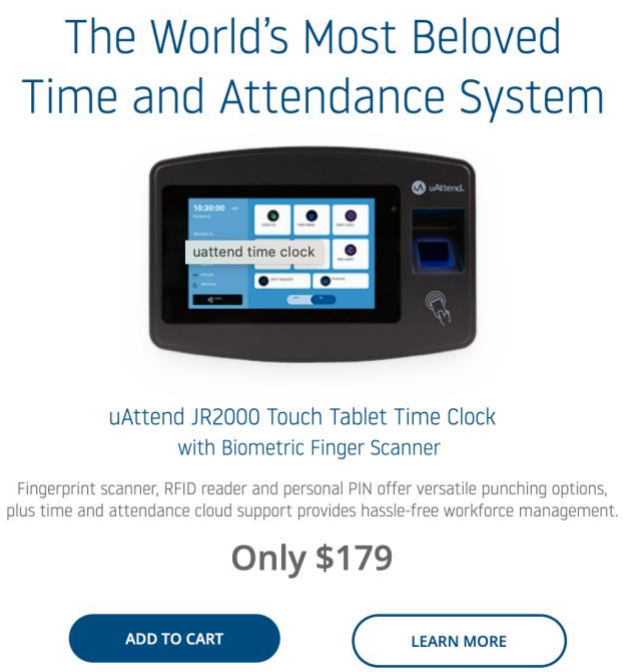


Figure 3: uAttend Shop, Touch Tablet Time Clock

About Page (located in the subsequent section - 3.4c iii.)

Biometric Data Policy

This is fairly lengthy, and I pulled only specific quotes as they related to the methodological framework. The Data Policy is divided into sections such as Definitions; Biometric Data Disclosure and Authorization; Retention Schedule; and Data Storage.

Privacy Policy

This is separate from the Biometric Data Policy, and includes the following sections: What Type of Information We Collect; How We Use the Information Collected; How We Use the Do Not Track Option; What We Share of Information Collected; Access to personal Information; How We Link to Other Websites; How We Handle Security of Personal Information; Privacy Notice for California Residents (CCPA); **Definitions**; Use of Personal Information; Sharing Personal Information; **Your Rights and Choices**; Access to Specific Information and Data Portability Rights; Deletion Request Rights; Exercising Access, Data Portability, and Deletion Rights; Response Timing and Format; Non-Discrimination; Who Can Use Our Website, Cloud App or Mobile App; **How Users Can opt Out;** Onward Transfers; Privacy Shield Framework(s); Privacy Shield Recourse; and How to Contact Us.

Workwell collects the following categories of Personal Information from consumers:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some Personal Information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	YES
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	NO
G. Geolocation data.	Physical location or movements.	YES
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	YES
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO
K. Inferences drawn from other Personal Information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Figure 4: Workwell (uAttend) Privacy Policy, captured 2/22/2023.

Workwell gathers Personal Information from the following categories of sources:

- Directly from our clients or their authorized representatives.
- Indirectly from our clients or their authorized representatives.
- Directly and indirectly from activity on our websites.
- From third parties that interact with us in connection with the services Workwell performs.

Disclaimers

Workwell is not advertising its products for use in the medical industry or for medical purposes. Our products are not intended to diagnose or exclude contagions such as COVID-19, SARS, or any other medical condition and should not be used as such. Our products are intended to serve as a first-line filter by assisting an organization and its employees in identifying those employees who may have an elevated body temperature. While our products may archive readings for reporting and audit purposes, it is solely the responsibility of the organization to communicate the use of the information to its employees, to obtain any necessary consent from its employees and to determine how the information is used. The organization should not rely solely on our products for making such a determination. Various environmental and methodological factors can impact thermal imaging; therefore, the readings from our products should not be relied upon as the sole determinant of a person’s body temperature. Competent medical advice and

further checks should be sought if there are concerns regarding an employee's health or possible illness. Workwell hereby disclaims all liability with respect to the conditions and limitations described in this paragraph.

Testimonials

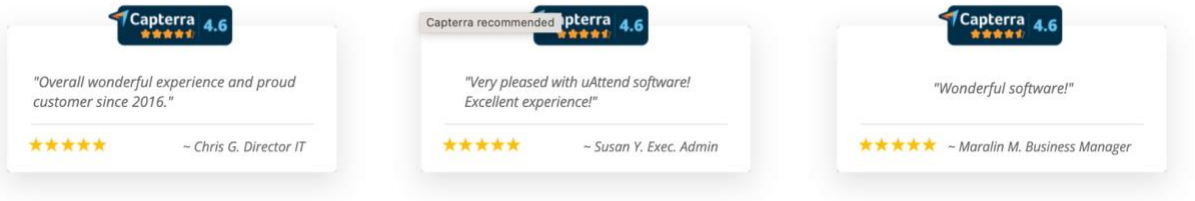


Figure 5: Testimonials (uAttend)

These examples should give a sense of the types of genres and information collected (or that could be collected) from biometric solution websites. The collections highlighted and listed are similar across the 15 biometric websites. For example, for every company, there was the homepage, along with genres/texts collected such as:

- product images and subsequent descriptions,
- FAQs
- an about page describing or justifying the technological solution,
- terms and conditions (though usually difficult to find),
- privacy policies for either specific products or general ones for all products distributed,
- case studies, blogs, and/or testimonials from clients.

It is important to note that not every company published a privacy policy or their terms and conditions; nor were they (with few exceptions) easily accessible if published on the website.

Table 1: Biometric Solution, Company, and Example Texts Collected

Solution	Company	Text Collected (Genre)
Voice	VoiceVault	Product Images/Descriptions; About Page; Terms and Conditions; Privacy Policy;

		Testimonials
Voice	Spitch	Product Images/Descriptions; About Page; Privacy Policy; Case Studies
Voice	Sensiple	Product Images/Descriptions; About Page; Case Studies
Voice	Fortress	No longer accessible
Voice	rfIDEAS	Product Images/Descriptions; About Page; Case Studies
Facial	Johnson Controls	Product Images/Descriptions; About Page; Future Projects
Facial	Feigete Technology	Product Images/Descriptions; About Page
Facial	Reveal Media	Product Images/Descriptions; About Page
Facial	Estone Technology	Product Images/Descriptions; About Page; Case Studies; Tech Blog
Facial	GSI Technology	Product Images/Descriptions; About Page; Awards and In the News
Fingerprinting	American Health Biometrics	Product Images/Descriptions; About Page; Privacy Policy; FAQs
Fingerprinting	GenKey	Product Images/Descriptions; About Page; Timeline (Company History); Code of Conduct; Privacy Policy
Fingerprinting	TeReSol	Product Images/Descriptions; About Page; News; All Resources (Case Studies, etc) "Under Development"
Fingerprinting	Nundlab	Product Images/Descriptions; About Page; Case Studies; Blog; News; Terms and

		Conditions
Fingerprinting	uAttend	Product Images/Descriptions; About Page; Biometric Data Policy; Privacy Policy; Disclaimers; Testimonials

The following sections outline the companies labeled above in the table (Table 1: Biometric Solution, Company, and Example Texts Collected), their "about" sections *directly* copy and pasted from the website, and how I chose the specific biometric solution company from Biometric Update's website. Not all information collected from the textual corpus is included within the analysis (Chapter 4). More will be discussed as to reasonings, categories, and themes pulled from the corpus in Chapter 4's analysis.

i. Voice Recognition

To find the companies creating voice recognition tools and software for the healthcare industry to use, I searched underneath the link for the directory of companies from BiometricUpdate. I first searched for "health." From there, I found the following companies, who also have locations in the United States. To reiterate, all information about the companies in this corpus are copied directly from their "about" sections on their websites. All were accessed in February 2023.

- https://www.verint.com/engagement-data-management/active-voice-biometrics/
  VoiceVault is a voice biometric solutions company delivering to the Financial Services and Healthcare industries. Our solutions provide security, convenience and compliance via smartphone apps, the web or through traditional telephony channels. Delivering via partners, our voice biometric solutions provide data and application access control; transaction authorization; identity verification; e-signature provision; and out of band authentication. Biometric voice-based solutions enable business processes to dispense with knowledge-based authentication (something you know – like a PIN or password) or device-based authentication (something you have – a one-time password token device for example) and replace them with something you are – the sound of your voice.

I then searched for “medical” with one result, and then “United” to find United States-based companies. Since the location was/is in the United States for the Spitch company (or may be purchased in the United States), I counted this company as acceptable to use for the corpus.

- https://spitch.ai/
  Spitch is a global provider of B2B and B2C Conversational AI solutions, headquartered in Switzerland since 2014 with a presence in many countries across Europe and North America. Spitch helps enterprises to better understand and serve their customers through the use of Natural Language Processing (NLP), Artificial Intelligence (AI) and Machine Learning. Spitch both owns and is constantly developing its core technology. This is taken to market in the form of end-to-end products such as virtual assistants, voice biometrics and speech analytics.
- https://www.sensiple.com/
  At Sensiple we believe that ‘Technology’ is the axle of the wheel of progress in the digital economy, but we also know that it's human experience that's on the driver seat, deciding the direction and destination. So, in our journey of two decades, our priority has always been to use our acumen in technology to create solutions that translate to delightful human experiences. Whatever be the solution we design, whether it is next-gen contact center technology to rev up your customer experience or automation that irons out friction in your workflows, or migrating your applications to the Cloud, our goal remains the same – to delight people and drive them forward to a better future.

Many of the participants in the study mentioned fingerprinting being used by employees for record keeping, so I then searched “employee.”

- https://fortress-identity.com/
  No longer in service.

To find the last company, I searched the term “authentication” because many of the nurses mentioned that voice recognition would be for authentication purposes. That is, the voice recognition software would recognize the doctor dictating the notes into the table. This was an interesting differentiation, which will be discussed more in the interview section. Neonatal nurses mentioned wanting more voice implementation in their day-to-day, yet currently noted that doctors in certain units are the only ones permitted to use the voice authentication. Nurses described concerns with patient anxiety (them hearing the doctor dictating their notes),

inaccuracies (we all know what happens when we use talk to text), and momentary ease for the job (many doctors needed to reread patient notes to ensure all information was accurate).

- https://www.rfideas.com/
  At rf IDEAS, reliability and efficiency are our top priorities. It's how we empower companies just like yours to make security simple by implementing our authentication solutions. Across industries like healthcare and enterprise, our logical access control solutions are compatible with your existing credentials, giving you the tools to manage your security ecosystem. Our goal is to be so reliable that easy access becomes what you expect.

ii. Facial Recognition

Underneath the link for the directory of companies, I searched for "health." From there, I found the following companies, who also have locations in the United States. Since the location was/is in the United States or may be purchased in the United States, I counted these companies as acceptable to use for the corpus. Each company listed also includes their "about us" information.

- https://www.johnsoncontrols.com/
  Johnson Controls is a world leader in smart buildings, creating safe, healthy and sustainable spaces. For nearly 140 years, we've made buildings better and now we're transforming them again with our award-winning digital technologies and services. We're using artificial intelligence and data driven solutions to give you deeper insight into your building's health, sustainability and performance. It's changing the way we design, operate and maintain indoor environments and driving to a new era of autonomous buildings. We deliver the blueprint of the future for industries such as healthcare, schools, data centers, airports, stadiums, hotels, manufacturing and beyond through OpenBlue, our comprehensive suite of connected solutions. Johnson Controls offers the world's largest portfolio of building technology, software and services. Supported by a team of more than 100,000 dedicated employees working across 150 countries, we're helping customers achieve their sustainability goals and power their mission.
- https://www.smartfeigete.com/about-us_d1
  Founded in 2004. Headquartered in Shenzhen, which is specializing in manufacturing and developing various terminals including Smart fingerprint POS; Fingerprint RFID writers/readers (13.56 MHz for proximity or 840-960 MHz for long range); Fingerprint & Face Recognition time attendance; Wireless barcode scanners; Thermal printers; Industrial tablets etc smart devices. SFT highly focuses on offering one-stop biometric solutions in ticket Management, Park ticketing, Transportation and Logistics, Barcode solution, Police Affairs, Attendance, Bank Teller Fingerprint identification, Identity etc. Our products are widely applied in various fields, such as: mobile payment, banking

sector, healthcare, supermarkets, logistics, transportation, business ticketing system, manufacturing industries, inventory, asset management and traceability, which have gained a good reputation worldwide.

- https://www.revealmedia.co.uk/
  Our advanced technology is adopted by police, leading security organizations, healthcare professionals and flagship retailers, and we are continuing to grow into new industries. We remain the market leader in body-worn camera solutions and digital evidence management software with the most advanced systems in the world.

I then searched for the term "medical" and received the following results:

- https://www.estonetech.com/
  Founded by a group of seasoned industrial PC veterans with over 20 years of experience, Estone Technology is a leading design and manufacturing company for rugged computing solutions including rugged tablet PCs, medical tablet PCs, industrial panel PCs, and embedded computer systems. We leverage the newest computing technology to service the vertical markets of healthcare, transportation, field service, military, oil & gas, hospitality, and more. Partnering with industrial leaders such as Intel, Microsoft, and ARM allows us to provide a wide range of computing products to clients worldwide. Our established sales and support facilities with ISO9001 and ISO13485 certification in North America, Europe and Asia also support these efforts. We provide one-stop OEM/ODM service to clients, including ID design, prototyping, board level design, OS (Window, Android, Linux), chassis molding, certification (CE, FCC, CSA, PCM, RoHS, UL, Medical IEC-60601, Google GMS, Amazon Alexa), production, warranty, and logistic support. For many industrial clients, we manage and guarantee their product life for 7 years or more.
- https://www.gsitechnology.com/about-gsit
  Founded in 1995, GSI Technology, Inc. is a leading provider of SRAM semiconductor memory solutions. GSI's newest products leverage its market-leading SRAM technology. The Company recently launched radiation-hardened memory products for extreme environments and the Gemini® APU, a memory-centric associative processing unit designed to deliver performance advantages for diverse AI applications. The Gemini APU's architecture features parallel data processing with two million-bit processors per chip. The massive in-memory processing reduces computation time from minutes to milliseconds, even nanoseconds, while significantly reducing power consumption in a scalable format. Gemini excels at large (billion item) database search applications like facial recognition, drug discovery, Elasticsearch, and object detection. Gemini is ideal for edge applications with a smaller footprint and lower power consumption, where rapid, accurate responses are critical.

iii. Fingerprinting

As with the voice recognition and facial recognition, underneath the link for the directory of companies from BiometricUpdate, I searched for "health." From there, I found the following companies, who also have locations in the United States. Since the location was/is in the United

States or may be purchased in the United States (as in the U.S. is a market for the company), I counted these companies as acceptable to use for the corpus.

- https://americanhealthbio.com/
  American Health Biometrics specializes in live scan & ink card fingerprinting. We are located in Long beach and have been in business for over 9 years. We offer fast, excellent, and professional services in our office and mobile. We are qualified and certified by the California Department of Justice and Federal Bureau of Investigation to provide reliable and timely fingerprinting services for background screening, licensing or certification, employment and professions with applicants for employment.
- https://www.genkey.com/about-us/
  GenKey, founded in 2001, developed out of a merger with priv-ID, an off-shoot of Philips' biometrics research division. Since then, GenKey has delivered large-scale, biometric identity programs globally for governments, public institutions and businesses. GenKey has offices in Eindhoven (Netherlands HQ), Accra and Chicago (USA).
  I then searched for "medical" with one result from a country outside of the U.S., and then "United" to find United States-based companies.

- https://www.teresol.com/enterprise-level/hr-management-solutions/
  TeReSol is an ISO 9001 & ISO 20000 certified R&D company with more than five million man-hours of development experience. The company focuses on providing embedded solutions and software services for Avionics, Consumer Electronics, Automobile and Banking /Financial sector. These embedded designs include complex multi layers (18-24) high speed signal processing PCBs, Single Board Computers (SBC) for time scheduled applications, their board support packages/APIs for external integration and complete customized end to end product (qualified for tough temperature environment) with multiple designed cards. Software services includes design/development of Enterprise Service Bus (ESB) Architecture based scalable/secure solutions, Algorithm design using Machine Learning/AI techniques and their real time implementation in various fields/areas.
- https://nundnet.com/
  Nundlab, Inc. was established to serve the security & surveillance industry, experienced in design & production of the turnstiles & access controls, and various innovative security systems. With a very wide experience in research & development, the company has successfully launched several innovative products turnstile & access control systems. The turnstiles & access controls are designed as per the market requirements, and on the basis of specific requirements. Based on the six sigma principles & other quality management systems, strict quality control is key to our success. We do offer the high-quality turnstiles & access controls with replacement warranty for the period of three years. For over decade, Nundlab, Inc. supplies turnstiles and access controls under brand name Nundnet and is widely recognized by professionals. Nundlab, Inc. is a globally trusted name in OEM & ODM for various renowned brands. Our products are made in selected manufacturing plants worldwide.

Since many of the participants in the study mentioned fingerprinting being used for employee and patient monitoring, as well as new software for infant fingerprinting, I then searched "employee."

- https://uattend.com/
  Time clocks that work as hard as you. Advanced technology paired with powerful cloud software provide everything it takes to get the job done.

The following sections focus on the questionnaire and interviews conducted with neonatal nurses.

3.4d Questionnaire: I want the Snowball, not the Avalanche

The IRB-approved screening survey, or questionnaire, was created in Qualtrics (see Appendix A). This platform has a built-in analysis tool, allows me to export data, and is "protected" by the East Carolina University server. My study and research questions contribute to understanding how neonatal nurses define their role and job duties, as well as understand their overall perceptions of biometric technologies in healthcare. Surveys were the most appropriate means to collect a baseline understanding of how nurses defined personal information/privacy, as well as biometrics. To understand the neonatal nurse perceptions, I found surveying to be the most appropriate method of data collection. Further, surveying was an appropriate method to collect emails to interview participants. Surveying allowed for ease of distribution on various platforms.

From the list of nurses willing to be interviewed, I emailed neonatal nurses who provided their email addresses to gain a more in-depth insight into their usage and understanding(s) of biometric technologies. Crouse and Lowe (2018) write how snowball sampling[45] is a "sampling

[45] Snowball sampling: a sampling method used by researchers to generate a pool of participants for a research study through referrals made by individuals who share a particular characteristic of research interest with the target population. It is also referred to as chain sampling or chain referral sampling (Crouse & Lowe, 2018).

method used by researchers to generate a pool of participants for a research study through referrals made by individuals who share a particular characteristic of research interest with the target population." MacNealy (1999) references a slightly different definition of snowball sampling: "the population of interest [that] cannot be identified other than by someone who knows that a certain person has the necessary experience or characteristics to be included" (p. 157). Of course, MacNealy's definition isn't quite what this project did. Rather, Crouse and Lowe's (2018) overview of snowballing through *referrals* is what I had hoped would happen with my questionnaire: that fellow neonatal nurses would take the screener and then pass the link to their friends and fellow neonatal nurse networks. I titled this section "I want the snowball, not the avalanche" because the distribution of the screening survey slowly turned into an avalanche. Despite my hope to survey a wide range of neonatal nurses across the United States, with differing backgrounds, demographics, and experiences, the screening survey was largely distributed within the same networks. That is, neonatal nurses shared the link with populations who were very similar in experience, background, and location, thus creating more of a localized response in my surveys rather than a representation of neonatal nurse perceptions across the nation. Sure, that makes sense when we think about snowball sampling; however, from the list of networks I distributed to, I had expected (especially from the national organizations) to have a wide range of responses. I had also expected that the snowballing would happen inter-network: that is, I assumed that similar to technical communicators being part of professional organizations and from different institutions, that nurses would "snowball" to other nurses across the nations from the connections they made within the group/organization. Instead, I received a localized avalanche.

The IRB-approved consent paragraph and questionnaire questions are located in Appendix D. From this questionnaire, I am interested in analyzing how the context and environment can affect the way certain communities understand and interpret biometrics (such as differences based on healthcare location, background, experience, and specific biometric technology). I received a Research Grant from the Council for Programs in Technical and Scientific Communication to fund interview participants. This grant was awarded in June of 2022, prior to finalizing screening survey(s) and interview questions.

When designing the study, I considered Teston et al. (2019) notion of precarious positionality[46], or "research participants self-identify as one or more of the following: a racial and/or linguistic minority, economically disadvantaged, disabled, former or current drug user, undocumented, un(der)educated, oppressed, sexualized, disenfranchised, criminalized, and/or colonized" (p. 321). The recommendations from Teston et al.'s (2019) article contend with issues of ethics, inclusion criteria, privacy, stigmatized and misleading language, variations in discursive repertoires, accessibility, and liability (p. 321).

Both in my questionnaire and interviews, there is a trend in me stating that the participants will remain confidential, and no information will be distributed. Further, I state (and write) that there is little to no risk, and participants can choose to not respond to or exit the interview/survey at any time. But no risk to whom? This is the static, boilerplate language advised by the Institutional Review Board (IRB), yet technical communicators know that risk is not evenly distributed across populations. For example, Teston et al. (2019) writes how surveys are often viewed as both "efficient and expedient," and are "employed to unspool complexities

[46] Precarious Positionality: research participants self-identify as one or more of the following: a racial and/or linguistic minority, economically disadvantaged, disabled, former or current drug user, undocumented, un(der)educated, oppressed, sexualized, disenfranchised, criminalized, and/or colonized (Teston et al., 2019).

associated with health, medicine, and the human condition" (p. 322). In the case of this questionnaire, Teston is right: this survey *was* distributed for "efficiency" but certainly with the understanding that there are *many* ethical concerns, especially with privacy, surveillance, and understanding of health.

In particular, one concern that I had specifically was with the timing of my survey distribution. Not only did the Association of Women's Health, Obstetric and Neonatal Nursing (AWHONN), for example, distribute my survey prior to Thanksgiving, but they also distributed it a second time on December 7. The distribution fell during a time where many people in the United States had time off for the holiday(s), and therefore likely weren't checking their emails. This distribution was for efficiency's sake, in the sense of the organization sending out the questionnaire when it was convenient for them but likely not when a higher response rate would be expected. More information follows below. Barr, Spitzmuller, and Stuebing (2008) examined the correlations between survey participants' work-related stress and their participation in organizational surveys, noting that employees who experience high levels of work overload are less likely to respond to organizational surveys and therefore may be overlooked or underrepresented in survey data (p. 239). This certainly contributes to my snowball sampling, as well as the overall response rate.

Further, Tucker King, et al. (2017) argued that a "common theme" surfaced in the case studies they examined: "the IRB perspective on what is the best way to protect participant confidentiality and privacy, and thus to minimize risks for participants, is informed by a concept of health communication that is incommensurable with that of the researcher" (p. 909). As a scholar who studies privacy and surveillance, this is a concept I had at the forefront of my

research: how do I make sure I consider precarious publics[47], while also grappling with IRB expectations. For many researchers who contend with these tensions, I'm sure they approach the resisting of institutionalized norms through "consenting" with the terms of IRB, while shifting practice to protect those throughout the study. Let's read between the lines here.

This shifting, however, shouldn't *have* to occur. The real issue is that we need to revise our institutional practices to account for contextual needs, agency of research participants, and "non-Western" language, knowledges, and so on. And since precarious publics are often hyper-surveilled and are the targets of high amounts of surveying, it was especially important to me to create a multiple-methods approach for this study, gathering means to compensate interview participants while also considering how to best represent participants and their answers.

The questionnaire, with the guidance of Teston et al.'s (2019) suggestions, was piloted first with fellow professional networks prior to mass distribution on social media. To reach neonatal nurses across the United States, it was crucial to consider who may be included/excluded in this reach. Since the survey was about usage and perceptions of technologies, the decision was made that by distribution to email, social media, and snowball sampling, this would include sufficient responses from nurses. There are several other considerations that I should have implemented prior to interviewing and survey distribution such as more attention to usability, document design and preferred language/modes of communication (and more). Teston et al.'s (2019) article is a piece that I wish I read prior to the beginning of crafting my study yet helps with reflecting on all the ways I may shift my research practice with future participants. I especially believe that executing a screening questionnaire and specifically

[47] Precarious Publics: meant to index would-be participants whose survey responses illuminate—either deliberately or accidentally—infrastructural, institutional, political, socioeconomic, racialized, environmental, and/or gendered (f)actors that condition what the IRB and the Common Rule short-handedly refer to as "risk" (Teston et al., 2019).

targeting certain locations nationwide would have contributed to some of my concerns with access and financial barriers that I discussed during the community engagement section (3.4a). For example, Teston et al. (2019) decided that to "ensure that we obtain experiences from those whose precarious positionalities may make them less likely to encounter a survey online, we have decided to design an analog version of the survey to be distributed in hard copy format in several public health facilities in each state" (p. 335). Though I did have to contend with, as a graduate student, issues of time and resources, this is a significant design decision that would improve the quality of my data. Further, since it is unclear if participants understood the difference between confidentiality and anonymity (Teston et al., 2019, p. 336), I made sure to create a demographic question as the class question in the screening survey where participants were able to disclose what *they* wanted to, rather than a drop-down menu or multiple choice. Making claims about survey participants' anonymity requires that their responses would be impossible to trace back to them, which as surveillance and privacy scholars note, this is certainly not the case. Our identities are easily tracked through our IP address (with/without a VPN), data breaches, amongst the information we choose to disclose.

The questionnaire was distributed on Twitter on August 15, 2022, through my personal account. From the initial collection, I received two participants who were interested in being interviewed on August 22, 2022, and gave them a date to respond by to be interviewed. I never heard from the first two participants; however, I began to receive more responses through the questionnaire and reached out to two more participants the following week.

The following is the Twitter post (August 2022):

> Are you a neonatal nurse based in the United States? I'm a PhD Candidate conducting a research study about neonatal nurse perceptions and usage of technologies in healthcare. Your responses will be kept confidential. Here's the survey link: https://ecu.az1.qualtrics.com/jfe/form/SV_5ikAT5Ny4rjGFkG.

> Please dm with any questions or concerns. I'm happy to discuss this project further :) Feel free to also distribute amongst your networks!

The following are the accounts I tagged on Twitter (August 2022):

> @AWHONN
> @NeonatalNurses
> @BirthEquity
> @OpenAcademics
> @AcaHumanities
> @AcademicChatter
> @PhDForum

After soliciting participants through Twitter, I also posted the screening survey on my personal Facebook and LinkedIn pages. The following is the post that was published:

> Good afternoon,
> My name is Morgan Banville and I'm a PhD Candidate at ECU conducting a research study about neonatal nurse perceptions and usage of technologies in healthcare. If you identify as a neonatal nurse based in the United States, this survey is for you! Your responses will be kept confidential, and the survey should take approximately 10 minutes. The following is the survey link: https://ecu.az1.qualtrics.com/jfe/form/SV_5ikAT5Ny4rjGFkG. Thank you for your time!

Finally, my screening survey wasn't receiving as much traction as I had hoped. Because not a large number of nurses (3 total the first round; 12 the second due to localized sharing of the survey; 13 the last round prior to AWHONN) provided their email addresses to be interviewed (not all nurses responded), I researched nursing/neonatal nurse professional organizations to request distribution of my screening survey. The aim for the number of interviewees was 10 nurses; because nurses did not answer and there weren't enough nurses interested in being interviewed from the initial screening, I emailed the following accounts (Table 2: List of Organizations Emailed with Questionnaire) this paragraph on August 16, 2022:

> Good morning, My name is Morgan Banville and I'm a PhD Candidate at East Carolina University (ECU) located in Greenville, NC. I am conducting a research study about neonatal nurse perceptions and usage of technologies in healthcare. I am hoping to survey neonatal nurses across the United States. All responses will be kept confidential, and the survey should take approximately 10 minutes. The following is the survey link:

https://ecu.az1.qualtrics.com/jfe/form/SV_5ikAT5Ny4rjGFkG. Thank you for your time, and please distribute amongst your networks. I'm available for any questions/concerns at 508-817-6937 or email!

Table 2: List of Organizations Emailed with Questionnaire

National Association of Neonatal Nurses (NANN)	Emailed	http://nann.org/about/our-staff
Academy Online	Emailed	https://www.academyonline.org/general/?type=CONTACT
American Academy of Nursing (AAN)	Emailed	http://www.aannet.org/
American Association of Nurse Practitioners (AANP)	Emailed	https://www.aanp.org/
American Nurses Association (ANA)	Tweeted at, couldn't email	http://www.nursingworld.org/
Academy of Neonatal Nurses (ANN)	Emailed	http://www.academyonline.org/
Association of Women's Health, Obstetric and Neonatal Nursing (AWHONN)	Emailed	https://www.awhonn.org/
Association of Women's Health, Obstetric and Neonatal Nursing (AWHONN)	Coordinated paid screening survey - 1000 participants/$375	https://www.awhonn.org/
Florida Association of Neonatal Nurse Practitioners (FANNP)	Emailed	https://www.fannp.org/
Florida Association of Neonatal Nurse Practitioners (FANNP)	Facebook Group	
Tennessee Nurses Association (TNA)	Emailed	https://www.tnaonline.org/
National Association of Neonatal Nurse Practitioners (NANNP)	Couldn't access	http://www.nannp.org/

National Perinatal Association (NPA)	Emailed	http://www.nationalperinatal.org/
Southern Research Nursing Society (SNRS)	Emailed	http://www.snrs.org/
National Organization of Nurse Practitioner Faculties (NONPF)	Couldn't access	http://www.nonpf.org/

3.4e Interviews

My interviewees included a diverse (age, geographical location, gender, and sexuality) group of neonatal nurses who took my screening survey and noted that they would like to participate in a compensated interview. Nurses were able to disclose demographic information that they wished to share; there were no pre-fixed categories or prompting questions other than asking them to share whatever demographics they wanted to disclose. The requirements were that they were neonatal nurses based in the United States. Interviews were no longer than one hour. I approached interviewing through an interlocking feminist lens, borrowing from Garland-Thomson (2011a), who suggests that scholars ask, "difficult questions but accepts provisional answers," privileging "the partial, the provisional, the particular" (pp. 40-42). A consideration that interlocking surveillance helps us to imagine is *how* we interact with participants. Though I mentioned to interviewees that the interview would be through video (participants did not need to turn on video and only one did opt to), and that the video would be recorded, other issues of access such as transcription were only available to me. In retrospect, I realized after some reflection that I had been grappling with the access of my own study: do I provide interviewees with questions ahead of time, or withhold such access so I could document initial responses? What about questions I might potentially skip, and/or follow-up questions? I did not end up sending interviewees the questions ahead of time, but I did make sure that they could access

transcription on Microsoft Teams, and I left my video on when conducting the interview. I didn't send the questions because I did not want interviewees to rely on any other outside sources or research other than their own lived experiences.

The purpose of including an interview is to expand upon the questions in the screening survey and to dive deeper into understandings and usages of biometrics. From these conversations, I noticed some themes emerging around privacy, emotions towards biometrics and surveillance, protocols established by companies, identification and authentication procedures, safety, efficiency, and tensions between personal/professional obligations. I initially anticipated conversations about shifted processes due to the COVID-19 pandemic, including increase in digital technology use, choice in opting in/out, and potential employment concerns, however this was mentioned little to not at all throughout the interviews.

Participants' names are changed to "Interviewee" in this study to provide anonymity. In these interviews, I asked all participants if they wanted to remain "anonymous" and further, how they would prefer to be compensated. It is part of my research practice and pedagogy to pay participants for their labor, as oftentimes people (especially multiply marginalized populations) are not paid for their expertise. Interview participants were asked to send two websites that offered digital (e-gift) cards. From there, I chose the site and sent a $50 e-gift card after the interview. Many interviewees opted for Amazon e-gift cards.

In this study, I collected email addresses in the screening survey only from nurses who were interested. From there, I viewed their exported reports and emailed participants. I received a grant from the Council for Programs in Technical and Scientific Communication which afforded me the opportunity to pay my ten participants for their time during the interview. Interviews didn't last more than 60 minutes, and participants were compensated with e-gift cards

of their choosing. The standard interview paragraph that was distributed after the Institutional Review Board approved my study (Appendix D), and the interview questions (Appendix C) are located in the Appendix. After the questions, I shifted into scenarios. I chose two out of three scenarios to discuss depending on the questionnaire responses (Appendix C). That is, based on the definitions and chosen examples, I decided whether or not the neonatal nurse had/didn't have experience with biometrics. If they seemed to have a level of informedness about biometric technologies based on my definition, then I skipped the last scenario about wearables.

Table 3: List of Neonatal Nurse Interviewees

Interviewee Name	Demographics[48]	Date Interviewed	Length of Interview	Scenarios chosen
Interviewee A	Female, Black, American, 35	September 7, 2022	57 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee B	Male, Alaska, 35, Heterosexual	September 12, 2022	52 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee C	Male, African American, Atlanta, 37, Heterosexual	September 25, 2022	1 hour 2 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee D	Female, Black, 25, Straight	September 19/21, 2022	20 minutes/10 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee E	Female, 46, Latina, Mexican, married	January 11, 2023	44 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee F	Male, 24,	January 11, 2023	53 minutes	Infant

[48] Participants were asked to choose what demographics they wished to disclose.

	African American, heterosexual			Fingerprint (1) and Northwell (2)
Interviewee G	Male, 30, African American, Straight	January 12, 2023	39 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee H	Male, 30, African American, Straight/Heterosexual	January 13, 2023	43 minutes	Infant Fingerprint (1) and Northwell (2)
Interviewee I	Male, 26, American, Straight	January 19, 2023	59 minutes	Infant Fingerprint (1) and Northwell (2) Wearables (3)
Interviewee J	Male, 23, Black American, Heterosexual, American	January 24, 2023	27 minutes	Infant Fingerprint (1) and Northwell (2)

The following sections focus on the coding schema based on my methodological framework, interlocking surveillance. I discuss how I approached coding, including the themes, categories, and process of choosing terminology and selecting excerpts to privilege as evidence.

3.5 Coding

This section focuses on the ways I approached coding the corpus, questionnaire, and interviews. The qualitative approaches to coding focus on *elements* of holistic, open, and purposeful schemas. Because of the nature of my heuristic not having set codes, I wanted to approach coding through combining elements of analysis that were representative of the information collected. After the screening survey (questionnaire) and interviewee information was collected, I sifted through the data (collected responses and transcriptions) and noticed that

out of the biometric technologies listed and discussed by participants in the screening survey, voice recognition (19.15%), facial recognition (23.40%), and fingerprinting (27.66%) were the top three biometrics most used by (and familiar to) neonatal nurses. The percentages account for the total responses documented by the nurses in the questionnaire for Q5, which was 32 responses. Participants could choose more than one option. "Q5: Does your current workplace employ these kinds of technologies? Select all that apply."

The screening survey had a total of 118 participants (Report 1). From this information, I worked backwards to find companies based in the United States who created the voice recognition, facial recognition, and fingerprinting technologies. Though the specific brand of technology used within healthcare varies amongst institutions and is largely privatized information (as in not available to patients, and perhaps even employees other than administrators), I sought biometric corporations who were communicating their products to a specific industrial sector (healthcare).

On November 9, 2022, I visited a graduate class at East Carolina University to gain some insights into my coded and thematic categories pulled from my screening survey. There were overlapping categories that the fellow graduate students pulled from my screening survey responses that matched with my own categories. I'll provide some general insights into the categories which will be discussed in Chapter 4. Also, during this graduate class, I talked through my methodological framework and approach to coding. Though an informal conversation, this class did help inform coding reliability as the graduate students and instructor in the course participated in my coding process for the questionnaire, specifically. I also met with colleagues and fellow graduate students (outside of the specific course) to request feedback on how I was coding and understanding my own data. Other scholars such as Koerber and McMichael (2008)

informed my approach through giving examples of the ways qualitative health information could be analyzed and/or approached. While technical communication certainly doesn't have systematic and transferable vocabulary for "discussing and evaluating the traits of appropriate qualitative samples," this section explains *how* I approached qualitative samples, building off the previous chapter discussions of 'why this group (neonatal nurses)' and 'why these documents (textual corpus)' (Koerber & McMichael, 2008, p. 458). For example, I might classify my approach towards sampling the population as purposeful[49]. Healthcare researchers such as Simmons (2002) and Hoddinott & Pill (1999) are useful examples of purposeful sampling aimed at recruiting mothers in order to interview them about their experiences with infant feeding. Similarly, I knew the population I wanted to focus on (neonatal nurses) and recruited them to be interviewed about their experiences with biometrics. I further applied my heuristic to analyze the collected samples.

For the corpus, I searched the websites (as listed in 3.4c) for what I considered the biometric solution company to communicate intended purpose of technology, justification of standardization, categorizing of people (as they relate to demographics and predetermined social stereotyping and hierarchies), levels of informedness (that users would determine from the ways the company was transparent about their practices), and discussions of efficiency/urgency. The language was determined from the collected corpus based on the predetermined questions from my methodological framework. The following genres encompass the textual corpus:

- product images and subsequent descriptions,
- FAQs
- an about page describing or justifying the technological solution,

[49] Purposeful sampling: the researcher is looking for participants who possess certain traits or qualities.

- terms and conditions (though usually difficult to find),
- privacy policies for either specific products or general ones for all products distributed,
- case studies, blogs, and/or testimonials from clients.

For example, when I browsed through a solution's website from BiometricUpdate, I would look for language that *could* be categorized based on the heuristic. This may be referred to as holistic coding (Saldaña, 2015), as I already had a general sense of what I wanted to investigate and categorize based on my methodological framework. All of the information collected led to understanding(s) of healthcare as a site of surveillance, and how technical communicators could advocate, create awareness, and urge for transparency for the bodies harmed by surveillance tools and technologies. The following table (Table 4: Methodological Framework and Coding Language) is an example of the methodological framework's heuristic (on the left), and the language from the collected websites (on the right) that corresponds to the heuristic. For example, companies "justified standard usage" by referencing that the technology should be implemented for topics such as "customer satisfaction" and "data security and compliance."

Table 4: Methodological Framework and Coding Language

Methodological Framework Categories Goals: Awareness, Advocacy, Transparency	Coding Language Based on Corpus
What are the intended purposes of the technology?	Safety; Security; Efficiency "quick; time; attention"; Solutions to Help You Succeed
How does the corporation justify its standard usage?	Customer Satisfaction; Employee Engagement; Data Security and Compliance; Customization; Cost Reduction
How does it categorize people and into what categories (and for what purpose)?	"Acceptable" Customers and Those Who Are Fraudulent; Identity Theft

How does the corporation justify its technological usage?	Data and Access Control; Compliance; Transaction Authorization; Identity Verification; E-Signature Provision; Out of Band Authentication
How are people informed about the capabilities, data collection, and more?	Third Parties; Privacy Policy; Terms and Conditions; Biometric Data Policy
Is the technology poised for efficiency purposes, or implemented during a time of "urgency"?	Fraudulent; Security checks; Customer experience; Patient Experience

This framework is useful to apply to a corpus of biometric corporation statements because of the largely unseen ways that surveillance pervades our lives. Though biometrics within healthcare may be used for positive use, it is important to apply interlocking surveillance to the textual corpus to further analyze the language that is used to discuss issues of privacy, wellness, and health. The coding categories for the specific biometric corporate statements (textual corpus) focus on voice recognition, facial recognition, and fingerprinting; from there, themes emerged organically and are analyzed through the framework of interlocking surveillance in Chapter 4. The methodological framework specifically highlights how companies engage in principles of awareness, advocacy, and transparency in relation to data collection, storage, and distribution. Through my study's methods of interaction with people, interviewing and surveying, my approach to understanding is through rhetorically listening. I further extracted coding categories based on my heuristic by implementing an approach coined by Royster and Kirsch called strategic contemplation. I took elements of strategic contemplation by carefully contemplating my data to "take as much into account as possible but to withhold judgment for a time and resist coming to closure too soon" (Royster & Kirsch, 2012, p. 85). For example, after collecting my data and initially applying the heuristic, I took time to review my corresponding codes to the heuristic.

Further, when choosing interviewees based on the screening questionnaire, I set aside any assumptions based on the collected data. This meant choosing interviewees that disclosed information that was not all the time: including, but not limited to, location of the practice (geographical), type of practice (private, public, etc.), responses to understanding biometrics and privacy, and demographic information (this question was open for participants to disclose as they saw fit). Some of the ways I set aside assumptions within the interviews themselves was through reiterating some of the screening questionnaire questions at the beginning of the interview (such as asking questions about the neonatal nurse's career, day-to-day, and follow-ups to ideas/comments I was unsure of). Reiteration also included defining key terms, such as biometrics, as this assisted in emphasizing inclusivity and respect for those who were being interviewed since strategic contemplation emphasizes not making assumptions (and this includes assumptions regarding knowledge "levels") and memory (regarding responses on the questionnaire).

After interviewing neonatal nurses, I approached a more holistic coding to the transcriptions. Though I am applying interlocking surveillance to the collected data (Chapter 4), this framework allows for flexibility in holistic understanding; that is, the collection of a textual corpus, screening survey, and the interview data is used *together* to better understand technical communicators' role in awareness, advocacy, and transparency at this site of surveillance. My approach towards open coding helped initially break down the interview transcriptions just because of the sheer amount of text. Open coding, as described by Saldaña (2015) as initial coding[50], helped to break down and categorize my interview data. I reread and listened to the transcribed interviews to highlight themes in relation to topics such as privacy, surveillance,

[50] Initial coding: Breaks down qualitative data into discrete parts, closely examines them, and compares them for similarities and differences (Strauss & Corbin, 1998, p. 102).

health, and the heuristic outlined by interlocking surveillance to describe perceptions and usage of biometrics. I then followed Dorpenyo's (2019) approach specifically for interviews after summarizing, by rereading the transcripts again and using words and phrases to name, label, and "categorize phenomena identified in data" (p. 366). I then pulled some themes from the interviews, such as the tension between professional role and personal feelings towards the usage and perceptions of biometric technologies. The details will be discussed further in Chapter (4).

As the interview data is shared and discussed, technical communicators may consider how this methodological framework seeks to engage in feminist applications through advocacy (how could you do this in your role); transparency (levels of transparency: from the top, all the way down); and awareness (creation of materials, technologies and their design) to empower. Technologies breakdown because "developers do not take into consideration the culture and nature of use in user contexts" (Dorpenyo, 2019, p. 362). Consequently, as we've seen thus far with the textual corpus of materials from the biometric solution companies, designs often do not reflect the ideology of users, but instead, they only make developer ideologies visible. From interviewing neonatal nurses who are actively utilizing the biometric technologies within healthcare, technical communicators are well apt to confront design challenges and interrogate the tensions between usability and social justice. The data thus far also displays the sheer disconnect between initial creation and communicating of the biometric solution, to the understanding of biometrics as they are intended to be utilized within healthcare. The accounts documented from neonatal nurses demonstrate how biometrics can potentially be a tool of marginalization and disenfranchisement. Overall, qualitative research was the best approach to this study because the focus was specific to exploring "natural settings, in detail, with the aim of

discovering the explanations for and the key patterns in the interaction of people with their environments" (Sullivan & Spilka, 1992, p. 595).

The following analysis in Chapter 4 allows technical communicators to examine the tensions between company advertising, legal language, and case studies to the people most likely to utilize these technologies in professional settings. Interlocking surveillance specifically understands sites of surveillance as assemblages: that is, the site of healthcare is interconnected. Through the corpus, surveys, and interviews, technical communicators can use the heuristic to better understand: What are the intended purposes of the technology? How does the corporation justify its standard usage; technology use; how does it categorize people and into what categories (and for what purpose); how are people informed about the capabilities, data collection, and more; and is the technology poised for efficiency purposes, or implemented during a time of "urgency"? The heuristic (interlocking surveillance) follows scholarly conversations and trajectories and are set questions rather than fixed codes and categories. Because of a lack of fixed codes, some of the questions may not apply to every study that explores a site of surveillance, such as healthcare. For example, the heuristic showcases the relationship between the collected textual corpus and the neonatal nurse interviews, as discussed in Chapter 4. Furthermore, interlocking surveillance was used as the coding scheme for the data from the questionnaires, a deductive approach[51].

3.6 Chapter Summary

This chapter discussed a methodological framework, interlocking surveillance, which bridges surveillance studies and feminist approaches to issues of surveillance. To summarize,

[51] Deductive: reasoning from the particular to the general. If a causal relationship or link seems to be implied by a particular theory or case example, it might be true in many cases. A deductive design might test to see if this relationship or link did obtain in more general circumstances (Gulati, 2009, p. 42).

interlocking surveillance combines elements of the new surveillance and intersectionality to develop a framework that addresses sites of surveillance and their levels of awareness, advocacy, and transparency of normalized surveillant practices. This methodological framework is useful in understanding surveillance tools and technologies through a feminist lens. This methodology is applied to data collected in Chapter 4: textual corpus analysis, screening surveys (questionnaire), and interviews. The methods and methodological framework work to answer: How do neonatal nurses define biometric technologies? What are neonatal nurses' perceptions of biometric technologies? The following chapter is a compilation of the data from the methods, where interlocking surveillance will be used as a framework to understand the collected information from the textual corpus analysis, screening surveys, and interviews.

REFERENCES

Adorjan, M., & Ricciardelli, R. (2019). A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide." *Canadian Review of Sociology, 56*(1), 8-29. https://doi.org/10.1111/cars.12227

Agboka, G.Y. (2013). Participatory localization: A social justice approach to navigating unenfranchised/disenfranchised cultural sites. *Technical Communication Quarterly, 22*(1), 28-49.

Alexander, J.J., & Edenfield, A.C. (2021). Health and wellness as resistance: Tactical folk medicine. *Technical Communication Quarterly, 30*(3), 241-256, https://doi.org/10.1080/10572252.2021.1930181

Banville, M., & Sugg, J. (2021). "Dataveillance" in the classroom: Advocating for transparency and accountability in college classrooms. *In The 39th ACM International Conference on Design of Communication* (SIGDOC '21), October 12–14, 2021, Virtual Event, USA. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3472714.3473617

Barr, C.D., Spitzmuller, C., & Stuebing, K.K. (2008). Too stressed out to participate? Examining the relation between stressors and survey response. *Journal of Occupational Health Psychology, 13*(3), 232–243.

Beauchamp, T. (2019). *Going stealth: Transgender politics and U.S. surveillance practices.* Durham, NC: Duke University Press.

Blakeslee, A., & Fleischer, C. (2019). *Becoming a writing researcher*, 2nd edition. Routledge.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Brucato, B. (2015). The new transparency: Police violence in the context of ubiquitous surveillance. *Media and Communication, 3*(3), 39-55.

Casper, M., & Moore, L.J. (2009). *Missing bodies: The politics of visibility.* New York: New York University Press.

Ceccarelli, L. (2013). To whom do we speak? The audiences for scholarship on the rhetoric of science and technology. *Poroi: An Interdisciplinary Journal of Rhetorical Analysis and Invention, 9*(1). https://doi.org/10.13008/2151-2957.1151

Crenshaw, K.W. (1989). Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum,* 139-67, p. 149.

Crenshaw, K.W. (2013). Mapping the margins: Intersectionality, identity politics, and violence against women of color. *In the Public Nature of Private Violence,* (pp. 93-118). Routledge.

Crouse, T., & Lowe, P. (Eds.). (2018). Snowball sampling. (Vols. 1-4). SAGE Publications, Inc., https://dx.doi.org/10.4135/9781506326139

Davis, J. (2022, December 1). HHS warning to providers: Use of pixel tracking tech without BAA violates HIPAA. *SC Media: A Cyber Risk Alliance Resource.* https://www.scmagazine.com/analysis/privacy/hhs-warning-to-providers-use-of-pixel-tracking-tech-without-baa-violates-hipaa

De Hertogh, L.B. (2018). Feminist digital research methodology for rhetoricians of health and medicine. *Journal of Business and Technical Communication, 32*(4), 1–24.

De Hertogh, L.B., Lane, L., & Ouellette, J. (2019). 'Feminist leanings:' Tracing technofeminist and intersectional practices and values in three decades of Computers and Composition. *Computers and Composition, 51,* 4-13. https://doi.org/10.1016/j.compcom.2018.11.004

Dubrofsky, R.E., & Magnet, S.A. (2015). *Feminist surveillance studies*. Durham and London: Duke University Press.

Flores Niemann, Y., Gutiérrez y Muhs, G., & González, C. (2020). *Presumed incompetent II*. Utah State University Press.

Frost, E.A., & Haas, A.M. (2017). Seeing and knowing the womb: A technofeminist reframing of fetal ultrasound toward a decolonization of our bodies. *Computers and Composition, 43,* 88-105. https://doi.org/10.1016/j.compcom.2016.11.004

Foss, S.K., Foss, K.A., & Griffin, C.L. (1999). *Feminist rhetorical theories.* Thousand Oaks, California: Sage Publications.

Foucault, M. (1995). *Discipline and punish: The birth of the prison.* New York: Vintage.

Garland-Thomson, R. (2011). Integrating disability, transforming feminist theory. In K.Q. Hall (Ed.), *Feminist Disability Studies*, (pp. 13-47). Bloomington & Indianapolis: Indiana University Press.

Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Glaser, B.G., & Strauss, A.L. (1999). *Discovery of grounded theory: Strategies for qualitative research.* New York: Routledge.

Glenn, C. (2018). *Rhetorical feminism and this thing called hope.* Southern Illinois University Press.

Gulati, P.M. (2009). *Research management: Fundamental and applied research*. Global India Publications.

Hoddinott, P., & Pill, R. (1999). Qualitative study of decisions about infant feeding among women in east end of London. *British Medical Journal, 318,* 30-34.

hooks, b. (1994). *Teaching to transgress: Education as the practice of freedom*. New York: Routledge.

Jones, N.N. (2016). The technical communicator as advocate: Integrating a social justice approach in technical communication. *Journal of Technical Writing and Communication, 46*(3), 342-361. https://doi.org/10.1177/0047281616639472

Katz, S.M. (2002). Ethnographic research. In L. Gurak & M. M. Lay (Eds.), *Research in Technical Communication* (pp. 23-46). Westport, CT: Praeger.

Kerr, I., Lucock, C., & Steeves, V. (2009). *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. Oxford: Oxford University Press.

Kimball, M.A. (2017). Tactical technical communication. *Technical Communication Quarterly, 26*(1), 1-7. https://doi.org/10.1080/10572252.2017.1259428

Koerber, A., & McMichael, L. (2008). Qualitative sampling methods: A primer for technical communicators. *Journal of Business and Technical Communication, 22*(4), 454–473. https://doi.org/10.1177/1050651908320362

Kynell-Hunt, T., & Savage, G. (2004). *Power and legitimacy in technical communication: The historical and contemporary struggle for professional status*. Routledge.

Larson, S. (2018, March 18). Beyond passwords: Companies use fingerprints and digital behavior to ID employees. *CNN Business*. https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html

Licastro, A., & Miller, B. (2021). *Composition and big data.* University of Pittsburgh Press.

Lyon, D. (2007). *Surveillance studies: An overview*. Malden, MA: Polity Press.

MacNealy, M.S. (1999). *Strategies for empirical research in writing.* New York Addison Wesley Longman.

Marx, G.T. (1998). *Undercover: Police surveillance in america.* Berkeley: University of California Press.

Marx, G.T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society, 1*(1), 9-29.

Monahan, T. (2022). *Crisis vision: Race and the cultural production of surveillance.* Duke University Press.

Moore, L.J., & Currah, P. (2015). Legally sexed, birth certificates and transgender citizens. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 58-79). Durham and London: Duke University Press.

Novotny, M. (2015). reVITALize gynecology: Reimagining apparent feminism's methodology in participatory health intervention projects. *Communication Design Quarterly, 3*(4), 61-74.

Reilly, C. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition, 61*. https://doi.org/10.1016/j.compcom.2021.102652

Royster, J.J., & Kirsch, G. (2012). *Feminist rhetorical practices: New horizons for rhetoric, composition, and literacy studies*. Carbondale: Southern Illinois University Press.

Sava, J.A. (2022, December 12). Biometric technologies - Statistics & Facts. *Statista.* https://www.statista.com/topics/4989/biometric-technologies/

Shivers-McNair, A., Gonzales, L., & Zhyvotovska, T. (2019). An intersectional technofeminist framework for community-driven technology innovation. *Computers and Composition, 51,* 43-54. https://doi.org/10.1016/j.compcom.2018.11.005

Simmons, V. (2002). Exploring inconsistent breastfeeding advice: 2. *British Journal of Midwifery, 10,* 616-619.

Staples, W.E. (2014). *Everyday surveillance: Vigilance and visibility in postmodern life, 2nd ed.* Lanham, MD: Rowman and Littlefield.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.). Thousand Oaks, CA: Sage.

Sullivan, P., & Spilka, R. (1992). Qualitative research in technical communication: Issues of value, identity, and use. *Technical Communication, 39*(4), 592-606. http://www.jstor.org/stable/43090168

Tsai, P. (2018, March 12). Data snapshot: Biometrics in the workplace commonplace, but are they secure? *Spiceworks.* https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure

King, C.S., Tucker, B., Kristin, M., Pumroy, E., Rauch, S., & Koerber, A. (2017). IRB problems and solutions in health communication research. *Health Communication, 33*(7), 907-916.

Walby, K., & Anais, S. (2015). Research methods, institutional ethnography, and feminist surveillance studies. In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 208-221). Durham and London: Duke University Press.

Walton, R., Moore, K., & Jones, N. (2019). *Technical communication after the social justice turn: Building coalitions for action.* Routledge.

Young, I.M. (1990). Five faces of oppression (Chapter 2). In I.M. Young, *Justice and the Politics of Difference.* (pp. 39-65). Princeton, N.J.: Princeton University Press.

Zuboff, S. (2019). *Age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

Chapter 4

The Tension between Professional and Personal, and the Age of Measurement

The previous chapter, Chapter 3, discussed a novel methodology, interlocking surveillance, which bridges surveillance studies and feminist approaches to understanding sites of surveillance. This methodology is applied in this chapter to the data collected from the textual corpus analysis, screening surveys, and interviews. The analysis done in this chapter identifies themes and trends that link the initial communication of biometrics to consumers and institutions, to those who use the technology in healthcare (neonatal nurses) through individual accounts (those interviewed).

The information in this chapter works to answer: How do neonatal nurses define biometric technologies? What are neonatal nurses' perceptions and usage of biometric technologies? Chapter 4 is a compilation of responses from the questionnaire and interviews, as well as the textual corpus, where interlocking surveillance is applied as a methodological framework. The goals of the analysis lead to understandings of the ways technical communicators may resist and intervene in communicating awareness, advocacy, and transparency in the site of surveillance: healthcare. The chapter is organized by summarizing interlocking surveillance, overviewing the corpus and questionnaire, discussing how the emerging themes of compliance, security, and efficiency manifested in the questionnaire, and bridging the themes to further explore how the interviews with neonatal nurses connect to the corpus.

4.1 Summary of Interlocking Surveillance

To reiterate, the framework of interlocking surveillance begins with my definition of surveillance: the collection of both visible and invisible data/information derived from those

being observed, suggesting an application of power over the observed audience, who are often not informed of such collection; and an adopted definition of intersectionality originally coined by Kimberlé Crenshaw in 1989. Intersectionality[52] is an understanding of oppressive structures as "intersecting, interlocking, and inseparable" (Walton, Moore, & Jones, 2019). Such structures recognize situated identities such as those influenced by race, gender, class, sexuality, that societal injustice is enacted differently. I categorize my methodological framework as an explicitly feminist framework of surveillance.

It is important to note that not all categories of the heuristic may be applicable to every site of surveillance, textual corpus, screening survey response/questionnaire, and interviewees for this study. Instead, the methodological framework may be used as a helpful guide in analyzing how surveillance scholars understand sites of surveillance (Lyon, 2007) as well as technical communicators' role in decision-making processes through the promotion of awareness, advocacy work, and transparent language/practices. Technical communicators are in unique positions to analyze and inform audiences of the varying degrees that surveillance is applied to bodies using interlocking surveillance as a framework.

[52] Intersectionality: "a metaphor for understanding the ways that multiple forms of inequality or disadvantage sometimes compound themselves and create obstacles that often are not understood among conventional ways of thinking" (Crenshaw, 1989, p. 149)

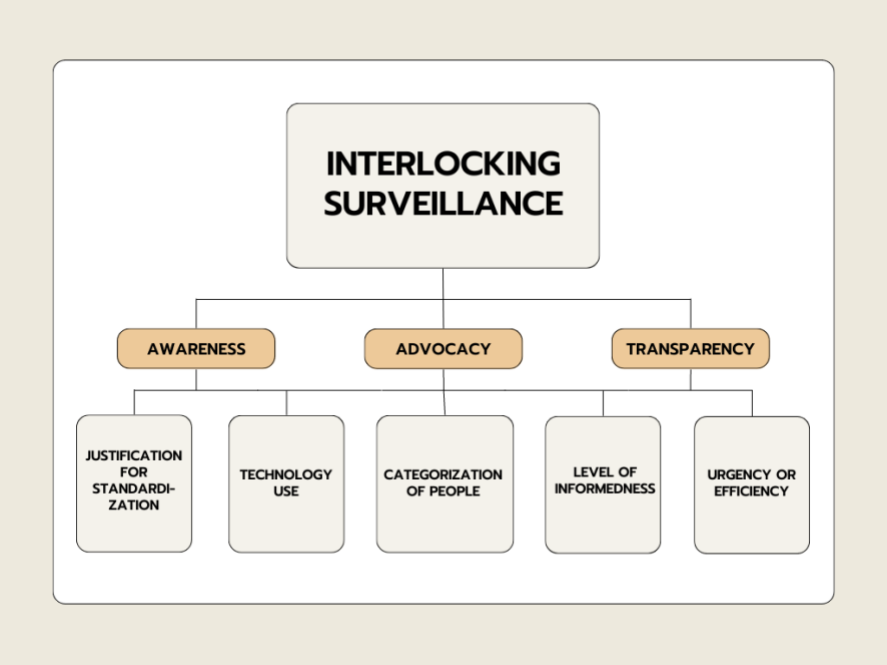


Figure 6: Interlocking Surveillance Framework Visual

The following is an analysis of a multiple-methods approach which relies on textual corpus analysis, a screening questionnaire, and interviews. One potential challenge of the coding schema and methodological approach is that researchers "bring our own perspectives, backgrounds, and experiences to our work—our stance and positionality as individuals, students, researchers, professionals" (Blakeslee & Fleischer, 2019, p. 180). Because of this, the approaches to coding influence how we look at our data and what we see in them (Blakeslee & Fleischer, 2019, p. 180). Therefore, I approached coding through creating my own methodological framework that relies on feminist methodological principles while also intersecting with surveillance studies approaches to analyzing data. I aim to walk readers through how I coded and analyzed data throughout this chapter so readers may understand how the framework was applied. Data is a record, particularly of our social world which is "mediated through decisions made about what or whom to include and exclude" (Guyan, 2022, p. 20). Especially when analyzing based on *levels of informedness*, for example, the coding

predominantly focused on the assumed levels of informedness that consumers would have about the biometric technology based on the website's materials.

4.2 Corpus Analysis

From the following information collected from the corpus, screening survey, and interviews, scholars may be able to determine how technical communicators can advise practitioners to engage in feminist acts such as collaboration, empathy, and the ability to interpret "patient 'language'" (Batistatou et al., 2010, p. 243). The collected information and analysis leads to conclusions about practicing medicine in a manner that not only improves patients' health outcomes but does so in an empathetic, compassionate way that raises levels of awareness, promotes patient advocacy, and is transparent for all stakeholders within the site of surveillance.

According to BiometricUpdate, there are over 400 biometric solutions companies listed in the world. As this is being written (and published), I am positive there will be many more companies listed/emerging than this. For example, when I began this study in 2022, there were about 400 United States-based companies listed on Security Informed[53]. This number is up to 481 companies in the United States. BiometricUpdate tracks biometric news and emerging companies across the world, and categorizes the companies by solutions:

> access control, behavioral biometrics, biometric cards, biometric software, biometric consultants, border management, biometric testing, civil/national ID, criminal ID, digital identification, facial recognition, fingerprint recognition, iris/eye recognition, liveness detection, mobile biometrics, payment solutions, surveillance, temperature monitoring, vein recognition, voice biometrics, and workforce management.

Many of the categories listed overlap in theme, and there are some biometric solutions that are not listed at all. For the purposes of this study, I am focusing on the facial recognition, fingerprint recognition, and voice recognition categories. These categories are focused on since

[53] https://www.securityinformed.com/companies/biometrics-united-states-of-america/directory.html

they were documented (in the following section) as the most used biometric solutions by neonatal nurses. The methodological framework of interlocking surveillance is applied to the 15 biometric solution websites to better understand how these technologies are communicated to consumers. The table below (Table 5: Methodological Framework and Coding Language) maps how the framework is applied to the websites, including the language that was coded as it relates to the methodological framework.

Since the specific site of surveillance this study focuses on is healthcare, interlocking surveillance doesn't just guide technical communicators in unpacking the ways information (and audiences) can (or could) create awareness, engage in advocacy efforts, and redefine transparency; but also the discourse arrangement patterns that rhetoricians of health and medicine often theorize and intervene in. For example, interlocking surveillance as an explicitly feminist methodology focuses on *people* and the ways technologies impact *people* (through design, control, privacy, consent, and so forth). Technical communicators have written about improving health and medicine, especially as it impacts peoples' health and well-being (Arduser, 2017; Elmore, 2013). This table (Table 5: Methodological Framework and Coding Language), which is also located in Chapter 3.5 (Table 4: Methodological Framework and Coding Language), outlines the ways the methodological framework of interlocking surveillance analyzes the language that biometric companies utilize to communicate to consumers and users. This language is specifically collected from the 15 biometric solution websites. The goal of the methodological framework is to call attention to the ways technical communicators may make suggestions and intervene in processes to advocate (for patients and users), create awareness (through accessible language and materials), and communicate transparency (about data collection and practices).

Table 5: Methodological Framework and Coding Language

Methodological Framework (Interlocking Surveillance) → Awareness, Advocacy, Transparency	Coding Language Based on Corpus → Themes of Compliance, Security, Efficiency
What are the intended purposes of the technology?	Safety; Security; Efficiency "quick; time; attention"; Solutions to Help You Succeed
How does the corporation justify its standard usage?	Customer Satisfaction; Employee Engagement; Data Security and Compliance; Customization; Cost Reduction
How does it categorize people and into what categories (and for what purpose)?	"Acceptable" Customers and Those Who Are Fraudulent; Identity Theft
How does the corporation justify its technological usage?	Data and Access Control; Compliance; Transaction Authorization; Identity Verification; E-Signature Provision; Out of Band Authentication
How are people informed about the capabilities, data collection, and more?	Third Parties; Privacy Policy; Terms and Conditions; Biometric Data Policy
Is the technology poised for efficiency purposes, or implemented during a time of "urgency"?	Fraudulent; Security checks; Customer experience; Patient Experience

Based on this framework and subsequent language pulled from the corpus, I categorized the data based on major themes of **compliance, security, and efficiency/convenience,** and applied the language to major takeaways from the three major biometric solutions that neonatal nurses use in their roles. The language that follows the three major categories are concepts, documents, and terms copied directly from the corpus (biometric solution websites). Many of the terms are fragmented, however, the list helps to showcase how I coded and understand compliance, security, and efficiency based on the corpus. I found that in the collected textual corpus, biometric companies utilized language that I classified and categorized into three major categories:

- **Compliance** generally refers to following set rules, regulations, and laws that relate to [healthcare] practices. Examples in the corpus include reference to compliance protocols; legalese such as HIPAA; privacy policy and terms and conditions; and customer satisfaction/employee engagement.
- **Security**, defined as protection or measures taken to guard against unauthorized entities from accessing information, accounts, or other personal information. Examples in the corpus include references to identity theft; fraudulent; safety; security; verification; identification and authentication.
- **Efficiency/Convenience**, which technical communicators have extensively critiqued (Frost, 2016; Blake, Longo, & Wills, 2006), often refers to the ability to complete or produce something quickly without wasting materials, time, or energy. Examples in the corpus include references to cost reduction; quick; time; and success.

The analysis of the corpus and interviews with neonatal nurses are integrated together in this chapter beginning in section 4.5, and further sorted by the top three most used biometric solutions by neonatal nurses: facial recognition, voice recognition, and fingerprinting. I analyzed the corpus and interviews together to showcase how nurse perceptions and usages of biometric solutions aligned (or didn't align) with the ways companies are communicating the specific solution. For example, the chapter has three main components or sections that focus on themes of compliance, security, and efficiency as they are discussed and applied to voice, facial, and fingerprinting solutions. These themes are applied to the questionnaire as well, which are analyzed in sections 4.3-4.4. The overall chapter documents the claims that biometric technologies are understood based on their communication materials, which alleged the solutions are secure, efficient, and in compliance with regulatory measures. The documentation of how

biometric technologies are understood leads to interlocking surveillance's goal of providing insights into awareness, advocacy, and transparency in the specific site of surveillance: healthcare. How so? The language documented by the corpus data informs how neonatal nurses respond to biometric technologies, not only based on their experience, but also because of the ways biometrics are communicated and positioned. Technical communicators can take away insights about awareness based on both neonatal nurse response to defining and using biometrics in healthcare, as well as how they assume their patients would respond to biometric usage. Further, the framework's questions help to uncover the holes (or concerns) in the seemingly "transparent" practices of biometric companies, as determined by their communication materials. The heuristic moves towards advocacy, exploring how technical communicators can intervene in design, implementation, and communication as it relates to biometric technologies in healthcare.

Before combining my analysis of the corpus and neonatal nurse interviews, it is important to understand not just *how* neonatal nurses are defining biometric technologies and personal information, but also *what* solutions they use, and *where.* This information was collected from my original questionnaire (screening survey) and helps to frame the ways nurses may be understanding and communicating about the biometric solutions they employ (and are employed on them).

4.3 Questionnaire (Screening Surveys)

This section focuses on providing context for how neonatal nurses define, use, and understand personal information and biometric technologies within healthcare. The information is pulled from three questions from the questionnaire. The goal of this section is to provide a background about the connection between neonatal nurses and biometrics, which informs the connection between the collected corpus of biometric solutions (voice, facial, fingerprinting),

and the interviews with nurses across the United States. The three questions included from the questionnaire in this analysis are:

- As a neonatal nurse, where/how have you engaged with biometric technologies within healthcare (broadly defined)? (Q6)
- This study is examining the use of and perceptions of biometric technologies, which are personal identifiers of the body that are collected for authentication purposes (commonly facial recognition, fingerprinting, palm scanners, and so on). What does the term biometric technologies mean to you? (Q4)
- In your role as a neonatal nurse, what does privacy or personal information in healthcare mean to you? (Q3)

In the Qualtrics Report 1, prior to Association for Women's Health, Obstetric, and Neonatal Nurses (AWHONN) Report 2 questionnaire, participants reported that facial recognition, fingerprinting, and voice recognition were the top three (based on percentage) most used technologies. Founded in 1969, the AWHONN organization is a 501 nonprofit membership organization, created to promote the health of women and newborns. The top three technologies reported were in response to the screening question (Q5) that asked participants to choose the technologies that their workplace employed. The questionnaire section is separated by two parts (Report 1 and Report 2), since there were two different screening surveys distributed in this study.

4.3a Report 1: Accessing Nurses through Social Media

The initial Report 1 survey listed 118 total responses, though the total responses collected varied for each question. Out of these, for the specific question about technologies that the workplace employed (Q5), the following pie chart (Figure 7: Report 1, Biometric Usage in

Healthcare (Q5)) displays the top 5 percentages (and technologies). This pie chart displays 33 total nurse responses that charted their usage of biometrics in their day-to-day role, such as fingerprinting (27.66%) and facial recognition (23.40%) as the most used biometric technologies by neonatal nurses within the workplace. The third most used technology in the workplace is voice recognition (19.15%) with palm scanners (17.02%) and skeletal tracking (12.77%) closely behind.

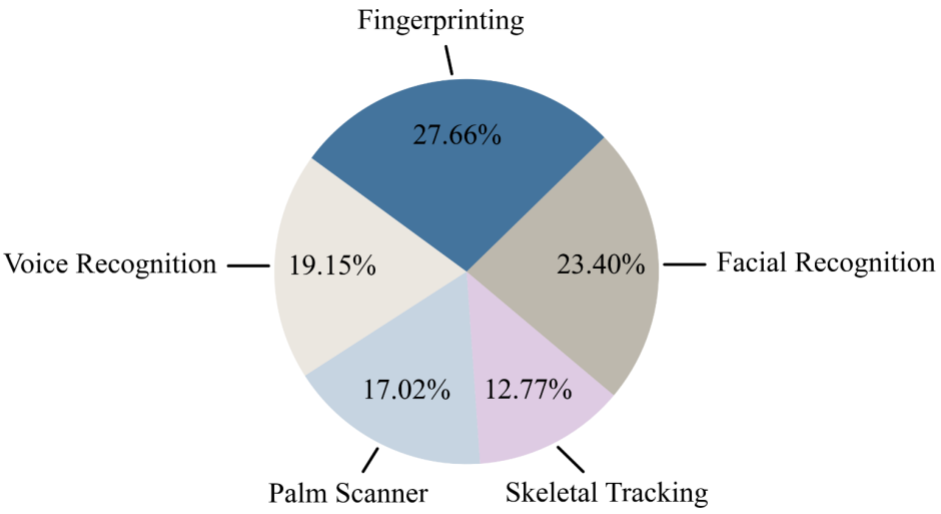


Figure 7: Report 1, Biometric Usage in Healthcare (Q5)

The percentages of most used biometric technologies were used to categorize and inform what biometric solutions websites were collected for the corpus. To elaborate on the most common biometrics utilized in healthcare by neonatal nurses, the questionnaire then asked nurses what the term "biometric technologies" meant to them. Q4 specifically stated: "This study is examining the use of and perceptions of biometric technologies, which are personal identifiers of the body that are collected for authentication purposes (commonly facial recognition, fingerprinting, palm scanners, and so on). What does the term biometric technologies mean to you?"

My personal favorite nurse definition was one word: “trouble.”

Trouble they are.

The following table (Table 6: Report 1, Question 4 Themes) is a representation of the commonly used words when neonatal nurses responded to Q4 or defining biometric technologies. This question received 33 responses, and there are overlaps with terms in nurses’ definitions. These generalized terms may assist technical communicators in understanding perceptions of biometric technologies in healthcare by the very people who utilize and are trained in using the technologies. Nurses referred to “technology” and “biometric” in their responses; however, I did not include the terms in the table because their response is a restating of the question. For example, a nurse wrote “biometric technologies generally refer to…” which suggests a restating of the question asking how nurses define biometric technologies. This table (Table 6: Report 1, Question 4 Themes) represents common verbiage that nurses used to refer to biometric technologies.

Table 6: Report 1, Question 4 Themes

Terminology used to Define Biometrics	**Percentage of Nurses Referencing the Term**
Characteristic	30%
Identity or identifying	Approximately 33%
Person	27%
Fingerprint	27%
Body	21%
Measurement and recognition	21%

As shown in the table (Table 6: Report 1, Question 4 Themes), for approximately one-third (33%) of the nurses, “identity” or “identifying” is a major part of understanding biometrics. The main purpose of their implementation in their roles is for the purpose of confirming the

patient is who they say they are. Further, through facial or fingerprinting technologies (predominantly), biometrics collect the patients' information to match "characteristics." Nurses also referred to terms such as "measurement" and "recognition" to define biometric technologies; the tools are able to confirm the person is who they claim to be, thus providing the nurses with "easy" access to the patients' charts and records. The following are some examples of the common verbiage nurses used to define biometrics.

Table 7: Questionnaire Report 1, Question 4 Quotes

Quotes from Nurses: Questionnaire Report 1, Question 4
Biometrics is the analysis of unique biological and physiological characteristics with the aim of confirming a person's identity. The five most common types of biometric identifiers are fingerprints, facial, voice, iris, and palm or finger vein patterns.
Biometric is the measurement and statistical analysis of people, unique, physical and behavioral characteristics
Is to identify a person based on some aspect of their biology. Fingerprint recognition is one of the first and original biometric technologies that have been grouped loosely under digital forensics.
Biometrics usually refers to automated technologies for authenticating and verifying human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements.
Biometric technologies generally refer to the use of technology to identify a person based on components of their body.
It means electronic security identifiers.

To reiterate, I define biometric identification[54] as any identifier of the body that is collected and used for personal identification (and authentication). I coined this definition prior to the dissertation study (and subsequent data collection). The influence of this definition comes from the long history of the implementation of biometric technologies within the United States

[54] Biometric identification: any identifier of the body that is collected and used for personal identification.

(as explored in 1.2 and 2.5). My definition was referenced in Q4 of the Reports (1 and 2), which may influence the way some neonatal nurses defined or referred to biometric identification. The neonatal nurses had similarities in the ways that they defined biometrics, in comparison to my own definition. For example, nurses did focus on identifiers of the body that are collected; however, they specifically *named* examples of identifiers (such as characteristics or specific biometric solutions). In their definitions, nurses also focused on how biometrics are "used" or implemented. For example, one nurse defined biometrics as "I would describe it as the measurement and analysis of unique human characteristics such as DNA, fingerprints, voice patterns, hand measurements, and eye retinas and irises." This example definition displays an overlap with my own definition by including specific identifiers that are collected from the body (i.e., DNA, fingerprints, voice patterns, hand measurements, and eye retinas and irises).

In terms of defining biometrics, the technologies should not be "regarded in isolation or as a technique that is completely new" (because they aren't!), but rather in "relation to its predecessors so as to understand the continuities between them and establish what is particularly new about biometrics" (Ajana as interviewed by Beer, 2014). One aspect of the included definitions by neonatal nurses that was different from my own definition, emphasized "measurements," "calculations," and "analysis." From an etymology perspective, this makes sense: *metric* refers to measurement, whereas *bio* refers to relating to living things. Thus, measuring living things (bodies) = *biometrics*. Whether we are talking about work performance, lifestyle and health, budgeting, security, marketing, and so on, all areas of life seem to be penetrated by the age of measurement. Related to "health," we measure our steps, our calories, weight, height, everything. Ajana mentions that with the development of new technologies, new forms of measurement are emerging; however, measurement is not something new (as quoted in

Beer, 2014). I understand *how* and *why* the neonatal nurses included the term "measurement" in their definition, especially in terms of their careers, responsibilities, and more. Measurement was curious to me as a response because 7 nurses out of the 33 responses (21%) included the term as part of their definition. What is being measured? Analyzed? Is the biometric solution in relation to the repository—to prove you are who you say you are? History is filled with examples where "records, numbers and measurement have been instrumental to understanding and intervening in the social world, and to defining what is normal and what is deviant, oftentimes with material consequences" (Ajana as quoted in Beer, 2014). Nurses view (and define) biometric technologies as a way to record or measure patients: whether the measure is about identity (are you who you say you are), or personal identifiers such as voice and fingerprints. Further, as the following sections will discuss, "normal" and "deviant" have long defined and justified the usage of biometrics. Are you who you say you are? Are you "in compliance?" Not only will the following sections document how companies use this language to communicate to users and consumers, but they also will further elaborate on the nurses' definitions of biometrics as documented by the questionnaire. These definitions guide neonatal nurses' approaches to perceptions of biometrics in healthcare, and their own personal relationship and experience with the technologies.

Further, nurses defined biometric technologies in terms of "safety" and "security," as well as "authentication" purposes. There is overlap with understanding authentication and identification: as discussed in Chapter 2, biometric technologies have a long history of implementation as a means to not just identify but authenticate that the person (body) is who they say they are. Safety and security may be the underlying goal or intention of biometric technology; however, this was separate from my own definition. In fact, one of the aspects of biometric solutions that I have questioned thus far is how biometric solutions are touted as "safe"

and "secure." But for whom? And from whom? It can be assumed that one of the major reasons nurses discussed safety and security in their definition is due to the legal ramifications they may face if they do not remain in compliance and/or keep their patients safe. Interviewees, which will be referred to in sections 4.5-4.7, mentioned for example, that one of the major benefits of biometric technologies are the safety feature: infants won't be swapped, patient records won't go missing, people who are allowed to access certain files, doors, and more will have that access. Security for nurses wasn't just about personal identification as my definition suggests, but it was about the literal protection of the people (mostly infants, but mothers as well) they were expected to attend to. Apart from complying with security legalese such as HIPAA, nurses included biometrics in their definitions because of the ways they viewed their roles.[55] While only one nurse explicitly mentioned "safety" in their response, the implications of security, or protection, were staggering. This could be categorized by the ways in which 79% of neonatal nurses in Report 1 referenced "care" or "caring" for their patients as part of their roles and responsibilities (Q1). If neonatal nurses believe that they should care for their patients, then it may follow that part of "caring" for someone is "protecting" them or keeping them secure. The reference to security and safety in defining biometric technologies, tech that nurses use in their day-to-day to identify patients and collect their information, displays that even when nurses use technologies in their jobs, their responsibilities are still to keep their patient safe (even if that is a perceived level of safety).

In terms of safety and security, which will be mentioned further in the next section, nurses also discussed personal information and privacy (Q3) in terms of "maintaining the security and confidentiality of patient records." This particular question will also be discussed in

[55] Q1 in the questionnaire: Describe your responsibilities as a neonatal nurse.

4.4, where the questionnaire will be analyzed based on how themes of compliance, security, and efficiency manifest. Here, readers will further read how neonatal nurses discuss how they understand biometrics and personal information. For example, as one nurse in the questionnaire writes: "Protecting the integrity of the babies and that of the parents, maintaining confidentiality of all patient information, both personal and clinical, in the work setting and off duty in all venues, including social media or any other means of communication."

The following section focuses on Report 2 of the questionnaire, which differed in both quantity (how many people took the screening survey) and nurse definitions of biometric technologies.

4.3b Report 2: Responses from a Nonprofit

For the screening surveys, I also distributed a survey through the Association of Women's Health, Obstetric, and Neonatal Nurses (AWHONN) email list (Report 2). The survey was separately distributed, and I refer to the report as Report 2 to document the differences in responses from my distributed survey through social media channels (Report 1), versus the responses targeting neonatal nurses through a nonprofit organization dedicated to people in the profession (as discussed in Chapter 3). I kept the Qualtrics survey questions the same, but the reports separate because I was curious to see if there were any major discrepancies between a sample of neonatal nurses and a specifically targeted organization for neonatal nurses. It's difficult to account for why there was such a difference in the responses from Report 1 and Report 2; however, the information may help technical communicators think about design concerns, audience awareness, and decision-making protocols for the creation, communication, and usage of biometric technologies.

For example, out of the 28 responses submitted in Report 2, the 8 nurses that responded to Q5 reported that their workplace employed fingerprinting (33.33%), vein scanners (22.22%), and/or no biometric technologies usage (33.33%) as the top three responses with other as (11.11%). This was starkly different from the top three biometric technologies that participants cited using in Report 1, which were facial recognition, voice recognition, and fingerprinting technologies. It's difficult to say for sure why nurses in this report were different than the previous report; however, I might imagine that nurses who are associated with a professional organization might also overlap in working in higher education, for example. These nurses could also be finishing up schooling themselves. The neonatal nurses in Report 2 may understand what biometric technologies are much differently than those who do not belong to a professional organization. This is *pure speculation*; however, I could imagine the nurses who belong to the professional organization may work part-time or are used to working in settings that may not be implementing the most recent emerging technologies into their system.

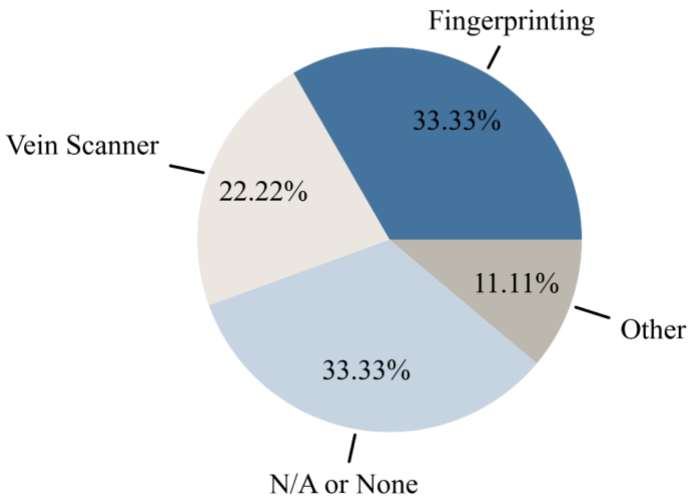


Figure 8: Report 2, Biometric Usage in Healthcare (Q5)

To highlight the protection of confidentiality and gain patient trust, I asked neonatal nurses about their usage of biometric technologies. Q4 of Report 2 stated: This study is examining the use of and perceptions of biometric technologies, which are personal identifiers of the body that are collected for authentication purposes (commonly facial recognition, fingerprinting, palm scanners, and so on). What does the term biometric technologies mean to you? The neonatal nurses from Report 2 said the following examples documented in Table 8: Questionnaire Report 2, Question 4 Quotes.

Table 8: Questionnaire Report 2, Question 4 Quotes

Quotes from Nurses: Questionnaire Report 2, Question 4
"Omnicell- medication administration."
"iPhone- facial recognition.
"The scanning of identifying information of care providers for access to private property."
"Facial recognition like the iPhone or fingerprint scanning like Pyxis or the iPhone."
"I just think of fingerprint scanners on a phone or electronic temperature monitors at time clock machines."
"I am not tech savvy, however; I did use hand scanning when doing my Nurse Exams and I felt like it was an accurate way to ensure you have the right person."

Report 2 differed greatly in response from Report 1 in the ways that the nurses described specific technologies, even those outside of healthcare. For example, one listed a specific medical administration, while others listed iPhones and their facial recognition capabilities. Separate from what was listed were the electronic temperature monitors.

To provide further context into how nurses define or understand biometric technologies, Q3 asked nurses to describe what personal information and privacy meant to them in their roles as neonatal nurses. Nurses discussed topics very similar to how they defined biometrics, as embedded in their responses about personal information. For example, one nurse said that

personal information means “I do not discuss or talk about my patient unless I am authorized to. I ask names, I ask for identification, and I discuss nothing over the phone.”

Further, nurses brought up security concerns such as how personal identification may pertain “to the patient; it can mean any documentation that, if found by others, could compromise that patient's rightful, personal privacy. This could mean admission paperwork with names or MRN. It could also mean my posting a particularly detailed account of my day on a social media site. Either could compromise a patient's information or trust in healthcare.” Nurses continued to emphasize care in relation to their patients and their families. For example, one nurse mentioned that “Information is kept confidential to the mother or father of the baby, and care team. Social workers and care coordinators could become involved. But questions asked by friends or extended family. That information needs to be given out by the parents.” Nurses took care to mention their own role in the privacy process, or the ways they could/couldn’t share information.

Overall, this section provided context for how neonatal nurses define, use, and understand personal information and biometric technologies within healthcare. The goal of the section was to provide a background about the connection between neonatal nurses and biometrics, which informs the connection between the collected corpus of biometric solutions (voice, facial, fingerprinting), and the interviews with nurses across the United States. The following sections explicitly discuss how the themes (compliance, security, and efficiency) pulled from the collected corpus may be applied to the questionnaire.

4.4 How Compliance, Security, and Efficiency Manifest in the Questionnaire

This section builds off the corpus themes of compliance, security, and efficiency to apply such themes to the questionnaire. This guides technical communicators in understanding (and

contributing) how the corpus materials connect to how nurses define and perceive biometrics, and further, how the nurses discuss biometric technologies in the interviews.

As mentioned, a majority of nurses in both Report 1 and Report 2 defined biometric technologies in terms of examples of them. For example, 12 out of the 33 (37%) reports from Report 1 (Q4) defined biometrics by mentioning specific technologies such as eye scanners, fingerprinting, facial recognition, and/or hand scanners in their response. Nurses also defined biometric technologies based on identification and authentication, and to measure human characteristics. The following screening survey and interview information assists in determining: How do neonatal nurses define biometric technologies? What are neonatal nurses' perceptions and usage of biometric technologies?

One of the major themes that biometric solutions referred to in the textual corpus was in relation to compliance. I specifically focused on two questions from the screening survey to understand how neonatal nurses defined personal information and privacy (Q3), as well as biometric technologies (Q4). I selected responses from the 33 responses that specifically focused on compliance: that is, language that displayed the nurses' understandings of legal issues such as HIPAA, or compliance as it related to their job (such as their role or responsibility). Nurses also discussed compliance efforts through communication materials. For example, the nurses interviewed talked through how they communicate with patients verbally about usage of biometrics, rather than including written materials. Not only is a lack of written material not accessible for all patients, but communication is often complicated by the hustle of the hospital. Patients are in a particularly vulnerable population in the hospital already, complicated further by a potential lack of choice in opting out.

To further complicate the relationship between understanding biometrics and their usage, and personal information and privacy, neonatal nurses were asked to define what personal information or privacy means to them. The following (Table 9: Compliance, Security, Efficiency, and Interlocking Surveillance) are some pulled responses from Report 1 that document nurses' definitions, representative of the coding schema, framework, and the total sample of responses collected from nurses.

Table 9: Compliance, Security, Efficiency, and Interlocking Surveillance[56]

Quotes from Nurses	**Language related to themes/framework**	**Themes and Interlocking Surveillance Framework**
Protecting the security of data in health research is important because health research requires the collection, storage, and use of large amounts of personally identifiable health information, much of which may be sensitive and potentially embarrassing.	Protect Personal Data Identifiable Sensitive	Security and Compliance *Justifying technological usage* *Purpose of technology*
Entails a set of rules and regulations to ensure only authorized individuals and organizations see patient data and medical information. It can also refer to an organization's processes to protect patient health information and keep it away from bad.	Rules and regulations Patient data Processes	Compliance and Security *Justifying technological usage* *Purpose of technology* *Standard usage*
Morally, the obligation to keep patient information confidential is linked to a respect for patient **autonomy** and a prerequisite for **trust**.	Confidential Autonomy Trust	Compliance and Security *Levels of informedness*

[56] Elements of Interlocking Surveillance are italicized in the "Themes and Interlocking Surveillance Framework" column.

It means everything to me. It is a nursing principle. The worth, integrity, dignity, uniqueness, and human rights of patients, employers, colleagues, students, employees, parents, and families of the infant will be respected regardless of ethnicity, gender, social/economic status, or physical or mental challenges.	Integrity Human rights Principle	Compliance and Efficiency *Categorize people*
Privacy to me means keeping the information gotten from the patient confidential without discussing it or sharing it with anyone else but in and **outside** of my workplace.	Confidential	Compliance and Security *Levels of informedness*
Confidential patient information is information that both identifies the patient and includes some information about their medical condition or treatment.	Confidential Identifying Treatment	Compliance and Security *Justifying technological usage* *Purpose of technology* *Standard usage*
Protecting the **integrity** of the babies and that of the parents, maintaining **confidentiality** of all patient information, both personal and clinical, in the work setting and off duty in all venues, including social media or any other means of communication.	Integrity Confidentiality Patient Information	Compliance and Security *Standard usage* *Categorize people*
Not **disclosing** information unless directly working with patients.	Disclosure	Compliance *Levels of informedness* *Justifying technological usage*
Patient and family's right to privacy involving current and	Right to privacy	Compliance and Security

past medical, social and personal situations.		*Levels of informedness* *Urgency*
HIPAA is very important. You only give information **necessary** for the care of your patients.	HIPAA Necessary	Compliance, Security, Efficiency *Levels of informedness* *Standard usage* *Urgency*

Though the table above (Table 9: Compliance, Security, Efficiency, and Interlocking Surveillance) charts examples of responses from neonatal nurses and how the language was coded to determine themes such as compliance, security, and efficiency, I also noticed the ways in which the nurses' responses were attuned to my methodological framework. For example, the following table (Table 10: Nurses Referring to Themes (Q3, Report 1) documents percentages of the *total* responses to Q3 which focused on definitions of privacy and personal information. It is important to note that responses were often coded twice, as the nurses would refer to issues of compliance *and* security, for example. I refer to Q3 in Report 1 because there were the most responses, and a geographically wide range of nurses across the nation participated in this screening survey.

Table 10: Nurses Referring to Themes (Q3, Report 1)

Theme	**Percentage of Nurses (out of 33) Referring to Theme (Q3, Report 1)**
Compliance	13/33 or 40%
Security	17/33 or 52%
Efficiency	7/33 or 21%

These percentages make sense: if someone asked you how to describe privacy or personal information, it is likely that, as suggested, more than half of the reported responses would refer

to security or safety measures. In fact, despite privacy and security concerns having lots of overlap, these terms are different. Often security measures are put in place to *protect* privacy. For example, Tham and Duin refer to privacy in terms of having control over the extent, timing, and circumstances of sharing oneself physically, behaviorally, or intellectually with others (Beck & Hutchinson Campos, 2021, p. 95). Relationally, security is defined by Merriam-Webster dictionary as "freedom from danger," or "protection; measures taken to guard against espionage or sabotage, crime, attack, or escape." Often the difference lies between placing safeguards to prevent unauthorized people from accessing information, accounts, or other similar things (also referred to as maintaining your privacy).

Some of the terms pulled from the responses above such as HIPAA, necessary, disclosing, integrity, confidentiality, encryption, morally, trust, autonomy, and outside were language that are included in the coding table. Nurses reported that legalities or *compliance* measures, such as HIPAA, led them to consider the implications of breaking such a law within the workplace. For example, one nurse noted that, "HIPAA is very important. You only give information necessary for the care of your patients." I coded this response within the themes of compliance, due to the legalese with HIPAA and the nurses' urge to comply, as well as *security*, due to the distribution of information for patients. Further, this response may be understood through the methodological framework as attending to urgency, levels of informedness, and standard usage. Levels of informedness may be determined by how nurses are aware of the information about patients they are able to disclose. It seems that protection under HIPAA occurs in the eyes of the law, society, and even morally by nurses, yet biometric data is detached from this protection. It seems that nurses consider the ways they disclose based on the legalese involved with HIPAA, but this does not extend as concretely to maintaining the same laws and

principles for biometric disclosure[57]. Nurse responses to urgency is determined by the emotion associated with HIPAA being "very important." Perhaps, if HIPAA is so important to nurses to follow, then this is one area of intervention to amend the Act to account for digital and emerging technologies in healthcare. Standard usage of the technologies were determined by nurses responding to how the biometric is "necessary" in the sense it is used for the care of the patient. I also saw responses such as, "HIPAA is very important. You only give information necessary for the care of your patients" as overlapping with all three themes (compliance, security, efficiency). Not only was "HIPAA" mentioned (as a compliance measure), but also "information" (in terms of security), as well as "necessary" which may be viewed as efficiency for nurses to determine when/why a patient would need information disclosed. These responses also attended to interlocking surveillance's categories of levels of informedness (as documented by how nurses understand HIPAA), standard usage (why personal information is a necessity), and urgency (when to disclose or share).

Not only did topics such as consent with disclosing information and maintaining integrity arise, but curiously enough nurses also discussed how privacy occurs not just within the workplace. A majority of the neonatal nurses reported that privacy and personal information means keeping information confidential both inside and outside of the workplace. This for them meant not sharing or discussing the information. Yet during my interviews, the key component with the usage of biometric technologies *is* sharing. One nurse claimed personal information means, "Protecting the security of data in health research is important because health research requires the collection, storage, and use of large amounts of personally identifiable health

[57] See the Privacy and Security Rules: https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

information, much of which may be sensitive and potentially embarrassing." Neonatal nurses mentioned that a large appeal of the biometric technology in healthcare was to assist nurses with their day-to-day. Since the shifts often rotate, there is in fact a sharing, disclosing, and distributing of patient information. The usage of biometric technologies by nurses seems to create a sense of detachment; that is, since a technology is mediating the interaction between nurse and patient, there is a detached responsibility. The detachment occurs because nurses state that their responsibility is to care for the whole patient; however, they do not view technologies involved in the interaction as potential *threats* to the patient's safety.

The questionnaire provided evidence for the collected corpus results that suggested companies communicate biometric solutions based on adherence to compliance, for security and safety, and efficiency and convenience. The Report 2 nurse responses to the privacy and personal information Q3 overlapped with Report 1. For example, the neonatal nurses in Report 2 found similar definitions and concerns with patient rights, personal privacy, and providing confidentiality: "Regardless of the area of nursing, working in privacy and personal information is important for patients and their families." This response from the questionnaire depicts the methodological framework's understanding of categorization of people (such as patients and families), as well as justification of the usage of technology (maintaining privacy and personal information).

The following tables (Table 11: Compliance, Nurse Engagement with Biometrics (Q6) and Table 12: Efficiency, Nurse Engagement with Biometrics (Q6)) further analyze themes of compliance, security, and efficiency as they relate to interlocking surveillance. The answers are collected from the questionnaire from Q6: As a neonatal nurse, where/how have you engaged with biometric technologies within healthcare (broadly defined)?)

Table 11: Compliance, Nurse Engagement with Biometrics (Q6)[58]

Compliance	Pretty normal; we were trained on how to use it.	*Justify Standardization / Levels of Informedness*
	When interacting with patients that becomes a major thing to be done also personally, I use the gadgets e.g. For recognition.	*Categorizing People*
	As a neonatal nurse, I have engaged with biometric technologies in restricted zones for employees only within my workplace facilities, which serves as a means of identification and gives me access to private spaces.	*Specific Technological Use*
	I have engaged with biometrics in my workplace to help access confidential information of patients, it has helped prevent fraud or unauthorized access to individual information.	*Urgency Or Efficiency of The Technology*

Ultimately, I selected these responses from the questionnaire since in the following sections the quotes will be used to help guide the specific sections (compliance, security, and efficiency/convenience) through understanding how neonatal nurses in *interviews* elaborated on their *questionnaire* responses. For example, neonatal nurses elaborated on the ways biometric technologies were *justified* to them through training materials in the healthcare settings. Further, compliance was communicated through nurse responses to understanding *specifically* what technology they used and for what purposes, such as identifying and categorizing people (patients). These pulled responses identify aspects of applying the methodological framework,

[58] Elements of Interlocking Surveillance are italicized in the third column from the left.

interlocking surveillance, to help situate understanding of healthcare as a site of surveillance and how nurses (technical communicators) may provide suggestions for advocacy, awareness, and transparency.

I included the following response from a nurse in the compliance section, "As a neonatal nurse, I have engaged with biometric technologies in restricted zones for employees only within my workplace facilities, which serves as a means of identification and gives me access to private spaces" because this response displays how nurses engage with specific technology usage (as classified by interlocking surveillance) in "restricted zones." This response suggests that the technology is specifically used for zone access, and further, compliance through identification (is this person allowed in this space?). I also included this response over some of the other responses because it encompasses what many of the nurses spoke to or alluded to in their responses. For neonatal nurses, issues of safety and compliance are important to them. Not only do the nurses value compliance in terms of employee expectations such as utilizing biometrics to not just confirm their identity, but also because their employer expects them to comply with this technology for their job (never mind the added legalese with compliance for healthcare protocols). Nurses don't just value the safety of their patients, but also themselves. Nurses discuss this more in their interviews (4.5-4.7). Further, neonatal nurses referred to themes of compliance and safety through defining privacy in terms of physical spaces. For example, the nurse quoted above from the questionnaire mentioned using biometrics in "private spaces," as did nurses who referenced not sharing "private" information outside of expected spaces (including digital) to remain in compliance. It was also curious to view how nurses spoke about their usage of biometrics in healthcare in reference to physical spaces (27%), versus patients (64%). Since the question asked where/how neonatal nurses engaged with biometric technologies

within healthcare, and considering the rise in employee identification and authentication, I expected more nurses to mention their own identification *along* with how they used the technologies for patient identification.

Alongside compliance, nurses also discussed how technologies were efficient or convenient to use within the workplace. This extended past patients, to the roles and responsibilities in the day-to-day of neonatal nurses. For example, one nurse mentioned in response to (Q6), "As an employee in my organization, the main source of easy identification of patients and employees is greatly characterized by the biometric technologies." This response was coded as efficiency because of the ways the nurse mentioned its "easy" identification and furthermore is classified by interlocking surveillance as the site of healthcare showcasing biometric technologies and their urgent implementation. The response suggests that the nurses "need" the technology for "identification" purposes that would otherwise be difficult without.

Table 12: Efficiency, Nurse Engagement with Biometrics (Q6)[59]

Convenience/Efficiency	When getting details or the **true identity** of a patient.	*Categorizing People*
	Patient identification especially for newborns **Easier identification** of patients at hand in respect of trying to avoid duplicate records Considering my line of work, I have used the system in telehealth, as it helps me to safely and securely login to the portals.	*Justify Standardization / Specific Technological Use*
	As an employee in my organization, the main source of **easy identification** of patients and employees is	*Urgency Or Efficiency*

[59] Elements of Interlocking Surveillance are italicized in the third column from the left.

	greatly characterized by the biometric technologies.	

Neonatal nurses also mentioned in interviews, which will be discussed in the next section, biometrics are poised as a convenience for their job. For example, one nurse[60] said, "Plugging in your 5-digit code with your fingerprint is a lot easier than plugging in your entire email with a password in order to get medication in an emergency." This makes sense: it *is* faster and more convenient to plug in a code rather than an entire email and password. However, the convenience and assumed efficiency of the biometrics fail to account for the long-term effects of using this technology. The trade-off for convenience or "efficiency" extends far past privacy, as previous chapters suggest.

Overall, neonatal nurses largely cited utilizing biometric solutions for efficiency and convenience's sake. Though voice recognition, facial recognition, and fingerprinting were the most popular biometric solutions nurses utilized in their day-to-day, eye tracking (referred to as iris recognition) was also mentioned as a software that nurses used (especially for convenience). For example, one nurse mentioned: "As a neonatal nurse I have also used eye tracking where I can comprehensively address a patient's concern more easily and efficiently."

The pulled responses identify applied parts of the heuristic, interlocking surveillance, to help situate understanding of healthcare as a site of surveillance and how nurses (technical communicators) may provide suggestions for advocacy, awareness, and transparency. These responses also show how neonatal nurses define biometrics, which relates to how biometric companies communicate their solutions, as well as where and how they use the technologies. The responses also help to understand what personal information means to neonatal nurses in terms

[60] Redacted (Interviewee E)

of their roles and responsibilities. The ways nurses discussed compliance and efficiency measures ultimately overlapped with security or safety concerns. For example, nurses communicated security concerns through categorizing people through record/fraud as it relates to identity, as well as justification of standardization as to why biometrics are implemented in healthcare: safety and security. For example, one nurse discussed usage of biometrics in terms of safety or security: "Access to medical records via fingerprint scanning which is crucial as privacy and confidentiality in this case is highly maintained. Signing in and signing out of duty."

As the response suggests, the justification of standardization is for signing in and out, which will lead (as documented by nurses) to privacy and confidentiality. The table (Table 13: Security, Nurse Engagement with Biometrics (Q6)) below includes responses to Q6 of the questionnaire, which notes how security and safety overlap with interlocking surveillance's understanding of how technologies are justified within healthcare.

Table 13: Security, Nurse Engagement with Biometrics (Q6)[61]

Safety and Security	The main entrance door and exit door to the building.	*Justify Standardization*
	Within the hospital's emergency rooms and intensive/special care units.	*Justify Standardization*
	It is used in systems such as national identity cards for ID and health insurance programs, which may use fingerprints for identification. Airport security. This field sometimes uses biometrics such as iris recognition.	*Justify Standardization / Urgency or Efficiency*
	I identify patients based on biologically unique traits	*Categorizing People / Specific Technological Use*

[61] Elements of Interlocking Surveillance are italicized in the third column from the left.

	(face, fingerprint, iris, voice) ensuring that care is provided to the right people, leading to a safer and more effective global health environment. When a patient enters a medical facility, a biometric search using their biometric data can confidently locate the corresponding identity in the master patient index. This search determines with a high degree of certainty if a record exists for that patient.	*Levels Of Informedness / Categorizing People*

These specific responses summarize what a majority of neonatal nurses stated: they used biometrics as a means of compliance with their job, while also maintaining patient security and efficiency's sake for their responsibility. For example, the nurse that responded, "I identify patients based on biologically unique traits (face, fingerprint, iris, voice) ensuring that care is provided to the right people, leading to a safer and more effective global health environment" may be labeled as identifying a specific technology use at the site of surveillance (face, fingerprint, iris, voice) as well as further categorizing people (right people) which would, as they suggest, lead to a "safer" environment. This language, as we will read in the following sections, depicts the ways in which the collected corpus directly links to how neonatal nurses are trained to use and perceive the biometric solutions within healthcare. Understanding communication materials from specific biometric solution companies and where/how the solutions are used in healthcare by neonatal nurses can provide context for usages and perceptions of the solutions within healthcare.

The trend here is that companies, as documented by the textual corpus, screening questionnaire, and interviews, do not ask consumers what they *need.* They create what they

believe the consumer will *want.* A *convenience* if you will. These technologies and assumptions justifying their use, as referenced through examples in Chapters 2 and 5, are ableist, racist, and beyond shoring up the issue to systemic problems, biometric technologies have a plethora of security and usability issues. For example, as Walton, Moore, and Jones, (2019) note, the design of such technologies contributes to the "visibility" and "invisibility" of dominant bodies by anticipating their needs (visibility) and allowing them to seamlessly fit into existing environments (invisibility). Bennett (2022) posits that the myths of neutral design, especially as they relate to biometric technologies, "naturalize the privilege of certain bodyminds and disregard the intersectionally complex embodiments and experiences of others" (p. 228). Nurses and patients care about their privacy, and as we will see in the following sections, the interviews only contribute to our understanding of the tension between professional obligation and duty, and ethical or personal reservations or concerns. In fact, aside from the ways nurses defined personal/private information, I also observed the neonatal nurses interviewed in this study discussing a tension between their professional role and its expected responsibilities and their own personal interests and feelings. As I claim in Chapter 5, I view neonatal nurses as technical communicators: they communicate and negotiate specialized information. Technical communicators can include a range of people, from academics to practitioners (such as the neonatal nurses), and more. Because technical communicators are often agents in decision-making processes, whether that is in the healthcare sector or work within the companies creating the biometric solutions, technical communicators may be better positioned to participate in the decision-making process, particularly in times of exigency more than the public, such as patients (Katz & Miller, 1996; Waddell, 1996). Technical communicators can use action research—"research [that] is contextual, local, and requires intervention, not simply description"—to

advance social justice and feminist agendas applicable to all sites of surveillance (Blythe, Grabill, & Riley, 2008, p. 273). The screening survey (questionnaire) responses proved to overlap all of the themes pulled from the textual corpus: compliance, security, and efficiency/convenience.

4.5 Compliance and Introducing Biometric Solutions

What follows are the scenarios used within the interviews, and neonatal nurse responses. This is helpful in framing the ways across the textual corpus, interviews, and screening surveys, major themes such as compliance, security, and efficiency were discussed. Throughout the rest of this chapter, the scenarios which were used as a second part to the interviews with neonatal nurses will be referred to as they relate to themes of compliance, security, and efficiency—and further classified by their connection to the biometric solutions (voice, facial, and/or fingerprinting). These interview scenarios help to provide context and evidence for the ways in which neonatal nurses perceive and use biometric technologies, which is why they are overviewed before some of the questions from the interview. During the interviews, there were two out of three scenarios that I would share with neonatal nurses. One scenario depended on the answers from the questionnaire, which helped determine whether or not the nurse was familiar with biometric technologies. This was determined by their answers to *where* they used the biometric technology in their workplace, and the multiple choice of *which* biometric technologies they used in their roles as neonatal nurses.

The first scenario presented in the second part of the interview was as follows[62].

> Researchers have developed a new technology that fingerprints newborns. This technology collects temperature, pulse, breathing and oxygen, and identifies the infant

[62] https://health.ucsd.edu/news/releases/Pages/2018-09-12-researchers-develop-biometric-tool-for-newborn-fingerprinting.aspx

> through their fingerprint. Let's imagine you have been told this technology would be implemented in a month…

This first scenario will be discussed in the fingerprinting sections of this chapter (4.6c and 4.7c). The second scenario presented to nurses in the interview focused on neonatal nurses' responses to imagining working (present or future) in a healthcare setting that has more access and usage of biometric technologies:

> Northwell Health, based in New Hyde Park, New York, United States, is a healthcare network made up of 23 hospitals and over 700 physician offices and urgent-care centers. Northwell began rolling out a biometric system using iris scanning and facial recognition technology from RightPatient Inc. Northwell is one of the first major medical systems in the United States to outwardly discuss and deploy biometric technologies—and, as such, have been widely lauded by online medical, technology, and business publications as a "pioneer" in medical innovation.

This scenario will be further discussed in the facial recognition section (4.7b). It is important to note that aspects of the scenario may also be briefly discussed in other sections of this chapter as they relate to compliance, security, and/or efficiency concerns.

Included in this section specifically is a brief overview of interview responses from neonatal nurses about compliance in healthcare as they relate to biometric technologies, to help frame the voice, facial, and fingerprinting sections. The chapter sections then chart voice recognition and examples of compliance from the textual corpus collected; facial recognition and examples of compliance from the textual corpus collected; and then fingerprinting and examples of compliance from the textual corpus collected. More than the collected corpus, the neonatal nurses' responses can be categorized by the methodological framework and how communication materials justify standardization (how do healthcare institutions communicate a need), specific technological use (what types of technologies and why are they used), categorizing people (based on identity: confirming identity or fraudulent), levels of informedness of nurses (and patients), and urgency or efficiency of the technology as it relates to compliance.

For example, during interviews, I asked nurses about their concerns with implementing biometric technology, if any, and why? Some responses focused on finances. Others focused on such technologies being complicated, which may be labeled as efficient or categorized by my methodological framework's focus on justification for technological use and standardization. For example, Interviewee I mentioned that despite nurses stating biometric technologies were efficient or convenient, compliance in terms of training to *use* the technology became a topic of inconvenience:

> It makes our job tough with training but then you'd be able to utilize them [biometrics] and understand. Knowing how to use the technology is hard to understand especially a new nurse coming in and not used to this technology. Someone who is using it for a while would make their jobs easier. Cons would only be with training and sometimes technologies can fail so that is another cons.

For some neonatal nurses in their specific healthcare system, biometric identification occurs manually rather than digitally. This manual recording, for example, identifies patients through wristlets (barcodes) or driver's licenses/passports; nurses claimed the manual method was an option if patients did not want to be digitally authenticated. Further, Interviewee I talked through inherent power dynamics, or the ways in which their expertise persuaded patients to "opt in":

> Of course, their power or lack of power means we can't use the technology. That is another con for this technology. Some people might just not be willing or able to accept this technology. It can be very hard to convince people to use it.

The language used to persuade was based on the communication materials *from* the biometric solution websites. This suggests that when nurses are trained on how to use biometric technologies, that the communication materials influence their discussion and reference to the technologies once interacting with patients. One of the themes that I pulled from the interview transcripts was the idea of what patients *should* know. This included preconceived ideas from the neonatal nurses, as well as a level of privileging information by nurses based on what they

perceived patients *should* already know and/or information nurses were *willing* to share. In some scenarios, there's a level of perceived risk with choosing whether to disclose/not all the potential impacts of using biometric technologies in the NICU. For example, Youngblood (2012) writes about the tension between "dispersing risk information for the public's own good" and also "restricting that information because of safety concerns, also for the public's own good" (p. 36). This topic of risk assessment also fits into the ways technical communicators might work to intervene in transparent communication, a key component of my methodology. For instance, communication materials regarding biometrics might be ambiguous because it is vague, allowing the receiver of information to make assumptions. Even so, communication could be more specific, as we read with some of the biometric data privacy policies, but still ambiguous because it lacks the context that the reader needs to interpret the information.

According to a study by MAGNA Media Trials and Ketch, 74% of people now rank data privacy as one of their top values. Across every age group, consumers consistently rank data privacy as their top concern — it is more highly valued than equality, sustainability, or any other ethical issue (Joseph, 2022). Joseph (2022) discusses what businesses can do to win customers' trust. The key is to look beyond compliance, and find ways to communicate transparently, give consumers meaningful and ongoing control over their data, and make data stewardship a core part of the brand. The following sections document how the top three biometric solutions neonatal nurses cite using in their day-to-day—voice, face, and fingerprinting—identify compliance as one area where awareness, transparency, and advocacy can be bridged in healthcare.

4.5a Voice Recognition: Something you are, to something you have[63]

Based on the questionnaire, voice recognition was the third most popular biometric technology that neonatal nurses cited using in their jobs, despite iris scanning being discussed more during the interviews. Voice biometrics systems can be used to verify a person's claimed identity or to identify a particular person. It is often used where voice is the only available biometric identifier, such as over the telephone. The following companies in this section were collected from BiometricUpdate[64]. In the following sections I describe the biometric solution, provide some background on the technology, and then follow with ethical considerations including the application of my framework.

The voiceprint of a person can shift (and does shift) over a single day. It is not foolproof to claim that voice may confirm identity. Two people can also sound very similar and since voiceprints are not produced through direct physical measurements, they are solely indirect representations of the complex physiological and environmental factors related to voice. One of the first records of voice identification occurred in 1988, where Nakasone and Melvin (1989) worked on a project funded by the US Secret Service called CAVIS, or the Computer Automated Voice Identification System. Though voice biometrics are newer in the biometric technology scene, they have been quick to get adopted, and even misused. For example, one of the most recent adaptations of voice biometrics is through deep fakes. While the term "deepfake" typically means images and video, it can (and has) focused more recently on synthetic voice content or computer-generated speech. Deepfake voice, also called voice cloning or synthetic voice, uses AI to generate a clone of a person's voice. According to Song (2019), computer vision, the academic umbrella that deep fakes fall under, is an "intricate field primarily concerned with

[63] A reminder that information about the companies used in this study are listed in 3.4ci.
[64] https://www.biometricupdate.com/service-directory/voice-biometrics

image and video processing-giving computers the ability to understand information from images and videos." As Song (2019) writes, applications for computer vision technologies are common: such as autonomous vehicles that use computer vision to analyze road paths and obstructions, and *medical systems* that use computer vision to diagnose patients.

One of the ethical dilemmas that technical communicators should be aware of is based on the corpus' analyzing and informing healthcare as a site of surveillance: how can you protect yourself against voice fraud, if you are unable to opt out of voiceprint in healthcare? The use of this software has increased due to its ease of use among health care providers (Urquhart et al., 2009; Fadahunsi et al., 2019). For example, patients have cited accounts from doctors' visits, where they were asked by a nurse if the doctor could use voice recognition to transcribe their notes (Joint Commission, 2022). Oftentimes patients have agreed; after all, it's what the doctor needs! Yet, according to the neonatal nurses interviewed, the actual concern about doctors voicing notes created feelings of anxiety and concern in patients. Imagine hearing your doctor dictate your prognosis aloud. Of course, discussing the affective dimension of patients' feelings with healthcare compliance protocols such as usage of voice recognition, is a whole different study. Even so, scholars in rhetoric of health and medicine have discussed patient feelings related to compliance (Skinner & Franz, 2018; Stimson, 1974). Hearing the prognosis aloud, alongside with other observations created a feeling of discomfort, alongside questions of if their [patient] own voices were being transcribed during the exchange. This concern, and action, contributes to reinscribing provider power over patients (Waitzkin, 1993; Zuckoff, 2012).

With only the verbal consent given by the patient, this should be recognized as a low level of informedness. Studies cite that less information is lost, and misinterpretations are reduced with voice recognition software implemented (Ammenwerth et al., 2011). However,

there are also studies that mention the severe, and sometimes even deathly implications, of voice recognition going wrong (Joint Commission, 2022). Also in a study, the voice software increased the quality of nursing reports because of direct and on-time recording of data as opposed to handwritten reports which may be recorded hours later (McCartney, 2013). This result was also reported in the interviews conducted with neonatal nurses. Nurses mentioned both a desire to implement voice recognition technology for efficiency's sake, a likely justification, while also concern about accuracy and extra work fixing recording errors. Also, despite the voice recognition software having relatively high accuracy, Peivandi et al., (2022) did find that it creates more errors than the paper method; this ultimately leads to nurses having to manually adjust any of the documentation errors. Not only are the nurses, people who are familiar with healthcare legalese and technical terminology, concerned about their own voice data being collected, but they also were never told how it was stored, distributed, and so on. And with the rising concern of deep fakes, it is no wonder the nurses were so concerned with the potential ramifications of someone repurposing their audio.

For many of the biometric solution companies, there was a section on their website specific to industries. From there, I chose "healthcare" since the study focuses on neonatal usage of biometrics within healthcare. Of course, this meant that the documents I looked at such as communication materials, privacy policies, and terms of service, also mentioned health-related concerns (especially in relation to HIPAA). Furthermore, when searching for solutions in the healthcare sector, topics such as security, compliance, and convenience were more than common. Security, however, is not the same as *privacy.* The biometric companies utilized language to suggest that without the technology, consumers (including patients and healthcare professionals in this instance) would not be safe. Yet the ways in which the companies discussed the

technology in terms of *privacy* were very different. Privacy was only mentioned in legal terms, that is, in documents such as the privacy policies which were located under separate tabs, and not as accessible to those browsing the website. Out of the five companies I chose who create and supply voice recognition software, only *one* (Verint) created a privacy policy that was transparent and "easy" to navigate. Transparency was determined by the ways the company specifically outlined topics such as consumer rights, data collection and management, and what is/isn't covered in the privacy policy. Despite the summarized points of the legal document, Verint also made sure to define how *they* viewed personal information and how the reasonings behind some of the more general points were due to differing privacy laws across the world. Verint wrote:

> Personal information may be any form of data that could be used to identify you, directly or indirectly. This Privacy Policy sets out important information on where and how we collect personal information, what we do with it, how we protect it, and what your rights are. This policy generally applies to our global operations. We know that some jurisdictions have unique privacy laws and where applicable, we will comply with those local laws.

Verint's privacy policy also contributes to how compliance is understood: in this case, compliance is in reference to complying with the *law*. To further elaborate on how the voice recognition companies were engaging in "compliance" rhetoric, Johnson Controls was the next company whose justification for implementation provides an apt opportunity for further research. For example, Johnson Controls writes how their products are "Powering impactful sustainability, respectful safety and security, while delivering an enhanced customer experience" (see Chapter 3.4cii list, "OpenBlue" webpage). We know that sustainability has been cited as second to data privacy in terms of what people value (Joseph, 2022). An increase in implementation of biometric solutions, such as voice recognition, for sustainability reasons (such as time saving, paper saving, and so forth) is becoming more and more popular in healthcare settings. Though

Johnson Controls doesn't specifically discuss voice recognition, the company *does* reference what the future of healthcare might look like, and this includes the types of technologies they're imagining. For example, Johnson Controls cites OpenBlue, which is a suite of connected solutions that includes AI-infused service solutions such as remote diagnostics, predictive maintenance, *compliance monitoring*, advanced risk assessments and more. Voice recognition *is* compliance monitoring: nurses interviewed in this study cited claims of not just concerns with the voice recognition systems complying with the healthcare practitioners, but also with patients complying with the technology. Many nurses, as I'll discuss in a moment, were concerned about patients being weary of complying with the voice recognition. Why does my healthcare practitioner need my voiceprint? What was interesting about Johnson Controls' imagined future in healthcare, was the way they discussed how their solutions (OpenBlue), "is how buildings come alive" (see Chapter 3.4cii list, Johnson Controls). The futuristic language is not just a fear-based, convenience-based, or compliance-based implementation of biometrics, such as voice recognition, but a claim or justification for implementing the technology that reads to consumers and corporations alike: if you do not implement this technology, then you are not *part* of the future. Healthcare institutions *want* to remain innovative: imagine a scenario with a clean office, built with the most up-to-date software and technology. Would this create a feeling of ease, safety, and maybe even comfortability for patients? Perhaps. Yet the emphasis on patient care still seems to be missing from the equation. This is part of the conversation of voice recognition being implemented in healthcare. Despite nurses mentioning that they utilized voice recognition in their day-to-day in their questionnaire, once interviewed, nurses retracted their statements. Many mentioned irises scanning, while others simply stated that they wanted voice recognition to be implemented for them (like the doctors they work with). However, after talking through

some of the concerns with voice recognition that they saw doctors grappling with, nurses began to shift their thinking. One of the concerns nurses mentioned that doctors had, for example, was with the presumed efficiency of the voice recognition technology. Though communicated by companies as "efficient" and "in compliance" with healthcare protocols, doctors were concerned with the added labor of revising their patient notes/files after the appointments. Efficiency and voice recognition will be discussed in more detail in 4.7a.

One adjacent concern to voice recognition (though not the same as collecting a voiceprint), is the collection of recordings whose audio *could* identify a person. According to a company called RevealMedia, their technology (body cameras in healthcare) is justified based on the alleged increase in "tense situations." This is yet another one of many examples where biometric companies implement technology as a response to a situation or event that has caused contention or fear. In this case, the Calla camera has a front-facing screen designed to calm down tense situations within the healthcare sector. What qualifies as a "tense" situation? How are patients notified that they are being recorded, scanned, and their faces and audio are being shared with a third party? RevealMedia states, "When required, footage can be played back and provide an independent third-party account of the entire situation" (see Chapter 3.4cii list, RevealMedia). When sifting through the website for textual corpus to explain the privacy policy, there was no mention of the specific third parties who would have access to this information. Would there be law enforcement implications? Potential denial of insurance? This is speculation; however, this is what happens when companies are not transparent with their processes and data practices. There needs to be more awareness and accountability for the usage and justification of implementing the technologies; and technical communicators can help through intervening in the communication materials put forth by companies. Within the context of the United States'

neoliberal healthcare system, in tension with coalitional efforts and ethics (discussed in 5.3), accountability begins with a *consciousness*. A critical consciousness, or accountability by the state and private sector may be determined or understood as a right: where, as Browne (2015) mentions, people have ownership of and access to one's own *body* data and other *intellectual* property that is generated from one's body data (p. 116). Accountability is contextual. For example, accountability could also look like biometric solution companies recognizing that their devices are not infallible. This accountability is based on an "Open Biometrics Idea" poised by Böhlen (2002). For example, companies, to be accountable, should not retain the user's or patient's biometric data for data mining (selling to third parties); in this way, "the user's digitized body data remains the property of the user, not that of state actors or a private organization or some other governmental body" (Browne, 2015, p. 117).

RevealMedia claims that their biometric technology will "play an essential part in mitigating violent and aggressive incidents in healthcare settings." Yet, this sounds like more policing than anything. The United States in the past few years has seen an increase in the usage of body cameras, and recording devices in general, to document police brutality across the nation[65]. In fact, the U.S. Bureau of Justice Statistics (2022) found that around 80% of large police departments had acquired body-worn cameras by 2016. Unfortunately, video doesn't *automatically* lead to accountability. Implementing body cameras in healthcare is yet another form of policing; except this policing is occurring not in a public space, but a space that claims to be private and secure. The Calla front-facing screen is "proven" to "deter aggression, de-escalate situations and provide an independent account of incidents, supporting the public and

[65] There are unfortunately a plethora of examples. One only needs to read/watch the news or browse social media/a search engine. For example, Tyre Nichols in 2023, Michael Brown in 2018, and Paul Castaway in 2015, and so many more. See an article by Ortiz, 2023.

safeguarding staff" (see Chapter 3.4cii list, RevealMedia). The company, however, does not explain how healthcare professionals use this device. Is the body camera mentioned to patients the moment they walk in the room? What happens to the audio, visuals, and more? Is the tradeoff of patient privacy more important than the few times healthcare professionals find themselves in aggressive situations? RevealMedia claims that "Studies show that when people see they are being recorded, it can calm them down and avoid conflict. That's exactly what Calla does by reducing disruption and recording an independent account of what happened" (see Chapter 3.4cii). When people are recorded, this *can* be disciplinary control in action; however, as studies and examples suggest, as exemplified by police interactions (Ortiz, 2023), the use of body cameras do not necessarily de-escalate a situation. Biometrics are deceptive design, and the level of informedness is unclear for patients. Yet since such technologies are situated as "protection," if patients do not "comply," then they are considered unruly. The biometrics are deceptive in this manner because of the tension between the intended design of the device and its implication in different sectors, such as that of healthcare. A body camera on a police officer makes sense; a body camera on a healthcare practitioner detecting audio and visual patterns does not. Though I am unaware of such studies documenting patient behavior in the presence of body cameras in healthcare, biometrics as surveillance tools in other settings are known to enact behavioral control (Clarke, 1988; Manolev, Sullivan, & Slee, 2019). I hypothesize that in an even more precarious place like healthcare, patients would filter their language (or voice), including what they disclose to their doctors, if they knew they were being recorded. How can patients trust their healthcare providers when they are now placed in even more precarious and vulnerable positions?

Even more problematic is the futile attempt for companies to communicate to consumers their safety. Yet, there isn't any mention of *why* or *who* the people need protection *from.* RevealMedia also creates a facial recognition software, which will be discussed more in the next section. If a match is found, the camera will respond in a predetermined way to create a safer, more effective, faster and streamlined workflow. RevealMedia, like many other AI-infused companies, claims to be creating technologies for the "future." They use the camera's "vision, audio, motion, and pre-configured information," to move society towards a "safer and better future for everyone." Technical communicators are well-poised to intervene in language creation and decision-making related to the design of technologies that do not account for, "everyone." Everyone does not benefit from the technology.

Based on the companies outlined, interlocking surveillance was used to analyze the corpus of text that the biometric companies published on their website. This methodological framework helps to understand healthcare as a site of surveillance that employs biometrics because of their perceived promise to be **secure**, **convenient**, and remain in **compliance**. The language coded from the corpus is intertwined with neonatal nurse interviews to help guide technical communicators' role in decision-making processes through the creation of awareness, advocacy work, and transparent language/practices. For example, technical communicators may advocate for more transparency through a summary of the privacy policy similar to Verint. Perhaps a rhetorical move might be to consider the downsides of implementing the technology, and creating awareness that despite popular consumer opinion, the biometrics are not a 100% indicator of authentication and identification. Facial recognition technologies are the second most used technology reported by neonatal nurses, and the next section documents how such

technologies are communicated by biometric solution companies and how nurses understand compliance and facial recognition.

4.5b Facial Recognition: Authenticating Your Face[66]

According to BiometricUpdate[67] a facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is typically used in security systems and can be compared to other biometrics such as fingerprint or iris recognition systems. In the following sections I describe the biometric solution, provide some background on the technology, and then follow with ethical considerations including the application of my framework.

Level of informedness and justification of technological use become very apparent when sifting through the materials from the biometric solutions. While the companies certainly do not acknowledge the discriminatory conversation swirling around such technologies, there is also justification of implementation as it relates to protection. For example, many of the technologies were created for law enforcement use and are now gaining traction in other sectors such as healthcare. Grother et al., (2019) write how there is a recent expansion in the availability, capability, and use of face recognition has been accompanied by assertions that demographic dependencies could lead to accuracy variations and potential bias (p. 2). A report from Garvie et al., (2018) work noted that prior studies on face recognition such as Klare et al., (2012), articulated sources of bias, described the potential impacts particularly in a policing context, and discussed policy and regulatory implications. Additionally, there has been a surge in studies focusing on the demographic effects of more recent face recognition (Cook et al., 2019;

[66] A reminder that information about the companies used in this study are listed in 3.4cii.
[67] https://www.biometricupdate.com/service-directory/facial-recognition

Krishnapriya et al., 2019) and gender estimation algorithms (Buolamwini, 2019; Raji & Buolamwini, 2019).

A massive concern that Grother et al. (2019) call attention to in The National Institute of Standards and Technology (NIST) (2019) report is the repository of faces that recognition software is matched to. I'm focusing specifically on this report because The National Institute of Standards and Technology is an agency of the United States Department of Commerce. Their mission is to "promote American innovation and industrial competitiveness[68]" which can assist in situating specifically *how* the United States government views biometrics such as facial recognition, as well as what research has been *suggested* (but as I'll note, the findings have not necessarily been acted upon). For example, four of the largest datasets of photographs collected in U.S. governmental applications that are currently in operation include domestic mugshots collected in the United States; application photographs from a global population of applicants for immigration benefits; visa photographs submitted in support of visa applicants; and border crossing photographs of travelers entering the United States (Grother et al., 2019, p. 2). As readers might gather from my literature review (Chapter 2) and analysis thus far, the United States has a preoccupation with implementing biometric technologies in order to determine the faces who are "non-compliant" in accordance with who the United States deems "compliant." For example, Gates (2011) has written about the "face of terror" that labeled Muslims "post-9/11." The spaces along and within the U.S. borders have become sites of experimentation for "automating the deceptively complex processes of facial identification and expression recognition," thus training systems to further marginalize specific groups of people (Gates, 2011, p. 3). Authorized travel, immigration or law enforcement processes are considered "good

[68] https://www.nist.gov/

compliance with image capture standards" while the last set does not, given constraints on capture duration and environment (Grother et al., 2019, p. 2).

A larger ethical concern in the NIST report is what Grother et al. (2019) found: false positives. False negatives are the failure to associate one person in two images; they occur when the similarity between two photos is low, reflecting either some change in the person's appearance or in the image properties. False positives are the erroneous association of samples of two persons; they occur when the digitized faces of two people are similar. False positives create a digital form of "stop and frisk." Further, the inability to "measure" is what Monahan (2010) calls "body discrimination" in technology design, where "unequal power relations are reproduced and reinforced by technological means" (p. 114). The National Institute of Standards and Technology (NIST) (2019) reports as follows:

> False positives: Using the higher quality Application photos, false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals. This effect is generally large, with a factor of 100 more false positives between countries. However, with a number of algorithms developed in China this effect is reversed, with low false positive rates on East Asian faces. With domestic law enforcement images, the highest false positives are in American Indians, with elevated rates in African American and Asian populations; the relative ordering depends on sex and varies with algorithm (Grother et al., 2019, p. 2).

The summarized results are important to include in full because they provide some important context for the usage and perceptions of biometric technologies. The United States *knowingly* implements technologies in various sectors that the NIST has reported are discriminatory. The information included about false positives is only one example out of an over 80-page report on the demographic effects of facial recognition devices. The NIST reports potential implications of the results; they write that since:

> different algorithms perform better or worse in processing images of individuals in various demographics, policy makers, face recognition system developers, and end users should be aware of these differences and use them to make decisions and to improve future performance (Grother et al., 2019, p. 3).

Notice the *individual* accountability on the end user. The end user. The person **not** responsible for the creation of the algorithm, but rather one of many individuals whose face trains the system, and whose harm the biometric technology likely deploys. Consider, for example, how Browne (2015) urges a questioning of our biometric past, to inform and think critically of our biometric present. As the NIST report suggests, amongst many other scholars such as Browne (2015) and Noble (2018), there is a direct correlation between how the tracking of "blackness as property" and those with demographics deemed "non-compliant" by the U.S. white heteropatriarchal society such as people of color, Indigenous populations, and certainly many others who do not "comply" with facial recognition "norms," inform the contemporary surveillance of the body. The NIST report, as well as the information collected from the neonatal nurses' interviews and corpus aligns with Browne's (2015) argument that prototypical whiteness, when "coupled with dark matter in the making of some bodies and not others" is problematic in "biometric technology and its attendant practices" (p. 92). It's also important to remember that there are different types of facial recognition. One of the more common usages, especially in healthcare, is one-to-one encryption. According to the NIST report:

> one-to-one verification is used in applications including logical access to a phone or physical access through a security checkpoint. It also supports non-repudiation e.g., to authorize the dispensing of a prescription drug. Two photos are involved: one in the database that is compared with one taken of the person seeking access to answer the question: "Is this the same person or not?" (Grother et al., 2019, p. 4).

Further, there are identification algorithms. First, the algorithms can be used to facilitate positive access like in one-to-one verification but without presentation of an identity claim. For example, a subject is given access to a building solely on the basis of presentation a photograph that matches any enrolled identity with a score above threshold. Second, they can be used for so-called negative identification where the system operator claims implicitly that searched individuals are not enrolled - for example, checking databases of gamblers previously banned

from a casino (Grother et al., 2019, p. 5). Further, the identification could occur through alienation of the body, despite claims of confirming identity. This idea is often referred to as "digital epidermalization[69]," or when "power is cast by the disembodied gaze of certain surveillance technologies (for example, identity card readers and e-passport verification machines)" (Browne, 2015). Interestingly enough, the NIST (2019) suggested that one solution (out of a long list) could be to mitigate false positive differentials through "threshold elevation, refined training, more diverse training data, discovery of features with greater discriminative power - particularly techniques capable of distinguishing between twins - and use of face and iris as a combined modality" (Grother et al., 2019, p. 10). This is a general overview of the NIST results; however, including *more* biometrics such as introducing iris scanning, doesn't seem to be the answer.

Nurses documented their process of implementing facial recognition to comply with training protocols. For example, Interviewee A stated that facial recognition is used to keep track of patients' information. The nurse mentioned that patients can say no (or opt out), but they had not experienced a patient doing so.

> [I tell them it is] for our own good. We still have to ask if they're okay with that [facial scan]. Supervisor trains us when the technology is first introduced. We have people experienced with technologies, organized training and functions of the technology, and it's in a day [the training].

Nurses explained that facial recognition was only used if the patient did not want to be fingerprinted, did not have a fingerprint, or some other outlier. In their roles, facial recognition was often used *for* them; that is, to log into or access systems, wings of the hospital, and for employee identification for tracking their hours. It seemed that through the conversations, though facial recognition was much more prevalent than voice recognition, fingerprinting was still the

[69] Epidermalization: the imposition of race on the body (Browne, 2015).

most common and used. This makes sense since this is also the most developed biometric solution (Sava, 2022). Despite patients having the ability to opt out, this ability is often not communicated to patients and if it is, nurses use boilerplate compliance language to suggest that the technologies won't cause harm. This includes language such as documenting how nurses were trained to use the technology, and that the biometric solution is for the patient's own good; after all, no one wants to be mixed up or "non-compliant," right? The trade-off of privacy and data mining of biometrics for compliance measures and security or efficiency's sake aligns with the ways in which the corpus collected from the biometric companies communicate their solutions. Fingerprinting technologies are the most used technology reported by neonatal nurses; the next section documents how such technologies are communicated by biometric solution companies and how nurses understand compliance and fingerprinting.

4.5c Fingerprinting: Success is at your Fingertips[70]

The neonatal nurses interviewed discussed fingerprints as some of the most common biometric technology used: both for employees and patients. Larson (2018) quotes Alex Simons, director of program management in Microsoft's identity division, mentioning that there is a rapid evolution from what used to be passwords, then smart cards, and now to biometrics. It's important to note that despite the assurance of security from these biometric companies, you can't (completely) change your face or fingerprints, and biometrics can be stolen. For example, in 2015, a breach at the federal Office of Personnel Management leaked 5.6 million people's fingerprints (Pagliery, 2015). In the following sections I describe the biometric solution, provide some background on the technology, and then follow with ethical considerations including the application of my framework.

[70] A reminder that information about the companies used in this study are listed in 3.4ciii.

According to BiometricUpdate[71] fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

Similar to the voice recognition and facial recognition companies collected for the corpus, fingerprinting solutions *also* provided testimonials and case studies as examples of justification for biometric usage. Companies also made a rhetorical move towards appealing with what their audiences *might* value by listing their own values. For example, GenKey wrote on their website that their motto is, "Identity for all, trusted by all" and how they are "experts in biometrics" (see Chapter 3.4ciii). This example suggests an appeal to what audiences, or consumers, might want in a company or solution: identification, trust, and expertise. Fingerprinting in particular was an interesting biometric to research because the emphasis on its usage in healthcare was more geared towards identifying the employee, rather than the patient. Despite this, neonatal nurses claimed that fingerprinting had replaced technology such as a wristlet or paper/pen for record-keeping.

For example, Interviewee G discussed how their job has changed over the past few years: "Job [has] only changed in terms of technology and record keeping. Used to be a lot of writing with paper, and now it's more computer. Easier and more efficient."

Though this response could be categorized as efficient, this response also showcases compliance. Interviewee G refers to how nurses comply with the changing times through digital technology rather than written. In fact, nurses often referred to fingerprints as a means of compliance through justifying their usage for identification and authentication purposes.

[71] https://www.biometricupdate.com/service-directory/fingerprint-recognition

For example, Interviewee F discussed how their role as a neonatal nurse contributes to compliance. The routine and responsibilities don't just comply with protocol, but also with biometrics:

> I get to work early in the morning, look at patient records and analyze, assign responsibilities, rounds to patients' rooms and check records. Previously records were written down, records are taken on a tablet/computer now…We use patient identification—fingerprints get the information on who they are, what is ailing you, medicine when you take.

Compliance also appears through patient "willingness" or consent. As Interviewee F expressed, fingerprinting only happens for willing patients. Yet how can patients consent or be willing, if there isn't choice or ability to opt out? Further, Interviewee B mentioned that in their healthcare setting, communication about biometrics with patients didn't extend past explaining that the technology made the nurses' jobs easier:

> We use voice recognition, we use fingerprints, and iris scanning. The sole purpose is for proper identification for employees and patients…It quite depends on the context of the situation. The biometrics help us navigate our activities easier. We don't tell patients the purpose behind why we need their biometrics. It's just being able to get things done more easily.

This method of communication is "in compliance" with what is expected of the nurses. Ironically, the very same nurse (Interviewee B), when asked about collecting their own biometrics in a healthcare setting, responded in a manner that suggested compliance, and efficiency maybe weren't reasons to use the biometrics:

> I won't lie, I wasn't comfortable because I wasn't really sure what my information or biometrics were going to be used for. I was in between positive and negative feelings at the same time. At the end, I should be grateful and hope for the best.

Despite the clear concern with data protection and security, which will be further discussed in the next section, the nurse chose to "hope for the best." This sentiment, surveillance

apathy[72], occurs with many people, not just nurses, who believe that they have no say or control when it comes to who has access to their personal information. Imagine a nurse, who knows the ins-and-outs of the healthcare system and *uses* the very biometrics that were used on them in their daily life, feeling as though there's nothing they can do. This is where nurses, as technical communicators, can intervene. If neonatal nurses view themselves as whole persons, rather than compartmentalize their professional role (as nurses) and personal role (as patients), they may be able to better advocate for themselves and as an extension, their own patients (through understanding their perspective). If neonatal nurses don't know what other healthcare offices are "doing" with their information, how can patients trust in what they communicate verbally to them about compliance protocols and security of the biometric? This is a classic example of nurses engaging in rhetoric that the biometric companies expect consumers to communicate, rather than training materials truly exploring all aspects of the technology to create more awareness and transparency.

The consensus remains the same for all of the neonatal nurses: biometrics make their jobs easier, convenient, and more efficient, which is the standard for remaining in compliance. Despite the concerns with training for biometrics, privacy, and communication, nurses still were in consensus that the pros of the technology "making their lives easier" outweighed any of their concerns both professional and personal. The following sections overview and document the way security/safety is discussed through the corpus of materials from biometric solution companies, and the interviews with neonatal nurses.

[72] Surveillance apathy: people believe that they have no say or control when it comes to who has access to their personal information.

4.6 Security

Included in this section is an overview of responses from neonatal nurses about security in healthcare as they relate to biometric technologies. The section then charts voice recognition and examples of security from the textual corpus collected; facial recognition and examples of security from the textual corpus collected; and then fingerprinting and examples of security from the textual corpus collected. As with the compliance section, neonatal nurses' responses can be categorized by the methodological framework and how communication materials justify standardization (how do healthcare institutions communicate a need), specific technological use (what types of technologies and why are they used), categorizing people (based on identity: confirming identity or fraudulent), levels of informedness of nurses (and patients), and urgency or efficiency of the technology as it relates to security.

Oftentimes biometric technologies, as the nurses discussed in their interviews, were not just used for identifying patients, but for securing patient information. If the only way nurses have access to patient information is through their own fingerprint/iris/voice/face, then in their perspective, the information must be safe and secure. There is a huge disconnect between the perception of safety and security, and the actual implementation of such. Where does the information go? How is it stored? What third-parties or other parties have access to this information? What can they do with the information? There are gaping holes in the links between what is perceived safety, versus true security. And this is the problem with deceptive design.

Deceptive design[73], also known as "dark patterns" are commonly referred to as tricks used in websites and apps that make you do things that you didn't mean to, like buying or

[73] Deceptive design: also known as "dark patterns" are commonly referred to as tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something (Brignull, 2023).

signing up for something (Brignull, 2023). I consider biometric technologies to be an example of deceptive design. Biometric collection is often situated for patient (and consumer) safety, protection, and greater security; however, who has access to this data, how does this impact healthcare topics such as insurance (including life) policies, what and who are considered the norm that the data is "measured" up against? There are increasingly more and more introductions to biometrics into the consumer arena; however, we must consider the implications of who the technology is identifying, protecting, harming, and how such are implemented (especially in a place as precarious as healthcare institutions). Biometrics can be considered deceptive design because of the ways they are marketed as safe. In reality, they are often racist, sexist, ableist technologies that perpetuate the very oppressive system they were created in. For example, though not specific to biometrics, patient experiences can and should be questioned in relation to the underlying stability and ideological aims of terms like "security" and "safety." Scholars such as Green (2021) reveal ulterior or "deceptive" practices of health and wellness that stem from the embodied realities of, for example, living with HIV. Dorpenyo (2019) mentions how technical communicators should consider the socio-cultural context surrounding when/where the biometric technologies are used. This would mean considering aspects such as "weather conditions, spatial relations, knowledge of users, social practices of users, the nature of work in which users are engaged, and how the work they do might affect successful use of the technology" (Dorpenyo, 2019, p. 373). Such socio-cultural conditions can affect the ways in which biometrics may deceive users, and authentication/identification processes.

In my interviews, neonatal nurses documented concerns with biometric technologies, especially with their newfound implementation on newborns (see the ION technology, Scenario 1 in the Interview transcript 3.4e and Appendix C). As Dorpenyo (2019) argues, if we are able to

let biometric producers know that "localization should happen at the user's site, where prevailing local conditions influence design..." (Agboka, 2013, p. 45), then, we could proudly say that we have taken a more active stance towards, as interlocking surveillance suggests, advocating for the disenfranchised and marginalized in our world. Technology design should be a collaborative effort between designers and users. And more importantly, it should consider the autonomy of the people who are using the technology, and those the technology is being used on.

In fact, neonatal nurses in the study mentioned that they used (or wished to use) iris scanning in their day-to-day responsibilities. Despite the screening surveys listing iris scanning (in both Reports) as not within the top five most used biometrics in healthcare, nearly every nurse mentioned iris scanning as a potentially useful technology that they'd like to see implemented in healthcare. According to BiometricUpdate, iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. Nurses cited the expectation that iris scanning would be similar and/or compliment biometric solutions commonly used such as facial recognition or fingerprinting. This response often came from participants during the scenario in interviews when nurses were told about Northwell Health's usage of biometrics (Appendix C).

For many of the nurses, they noticed a spike in biometric technology usage and integration into the hospitals during the height of the COVID-19 pandemic. Though the pandemic brought upon an onslaught of issues ranging from understaffing to lack of access to resources, the biometric technologies were implemented as a response to lessen the physical contact between nurse and patient.

Herein lies the "Privacy Paradox" that was mentioned in Chapter 2. Much of the ways people discuss privacy is through a detached view. There is an obvious tension, as we will see in the following sections, between the role of a professional and such obligations/responsibilities, and personal impact. For these healthcare professionals, personal information and privacy is important to them…for their job. For their patients' sake. But not necessarily for *them*. Not a single response focused on their own opinions of personal information or privacy. All focused on the role privacy played in their job. Perhaps this is because of the framing of the question. Yet it was fascinating to read how despite the question's framing of asking the nurse what personal information and privacy meant to them as a neonatal nurse, many of them discussed the impacts of privacy on their patients (and families). They also largely discussed legalities, such as HIPAA and securing information.

Another goal of interlocking surveillance is to analyze healthcare as a site of surveillance to create and/or suggest ways to create transparency about how surveillance manifests in the site. Other than the training that nurses received to *operate* the biometric technologies, there was consensus amongst those interviewed that there was no security, data privacy, or information training. I specifically asked (informally, as a follow-up to the identity theft), "Within your role itself, did supervisors ever chat or HR have a conversation about where that information goes or who has access to that information at all, including any sorts of third parties."

The nurse[74] answered simply, "Never. It's not disclosed." The nurse did mention that for the people who filed, HR knew which hospital was targeted, including what town the theft happened in, as well as specific nurses' social security numbers, names, and addresses. To address this breach, nurses were advised to "monitor our credit reports."

[74] Redacted (Interviewee E)

The following sections document how the top three biometric solutions neonatal nurses cite using in their day-to-day, voice, face, and fingerprinting, identify security as one area where awareness, transparency, and advocacy can be bridged in healthcare.

4.6a Voice Recognition and Security[75]

Interlocking surveillance helps to understand that voice recognition technologies don't center people as their audience; they center consumers. For example, the communication materials collected from the five websites spoke to the justification of standardization through attending to "Customer Satisfaction" or "Employee Engagement." Each company communicated their solutions as a means to "regulate" the body, "secure" the body, and "confirm" the body. That is, the solution created a sense of displacement from actual humans. The tool being used for monitoring, "data security and compliance" where aspects could be customized for the company or consumer's idealization, and most importantly: "cost reduction."

Though positioned as a tool that is secure and convenient, companies do not recognize the impact such biometrics could have on multiply marginalized populations. Who is this technology really for? Interlocking surveillance made visible the rhetorical moves that companies make to urge consumers to purchase a product that they really aren't sure they even need. When applying the methodological framework to the corpus of information, companies categorized consumers (remember, not people), through whether or not they were "acceptable" customers. That is, those who were "acceptable" are those who are not "fraudulent" or engaging in "identity theft." This brings us back to the urge for consumers or companies to purchase a product because of the push or urgency to "stop" identity fraud. Furthermore, language and communication materials through case studies, testimonials, and blog/news posts signaled to

[75] A reminder that information about the companies used in this study are listed in 3.4ci.

potential buyers the necessity and urgency to purchase the biometric solution for "customer experience" or "patient experience." Companies care about security, sure. What is interesting is that not one company shared *how* the biometric solution *provides* security. What does a biometric solution such as voice recognition *do* that is an urgent need for consumers? How is this positioned apart from other security tools and technologies? Take for example, Johnson Controls who claim they can "Contact us to take your hospital into the future." The future. The ways in which Johnson Controls refer to their biometric solutions appeals to an audience who are looking to be the next "innovator." Hospitals or facilities, like previously discussed in Chapter 2 with the history of biometric identification, implement biometric technologies with the perception that the newest technology is the "best" and "safest." Ideally, facilities want to be the safest for patients and employees, especially in healthcare. Patients value safety: however, when implementing new technologies, what buyers are *not* considering are the ways technologies are implemented as an urgent need to address the potential fraud or identity theft. Is this what patients, and employees, actually need? Where are they involved in the decision-making process? We don't need "smart" facilities; we need funding to focus on the healthcare inequity and inequality that is happening across the nation. There isn't any description on Johnson Control's website to account for *why* hospitals would need this specific product. Could it be "nice" to implement for efficiency's or security's sake? Maybe. But a necessity? Not so much.

Yet Johnson Controls employs the same tactics as determined by my framework's focus on justification of technological use and categorization of people similar to many of the other biometric companies. The companies focus on the output. The systems and solutions that are allegedly intended to keep patients' "secure"—this illusion of security—is what Johnson Controls argues leads to patient satisfaction, and subsequently healing. For example, Johnson

Controls claims that their "Integrated Systems Improve Satisfaction and Help Patients Heal." How? "A smart facility is an instrument of healing. When clinics and hospitals are secure, comfortable, and efficient, patient outcomes improve and satisfaction increases." Ah yes, with my new voice recognition software I will feel more comfortable being in a hospital bed. Oh, hang on, let's look another paragraph down: "With our security solutions, you'll know who is in your facilities, and when, and gain greater visibility and control of your medical and pharmaceutical inventory. Preventing even one incident more than covers the cost of a quality security system." Bingo. From a buyer's perspective, it seems the security solution isn't to help patients "heal" or provide "comfort," it's to make sure that the bodies who "belong" in the location are *who they say they are.* Though Johnson Control doesn't *specifically* claim that voice recognition technologies will lead to comfort and healing, they *do* claim that their smart facility, which encompasses emerging technologies such as biometrics, will. Biometric solutions are so preoccupied with fraudulent activity, that it's a wonder the companies don't (or maybe won't) consider how biometrics were adopted in the first place. Who are they trained on; who do they help; who do they harm; who creates them?

Interviewee A mentioned that in their experience with biometric solutions, "I was asked for a fingerprint in a hospital in Miami. I've also been asked for voice recognition, no idea what that was for in a hospital."

This response displays how oftentimes despite nurses using many of the biometric solutions, such as facial recognition, fingerprinting, and voice recognition in their day-to-day, the levels of awareness of *what* the technology is used for and *where* the data is distributed is outside of the training information communicated to them. The same nurse followed up by stating that when the biometrics were collected, the employees "Didn't have [the] option to opt out."

Nurses are told, as evidenced by the biometric companies' communication materials, that such solutions will be secure; as such, they believe that the solutions will also be secure for them when they visit healthcare institutions as patients themselves. Even so, more transparent efforts need to be implemented so that nurses can protect their own identity and subsequent information, as well as their patients. This includes having the ability to opt out, or even the option to inquire, learn more, and understand precisely what they [nurses and patients] are consenting to. Neonatal nurses' roles as technical communicators requires them to be patient advocates.

Advocacy in relation to identity was also a concern with nurses. For example, Interviewee E documented in their interview the following concern about fraudulent activity:

> During my conversation with other healthcare providers, there was a large amount of identity theft among nurses during the pandemic. Especially when we're receiving claims. So I was, uh, caught in that identity theft three times during the pandemic. Uh, the physician I know was twice. And unfortunately, it makes me apprehensive about allowing my picture. And allowing my information to be accessed by so many.

This is a typical response when technical communicators consider communication practices regarding security and privacy concerns. As previously discussed in other chapters, there is a privacy paradox involved. Further, people often do not "care" or know how to "care" about protecting their personal information. For example, as the neonatal nurse suggested in the above response, biometrics did not become a security concern until identity theft occurred to them. As the following section will document, fraudulent activity, especially when it comes to collecting biometric information, is a top concern that neonatal nurses have.

4.6b Facial Recognition and Security[76]

Facial recognition was discussed as both a popular technology utilized by neonatal nurses, as well as a technology that nurses hoped to implement more in healthcare. Security

[76] A reminder that information about the companies used in this study are listed in 3.4cii.

concerns were communicated through the corpus as to why the technology *is* secure or safe; however, many companies did not discuss *how* the technology maintained that security.

RevealMedia, for example, has a new feature called "Face Match" for their body cameras. The Face Match technology can "focus on people who are missing or vulnerable, the ability to stop crime before it happens and tackle the issues of proactively prosecuting re-offenders" (RevealMedia, "AI Enabled Body Cameras"). According to RevealMedia, the K-Series utilizes the latest chipsets, allowing the camera to perform various Artificial Intelligence tasks, including Face Match. "When this feature is enabled, the camera is programmed to match faces seen in the field against an uploaded pre-configured watchlist of people of interest" (RevealMedia, "AI Enabled Body Cameras"). RevealMedia claims that "body-worn technology should be accessible across multiple industries, not just the police sector." why? Their justification is solely based on "protection": "The ability to de-escalate situations before an altercation occurs using the front-facing screen as a deterrent." Furthermore, the company portrays the camera as an "impartial witness." This thus suggests a sort of humanistic application to non-human actors and agents, assuming the technology as neutral and unbiased. Security concerns were also discussed by nurses in terms of identifying children (Interviewee H):

> All these equipment [biometrics] could help ensure the safety of babies. It could also prevent mistakes in identifying mothers. You could have 10 to 15 to 20 mothers and deliveries at once in the hospital. Babies could be swapped and stuff. That happens. Facial recognition would go a long way in ensuring safety. It would be good. The problem is that equipment is not cost effective.

Though nurses thought an increase in facial recognition would ensure safety, they also cited financial concerns. The emphasis, however, is not just on patient and children safety, but also nurses. For example, Interviewee F mentioned that biometrics are required in their role to,

"access stuff in and around the workplace." The nurses mostly used facial recognition and fingerprinting.

Further, the same nurse (Interviewee F) mentioned that even though the biometrics were a requirement of the role (no communication regarding opting out), "The supervisor insists on privacy. All [biometrics] are stored on servers in the institution. If you ever decide to leave, they [the institution] destroy all evidence."

Though information about data collection was communicated to this nurse, it was communicated verbally, and such practices did not *fully* or *transparently* document what all stakeholders involved were consenting to. When I talked with nurses about how they felt to have their biometrics collected from them in a healthcare setting, they were all apprehensive or fearful at first. This was interesting considering their jump to implement technologies for their patients. The tension between personal feeling and professional obligation or the potential ease of the job was apparent. Interviewee F documented such concerns with their own biometrics being collected in healthcare:

> First, I was very nervous, it was not something I expected. I wasn't expecting my face and fingerprint id. I was very nervous - will everyone see this information? Will you give it to the IRS or someone else? I was fearful at first. I thought at first it was too much information, and I already gave them so much information like my documents at the front desk. They [nurses] changed my mind once they described things like ease of access, fast care, records at a second or different computers or scrolling through, etc. I decided I would give that information out.

As documented by my own personal definition of biometrics, or what I consider to be personal identifiers of the body, documents such as a driver's license needed for the healthcare institution are biometrics. What is a fascinating move is that nurses, once told that their personal information would help with "ease of access, fast care, and record keeping" (or identifying), felt that they would be comfortable giving up security (through ignoring their other privacy concerns).

4.6c Fingerprinting and Security[77]

As mentioned previously, the first scenario presented in the interviews with neonatal nurses was as follows:

> Researchers have developed a new technology that fingerprints newborns. This technology collects temperature, pulse, breathing and oxygen, and identifies the infant through their fingerprint. Let's imagine you have been told this technology would be implemented in a month…[78]

I include this scenario from the interviews in the security section because nurses cited the most concerns and claims with this scenario despite the overall mixture of responses from neonatal nurses. The answers, however, changed depending on if they answered as their professional role, a nurse, or their personal role as a parent (or imagining they were a parent).

For example, one follow-up question focused on how the biometric technology (newborn fingerprinting) would influence the day-to-day role. I asked, do/did you already use these technologies and what does this look like?

Interviewee E mentioned, "I would like to say it's along the lines of organ donations. You're taking a sensitive situation and you're asking them [parents] to give up their child's fingerprint. So, I think apprehension and fear will be the two immediate responses from a parent."

This response connected to my methodological framework, which charted biometric solution implementation of communicating during times of fear, or even urgency. I followed up with Interviewee E asking, "My next question was how you thought your patients might react and if you thought immediately there would be some apprehension and fear?"

[77] A reminder that information about the companies used in this study are listed in 3.4ciii.
[78] https://health.ucsd.edu/news/releases/Pages/2018-09-12-researchers-develop-biometric-tool-for-newborn-fingerprinting.aspx

Interviewee E stated that the apprehension and fear about implementing a biometric technology on newborns would come from the mother:

> Namely, because what is on TV shows and movies…with you being vulnerable and giving up your child's fingerprint that can be duplicated in some way. It can even go as far as cloning. So again, it has to fall on the educational level of the parent. But apprehension and fear since most of the public likes to relate what they see on TV or in the movies to real life.

This notion of television manifesting in the everyday may be best described by Nakamura (2008), who argues that in that film, "the act of seeing itself has become inseparable from the political economies of race, retailing, crime and surveillance" (p. 119-120). Nurses (Interviewee F) also mentioned security concerns that patients had:

> After you take patients' fingerprints, they assume you know everything about them. Criminal records, etc…like once you walk into the patient's room, every little idea of what the patient's life is like. It's all for identification, but we really don't know everything that's happening with this. Are you allergic to this? And they said you took my fingerprinting, you should know. But in all honesty, it has complicated things. You get to know everything that happens with the patient.

This sentiment was consistent throughout the ten neonatal nurses interviewed. Apprehension and fear would come from the *parent* or *patient,* but perhaps not from the nurse in their specific role. It marked a tension between personal responsibility and professional responsibility. Many of the nurses stated that they would not use the technology on their own children but would for their patients. Others also cited specific health impacts to newborns, for example:

> So, with us continuously grabbing their fingerprint and rubbing it against the surface, my thought would be, are we in any way shaping or changing the outline of the fingerprint by using it so many times?

Other follow-up questions asked: What potential pros and cons do you see with this technology? and a three-part question that asked: How would you, as a patient, respond to your

newborn being fingerprinted? How do you think your patients would react? What about your role as a nurse?

Interviewee A brought up a concern with biometrics that I cited in Chapter 2: How would biometric collection impact those who are "undocumented or [have] no insurance?" This is not just a security problem, but also an issue of compliance. The standards that force nurses to use biometrics, also force (since there is not usually a means to opt out) already precarious populations into further precarious and vulnerable situations. Even with this concern, the same nurse said that "the number of people who would say they aren't interested [in using the biometric technology] are so small." What was interesting was how even though nurses cited concerns, both personally and professionally for their patients, many were still under the same mindset: "We can still make them understand that there's nothing wrong, not hurtful."

This justification that the biometric "isn't hurtful" further proves that training and communication materials do not fully document *how* people could be hurt or discriminated against. Though the nurse (Interviewee A) mentioned that those who are undocumented or don't have insurance could be harmed by the biometric technology, the nurse still urged patients to use the technology and cited there was nothing wrong with it. This sentiment is problematic, not just because it is reinforcing systemic and systematic oppression, but because nurses as technical communicators won't intervene if they are under the assumption that there isn't anything they *can* do to resist the "norms" communicated to them. Nurses also tended to talk through their answers by justifying the potential usage of the biometric solution. As noticed in the responses, there was a tension between how nurses would personally react to a technology utilized for the infants if they had their own children, versus in their role as nurses: "I would love to know the reasons why it is being done and for what purposes. And maybe they use fingerprints and

biometric security for the baby." This response expresses how even though there's a sense of curiosity for how the technology could or would be implemented, security concerns were also on the mind of the nurses. Another nurse (Interviewee A) expressed similar:

> Some people would be curious… [this is] something that wouldn't affect the baby. Most times we use [fingerprint] the mother; enough information is given to them to convince them [to fingerprint their child].

In response to the patient's safety and fingerprinting mothers, the same nurse elaborated and stated: "I do tell them all the information, but sometimes you need to explain more if they feel unsafe or unsure and talk to them more and make them see why they should do otherwise." It's a particularly fraught rhetorical move to state that nurses communicate with patients and urge them to partake in the usage of a biometric technology that can very possibly cause harm both visible and invisible. Where does the information go? Who is it shared with? What is the impact on the patient(s), and the ubiquity of surveillance assemblages? Nurses should be trained on all aspects of the technologies that they claim are safe and secure.

As the most utilized biometric technology in healthcare, some fingerprinting companies were sure to disclose not just *why* the biometric solution was the "best" and most accurate, but also *how*. For example, uATTEND[79] was one of the few biometric solutions that discussed and disclosed their biometric data retention policy, separate from the privacy policy. Included in the policy are company-specific definitions, disclosure and authorization, retention schedule, and data storage. Despite uATTEND claiming that their technologies, Workwell, does not advertise their products for use in the medical industry or for medical purposes, healthcare is one industry that may utilize their technologies. Fascinatingly enough, uATTEND (Workwell Technologies) writes:

[79] https://uattend.com/biometric-data-retention-policy/

> While our products may archive readings for reporting and audit purposes, it is solely the responsibility of the organization to communicate the use of the information to its employees, to obtain any necessary consent from its employees and to determine how the information is used. The organization should not rely solely on our products for making such a determination. Various environmental and methodological factors can impact thermal imaging; therefore, the readings from our products should not be relied upon as the sole determinant of a person's body temperature. Competent medical advice and further checks should be sought if there are concerns regarding an employee's health or possible illness. Workwell hereby disclaims all liability with respect to the conditions and limitations described in this paragraph.

Workwell Technologies is a representative example of the ways companies may discuss disclosure, retention, and data, as well as how biometric solutions communicate their products. The language surrounding responsibility on the company purchasing the technology for disclosure is an area worth further exploring. Consent is of course a major concern, as previously discussed, in relation to usage of the technologies. If biometric solutions provide the necessary information for companies/consumers, then it is both the responsibility of the creator of the product and the implementer to properly disclose how the information is used, stored, and distributed. Further, Interviewee A cited claims when fingerprinting went wrong:

> Sometimes we use thumbprints of mothers to identify infant information…We have had issues where the information wasn't supposed to recover information, person mixed it up [the nurse mixed up patient identification information]. Not conscious of what they were doing and typed something under someone else's profile.

In this response, safety becomes a concern when the scanned thumbprint, in this instance, does not correctly identify the *right* patient. That is, the nurse scanned the thumbprint only to document notes under the *wrong* patient. Biometrics are not foolproof, and these mistakes can happen; however, when we consider compliance, security, and efficiency as they relate to biometric technologies, perhaps greater weight needs to be put on the implications of how biometrics may harm and discriminate against patients (and nurses!).

The following section focuses on efficiency and convenience as it manifests from the biometric solution companies, and bridges to how neonatal nurses experience and perceive biometric technologies to be efficient in their day-to-day.

4.7 Efficiency and Convenience

Included in this section is an overview of responses from neonatal nurses interviewed about efficiency and convenience in healthcare as they relate to biometric technologies. The section then charts voice recognition and examples of efficiency/convenience from the textual corpus collected; facial recognition and examples of efficiency/convenience from the textual corpus collected; and then fingerprinting and examples of efficiency/convenience from the textual corpus collected. More than the collected corpus, the neonatal nurses' responses can be categorized by the methodological framework and how communication materials justify standardization (how do healthcare institutions communicate a need), specific technological use (what types of technologies and why are they used), categorizing people (based on identity: confirming identity or fraudulent), levels of informedness of nurses (and patients), and urgency or efficiency of the technology.

For example, one of the main goals of my methodological framework is the creation of awareness through communication materials, as well as noticing *where* and *how* technical communicators could intervene in increased awareness. Interviewee I mentioned convenience as a means for *justification of technology use*. Easy identification became a code for efficiency. For example, Interviewee I mentioned that despite parents' potential concerns with biometrics, convenience and efficiency trumped security's sake. The nurse stated: "Children are kept in the nursery, and no parents are around so we can use the technologies on them. Sometimes without the parents noticing." In this example, the nurses would use biometric technologies for

identifying the infant despite parents asking nurses to opt out of such *digital* identification. In nurses' justification, the efficiency of the technology in their job was more important than the parents' comfort and perceived security of the infant.

Further, another goal of the methodological framework is advocacy, which was discussed through the ways nurses would advocate *for* using biometric technologies; however, not necessarily *for* patients. The same nurse (Interviewee I) mentioned the potential downside of *not* using biometric technologies, which would be labeled as a lack of convenience:

> Normal identification mode for the parents who are skeptical [about biometrics], is to manually write down the characteristics [of the infant] for the parents who refuse to use the technology.

Advocacy efforts overlapped greatly with the goal of transparency. For example, the above response outlined how nurses would urge parents to consider usage of the technology, and document why they were using the biometric. This could be labeled as transparent practices, though oftentimes even nurses' levels of informedness did not accurately convey full transparency (which would look like disclosure of *all* data practices and dissemination. The nurse did note that interestingly enough, there are very few cases that parents won't "consent" to the use of the biometric technology at all. In fact, nearly all of the ten nurses in their interviews mentioned that skeptical or concerned parents consent to biometric usage after the nurses explain to the parents that the technology "helps the newborns." The concern with this communication, as gathered from the interview data, is that this exchange between nurse and patient is always verbal. Further, this example is very similar to the ways in which the collected corpus communicates information about biometric technologies to potential consumers and users.

The following sections document the way efficiency and convenience manifests in the interview and textual corpus based on the top three biometric solutions that neonatal nurses utilize in healthcare: voice recognition, facial recognition, and fingerprinting.

4.7a Voice Recognition: Efficiency and Convenience[80]

Ironically, despite nurses mentioning that their workplace used technologies such as facial recognition and fingerprinting, when the topic of voice recognition was discussed, most nurses changed their response and stated that they more so used iris scanning. In the interviews, their justification for the shift was due to the desire for voice recognition to be implemented for nurses, as it was common practice in many of the workplaces for the technology to only be available to doctors.

The themes of compliance and security greatly overlap with efficiency and convenience concerns. For example, rf IDEAS mostly creates fingerprinting biometric technologies; however, they note that multi-factor authentication "provides the highest level of security for access to healthcare medical carts, financial records, government networks and other essential data." Part of the multi-factor authentication is the move for healthcare facilities to focus on implementing multiple forms of biometric authentication, in the case that one may fail or provide false positives or negatives. rf IDEAS claims that:

> A fingerprint is the simplest, most convenient way to identify authorized users uniquely. It provides the "something you are" in multi-factor authentication protocols. For the "something you have," as well as for applications that require only single-factor authentication, WAVE ID Bio readers support a variety of user credentials including proximity cards, smart cards and mobile tokens all in one simple, unobtrusive form factor (More about this will be discussed in 4.2c).

[80] A reminder that information about the companies used in this study are listed in 3.4ci.

I discuss rf IDEAS in this section about voice recognition technologies because of the "something you are" and "something you have" notion that rf IDEAS differentiates. In healthcare, voice recognition software could easily be a single-factor authentication; yet as we've determined thus far, the system is prone to more ethical and accuracy concerns than not. Biometric technologies are justified for being implemented in healthcare for their convenience and alleged safety, yet consumers are *not* informed about consent or opting out procedures, nor are they informed of the security measures that *are* in place. Voice therefore becomes part of "something you are," rather than "something you have."

This concern with efficiency was voiced by one of the neonatal nurses interviewed in the study. The same nurse mentioned that a doctor at [redacted hospital] was intending to roll out voice recognition. The nurse[81] noted that the physicians were overall "apprehensive" especially with the approach to dictation.

> She told me the way it works is she will call out each system. And then she will state her findings; everything for the head, everything for the eyes, everything for the nose. So, there's a lot of that kind of…she calls it robotic talk. But it's very similar to us charting. We just don't verbalize it to the patient. So that's going to be a change, with the voice. Much more anxiety.

Anxiety related to voice recognition is apparent within and outside of the healthcare setting. For example, one such application of deepfakes is to replicate or clone a person's voice. One of the more recent controversies surrounding the technology involved the replication of famed chef, travel documentarian, and author Anthony Boudin, whose voice was cloned and used in a documentary about his life. While people can use the technology to revive voices that are no longer with us, it does raise ethical questions (Baker, 2023). While there are a multitude of ethical concerns with voice usage in healthcare, many of the companies that I will refer to below,

[81] Redacted (Interviewee E)

do not mention such ethical concerns. In fact, the biometric technology is cited as the best use for healthcare practitioners for convenience and speed. Yet use of voice recognition for efficiency's sake brings up questions of what it means to be efficient. Technical communicators have long argued that efficiency is about consideration of impact, especially on people, rather than speed and time (Scott, Longo, & Wills, 2007; Katz, 1992; Frost, 2016). In this instance, voice recognition does more harm than good: harm for patients' emotional well-being, data privacy, and more, alongside healthcare personnel needing to review their speech-to-text after hours to ensure accuracy in translation and dictation.

Interviewee F elaborated on the concern or apprehension for voice recognition to be implemented in the day-to-day. For example, they stated that, "It [voice] is very unique. We don't really need it though. We just need to recognize and identify the patient. With your face and your fingerprint, the only addition would be voice. The problem with voice, newborn babies you cannot use that. Patients who are too weak or ill to talk, it would be too hard for them." Herein lies a glaring concern: access, disability, and ultimately, discrimination with biometric technologies. These technologies are not created for every nurse or patient to use. This has been previously discussed (Chapter 2); however, the study showcases how the biometric solutions are still used in healthcare despite their *known* harmful impacts.

Technical communicators and rhetoricians specifically intervene in and design for users' experiences. For example, what specifically needs to be addressed is the white-supremacist conception of "health," which, according to Piepzna-Samarasinha (2018) often frames health in terms of "individual patient outcomes, ignores systemic oppression's axiomatic role in creating toxic environments, and perpetuates the neoliberal lie that disability and illness are a result of personal failure"—as if one didn't try hard enough to achieve "health" (pp. 29–32). Awareness

of the ways biometric technologies are used within healthcare to promote "health" is important to understanding user experiences; as such, transparent communication for users is also crucial. As Bivens et al. (2018) argue, aural communication is a layer of health literacy, and users are more than just those who explicitly use these healthcare technologies. Though Bivens et al. (2018) specifically focuses on sounds in her study, some of the findings overlap with how technical communicators may intervene and respond to the information presented from the biometric solution corpus. For example, in this study, the physiological and other monitors that persistently surveil the infants' bodies send aurally delivered messages to expert and non-expert users alike. As Bivens et al., (2018), argues, "Whatever that message, for whomever the user, there is an embodied, aural layer to health literacy that needs to be attended to in healthcare communication" ("Aural" n.p.). If patients and healthcare professionals are expected to use voice recognition devices, this does contribute to a toxic environment: creating anxiety in patients, and perpetuating "failure" for those who are "unrecognizable," cannot speak, and so forth.

In my interview with Interviewee I, I stated: You mentioned that some of the technologies your workplace employs include fingerprinting, facial recognition, voice recognition, and a palm/vein scanner. How do you use each of these technologies in your role?

The nurse responded that facial recognition and voice recognition are only used once in a while. I labeled this response in terms of convenience and efficiency since the nurse described that facial recognition and voice recognition are only used in situations where a patient's "fingerprints aren't there because of accidents or disabilities or something." The nurse elaborated to say:

> The voice recognition we use only when the patient doesn't have the fingerprints or doesn't have their hands. We use fingerprints for more than half of the patients. We have been using face recognition alongside fingerprints to identify. This technology is very

> important. One technology could fail; if a face scanner fails then we need to look at the fingerprint and vice versa. Very important in terms of medical care.

The following section focuses on another biometric technology, facial recognition, that neonatal nurses cited as the second most used technology in their roles.

4.7b Facial Recognition: Efficiency and Convenience[82]

Many of the nurses in their interviews cited in their hope for more biometric implementation for efficiency's sake. They stated that the technologies would make their jobs "easier." This is not a new, nor surprising discovery. For example, an article written by Senior Product Designer at Ethen Taras Savytskyi (2022) documented the reasoning behind the design of the origin story of Sony Walkman, Mini Cooper, and the iPhone. How does this relate to biometric technologies? Simple. The research and vision are the same: create technologies for ease of use and access. Savytskyi (2022) writes about the Mini, "Every decision they made during the build phase was aimed at saving space and improving efficiency" (n.p.). Sound familiar? Neonatal nurses in this study mentioned that as long as the biometric technology was "easy to use," "didn't take up much space," and "saved time," then the product would be effective for their patients and their own job responsibilities. Like the Mini, neonatal nurses responded hesitantly to the implementation of biometric technologies within the workplace. But from the 10 interview participants in the study, each cited the general claim that once they were taught why the technology was being implemented, concerns eased.

Nurses interviewed in the study alluded to how they were often trained on the biometric solutions once they were introduced to the workplace, if any were introduced. For example, I

[82] A reminder that information about the companies used in this study are listed in 3.4cii.

asked participants: How do biometric technologies and issues of privacy complicate the relationship between you and your supervisor and you and the patients?

Interviewee I stated that they had been trained, and that the "hospital organizes workshops for training of the technologies. There are new technologies that are brought up." The same nurse (Interviewee I), like many others, described how initially paper identification was used rather than digital technologies, so the training is implemented to "adapt to using new technologies for more efficiency."

Interviewee H mentioned something similar in training protocols, which may be categorized as compliance. I classify the training(s) in the efficiency section because nurses mentioned that they were trained on technologies *for* efficiency's sake despite the technologies often requiring a learning curve that made their efficiency…not so convenient. For example, the nurse said that:

> A lot of times my hospital normally wants us to organize risk training, get us updated on recent technologies and apply them…If the hospital can't afford it yet, we can still be taught about the technologies in the near future. In-service training. Early last year was the last one. It was a blood pressure monitor machine.

For others, training was simply by word-of-mouth or by shadowing. Interviewee F mentioned that in their private practice: "From the time I've been working here, no training. Just word of mouth. No clear line of formal training. Very informal."

One of the more fascinating moves that biometric companies are shifting towards is the complete implementation of AI-infused service solutions. Take, for example, one of the scenarios that I present to interviewees of Northwell Health (Appendix C). This scenario was the second one used during the hour interviews with neonatal nurses. I include the responses in the efficiency and convenience section because each nurse responded to the ways Northwell seemed exemplary for healthcare models.

The following scenario focuses on neonatal nurses' responses to imagining working (present or future) in a healthcare setting that has more access and usage of biometric technologies:

> Northwell Health, based in New Hyde Park, New York, United States, is a healthcare network made up of 23 hospitals and over 700 physician offices and urgent-care centers. Northwell began rolling out a biometric system using iris scanning and facial recognition technology from RightPatient Inc. Northwell is one of the first major medical systems in the United States to outwardly discuss and deploy biometric technologies—and, as such, have been widely lauded by online medical, technology, and business publications as a "pioneer" in medical innovation.

The first question changed depending on the nurse. I stated: you mentioned that some of the technologies your workplace employs include [insert here based on screening survey: fingerprinting, facial recognition, skeletal tracking, voice/iris recognition, palm/vein scanner, and a pulsometer]. How do you use each of these technologies in your role?

I followed up by asking: If you don't directly use the technology, what would it look like if implemented in: your own unit, day-to-day, or personally? I also asked the nurses what some of their concerns with implementing this technology, if any, would be and why?

One nurses response highlights quite a few of the ways they view biometrics as efficiency as it relates to communicating with patients, as well as their personal relationship with the technology in healthcare:

> That would depend on the concern. It's small I would say it makes me feel more at ease because I have resilience and know more about the technology the more, I use it. The focus is not on how nurses make it seem the technologies are communicating. It's more communicating the technology with the body. I always detail concerns and I engage in a lot of options. Those things help strengthen the community in Atlanta. Options in technology and accessing the users. If patients are sensitive to their privacy and the baby's privacy, I give options for other technologies. But I tell them about something more beneficial…Yeah that was a fascinating thing to me to measure the wire connected to the baby's food or hand. Really want more work with this aspect, and my huge concern in this aspect. My wife wasn't given a lot of knowledge about what was being done with the baby. Things need to be explained more to patients and how easier it can make working with them seem and give accurate results. Temperature probe is placed on the

> baby's skin to help regulate the heat and keep the baby warm. Communicate even more stress free.

This is a *lengthy* response from one of the nurses, and it covers a *lot* of topics and ground. However, I include it because I think it encompasses what the other nurses in the study said in responses to this scenario. I also think that this answer informs my conclusion for technical communicators (more in Chapter 5). Not only does this suggest that nurses are aware of the importance of nurse-patient relationships, but they also distance the technology from the person. The technology is simply a tool, rather than an object that can and does create harm for many on the receiving end. Some nurses are considering topics such as privacy and security; however, they also didn't talk past the boilerplate language told to them in training. This is the very same language that is located on the biometric technology's websites. Furthermore, every single nurse shared a personal experience during the breakdown of the scenarios to explain when they felt there was a lack of understanding in their role as patients. The discrepancy however lied within their personal contributions in their roles. Nurses, despite their own experiences, did not change the way they communicated with patients even though they wished information had been broken down and explained to them.

Similarly, in Savytskyi's (2022) article, they cite the birth of the iPhone: "Basically, the team defined problems they saw in existing technology and came up with ideas on how to fix them in order to enjoy the magic of technology" (n.p.). Neonatal nurses are operating and have been operating utilizing the age-old pen and paper for patient records. As they have become digitized, developers and researchers have begun to consider ways new technologies could be introduced within healthcare. The problem is that many of these technologies that are poised as necessities for efficiency and safety, are not attending to other problems of security and health. Some of the neonatal nurses cited concerns, for example, of fingerprinting infants. Just because

we *can* create the technology, does not mean its impact will be solely positive. In fact, many of the nurses are urging researchers and developers to fully test all of the potential wrongs with the technologies before introducing them to the health sector. One nurse mentioned that their goal was to make sure patients are able to leave the hospital happy and healthy, not return later (in whatever timeline) with ailments because of the technologies (like cancers, and so forth).

The responses are included in the facial recognition section because over 23% of nurses interviewed cited either wanting to implement or already implementing facial recognition technology in healthcare. Since a majority used fingerprinting both for their own employee identification as well as the patient(s), nurses were interested in imagining a future with other biometric solutions incorporated into their roles.

4.7c Fingerprinting: Efficiency and Convenience[83]

In interviews in particular, and when defining biometrics, the neonatal nurses viewed the technology as efficient and for convenience. What was especially curious to note was the idea of lateral surveillance, known as peer-to-peer surveillance. An example of this would be the idea of a colleague observing your actions during your workday. Much of our lateral surveillance is labeled as everyday surveillance. We observe our friends and their responses, but not usually for nefarious means. Surveillance also is not always for nefarious efforts. In the case of using biometric technologies and considering what privacy means to patients, neonatal nurses seem to value the autonomy and trust of patients and they laterally surveil their colleagues in order to protect patient confidentiality while also maintaining the ease of use of the technologies.

[83] A reminder that information about the companies used in this study are listed in 3.4ciii.

Overall, nurses believed that the biometrics make "work easier for you [patient] and I." Interviewee F described how the technology is used for easy recognition, and though convenient for the nurses, they are often met with apprehension from patients.

> When you first ask a patient for their fingerprint, the first time they say "no." Why do you want them? Then we have a conversation. I say we don't have to interact or talk to you [once they take the fingerprint]. Majority of patients then let us take them [after the conversation].

As mentioned in the interview script (Appendix C) one of the scenarios I used in the interviews documented a potential (and in some healthcare institutions, current) biometric future with fingerprinting technology for newborns (ION):

> Researchers have developed a new technology that fingerprints newborns. This technology collects temperature, pulse, breathing and oxygen, and identifies the infant through their fingerprint. Let's imagine you have been told this technology would be implemented in a month…

From this scenario, I asked the following questions:

- How would this biometric technology influence your day-to-day role? Do/did you already use these technologies and what does this look like?
- What potential pros and cons do you see with this technology?
- How would you, as a patient, respond to your newborn being fingerprinted?
    - How do you think your patients would react?
    - What about your role as a nurse?

Nurses who were interviewed, and in their screening response, mention a responsibility to protect patient privacy, but only through their verbal interactions with other people. This concept is not applied to the technologies mediating interactions, such as the ION technology. Why? From the responses, especially in interviews, the biometric technologies are poised and viewed as tools to make the job "easier" for nurses. The efficiency, and presumed safety, allows for the nurses to move with ease from patient to patient. The question remains, at what cost? In this fingerprinting scenario, nurses responded with a majority of logistical concerns and efficiency as determined by making jobs "easier." For example, when considering implementing the fingerprinting for infants (ION), Interviewee I stated that this would be a disadvantage.

> Their [infants] biometrics used at one point may be hard to identify. If there was a technology to identify the young ones it would be helpful and so important. Maybe like heartbeat or vein scanners to help. It is hard for us to identify the young ones. It has been challenging to identify the kids because they are so young and developing. Challenging with fingerprints, skin might not be developed or cannot see the children and the device scanners, [the infants] are afraid of them. The child may cry and cry because we can identify the child because they are afraid of the device.

The same nurse, however, suggested:

> Technology that would be friendly to parents and children, and not use light rays because some parents are skeptical of these devices. Technology that would make parents not so skeptical and of course like a device that doesn't emit light. Many parents are scared of the light and light rays. That would make it more acceptable by the parents. Important to me and my work.

Though the ION technology in this scenario is communicated as efficient and convenient, and neonatal nurses can see the potential with the ease of using the technology, there has been concern with newborn fingerprints not developing. As Interviewee I noted:

> The main technology used to identify the patients are fingerprints, for newborns the fingerprints might not be well developed. Their skin is different, and we might have difficulty fingerprinting them…Fingerprints will be used when infants are older than six months old, it's challenging to identify and might not be able to opt in or the technology might not clearly identify. We have some scanners that can be used for infants that are more grown, scan their eyes to identify them.

Some nurses also documented concerns such as difficulty "identifying the young ones because they have similar characteristics" and that if the purpose of biometrics was for safety, efficiency, and identification (compliance), then some nurses mentioned the trainings on biometrics focusing on a "challenge at birth or stealing someone's child [if someone's child was swapped or stolen]." Although the ION technology is newly implemented and/or not even on the radar for most neonatal nurses, Interviewee I mentioned that they had a three-week workshop on ION technology, used to identify newborns.

Since very few nurses heard of the ION technology, never mind had used the technology before, it was helpful to talk through *how* the device was perceived from a firsthand perspective rather than an imagined scenario. Interviewee I stated that the ION technology is:

> Just a device that you hold near the finger. So, as I had said earlier there are difficulties, you have to put your hand and then the device, identify you. For the infants, it is difficult for them to put their hand on the device. Some babies are not used to it. We had some problems and people weren't all accepting this technology. They [nurses] aren't used to it and some feel it is hard to use. With time, they will get used to it. Some parents had concerns that the technology would affect their kids. Well accepted for a year now and very efficient so far.

Interviewee F documented the stark tension between personal feelings and professional obligations. While the nurse thought the ION technology would be convenient and helpful in their role, when it came time for considering their own children (in the scenario), nurses did not want the technology used. For example, the nurse initially stated:

> I think that [the ION technology] would be very helpful. It would be a brilliant idea with newborns. Say you had to go through 15 babies in a day, you'd have to go scroll through information. If we could fingerprint the child and we could get all the information in a second; the name, weight, etc., and everything we [nurses] need/want. It would make things easiest and could serve a higher number of babies.

While Interviewee F was initially enthused about the possibilities of implementing the ION technology, they mentioned that "The only negative I could see is you don't want kids' information going into the world. Raises a lot of eyebrows from the hospital. You don't want your kids fingerprints on devices. Don't want to expose the kid that early. So that might be a challenge I could think of."

I include the responses from the nurse together in this section to display the stark contrast in answers. There is a clear line between compartmentalizing roles: nurse, patient, parent. These responses aren't just exemplary of the technology thought to be efficient, but also security and compliance concerns. I label the technology as "thought to be efficient" because of the list of

concerns that nurses had with the technology. The same nurse (Interviewee F) stated that as a parent, they would not want their newborns being fingerprinted.

> I would not want newborn fingerprints taken at one day old. I prefer with newborn babies we stick to the old traditional way and record something. The amount of x-rays etc they expose you to is so high. The kid who has bones and cell tissues who have not developed properly. It is too early.

The efficiency of the ION technology as documented by nurses using the newborn fingerprinting and/or imagining their healthcare facility implementing the technology in the future based on the scenario provided insights into how biometric companies communicate their product as "efficient," despite a lack of consideration outside of the actual tool. Who does this impact? How? Why is the technology needed? Is it needed? Why?

Most neonatal nurses in the study discussed how facial recognition technologies were used on them in healthcare settings, but not necessarily that they used them in their day-to-day as much, despite the screening surveys suggesting about a quarter of the nurses used and/or implemented the facial recognition technology. Despite this, fingerprinting was also the most popular technology used; both in their roles and in their personal experiences in healthcare. Interviewee I expressed that they have had biometrics used on them several times:

> At first my feelings were like what, why do you want to recognize my face? Why do they need this? Then after they explained to me that they were recognizing my face and taking my fingerprints it would be easier for me to access medical care and they could identify me and my records quickly. I was a little bit skeptical at first, but then I came to understand the meaning of them taking and checking my fingerprints and face. If next time I was sick, they might not be able to identify me except through my blood. Biometrics taken can identify me and all my health conditions and features. Superb for me as a patient, very helpful as a patient.

As this response suggests, the biometrics poised as convenient and "helpful" or efficient create a sense of illusion that because the technology is assisting the healthcare facility, if patients do not comply then they are "non-compliant" and therefore not being "convenient." The

interview with the nurse showcased the hesitancy with the technology, but they also mentioned that communication only occurred verbally. Further, the onus was placed on the individual: **if** you want to be identified and access your records *quickly*, **then** you need to comply with our biometric collection process. Despite the promised convenience and ease, there is a tradeoff with privacy and data concerns. What data is collected? Where is it stored? What third parties have access to the data (biometrics)?

Overall, from the corpus of text collected from the voice, facial, and fingerprinting solutions, there were common themes such as adherence to compliance, efficiency and convenience, and safety and security claims. These three categories are how the screening surveys are sorted and categorized. How do neonatal nurses perceive and use biometric technologies in relation to how compliance, efficiency, and security are understood?

4.8 Chapter Summary

The analysis done in this chapter identifies themes and trends (security, efficiency, compliance) that link the initial communication of biometrics to consumers and institutions, to those who use the technology in healthcare (neonatal nurses), and individual accounts (those interviewed). The information in this chapter works to answer: How do neonatal nurses define biometric technologies? What are neonatal nurses' perceptions and usage of biometric technologies? Chapter 4 is a compilation of the data from the methods, where interlocking surveillance was applied as a framework to understand the collected information from the textual corpus analysis, screening surveys, and interviews. The following Chapters identify some of the themes documented to predict future areas of study, and to highlight their application in the classroom setting, especially for programmatic implementation in technical communication courses.

This chapter focuses on how themes of compliance, efficiency, and security are communicated to consumers, ultimately creating a tension that users navigate due to lack of transparency and awareness. Neonatal nurses can (and do) have a role in the design of communication materials, particularly with patient choice in opting in/out. The next Chapter (5) discusses implications of security, efficiency, compliance in healthcare and how technical communicators may intervene. These themes will then be applied to programs and the classrooms (Chapter 6).

REFERENCES

Agboka, G.Y. (2013). Participatory localization: A social justice approach to navigating unenfranchised/disenfranchised cultural sites. *Technical Communication Quarterly, 22*(1), 28-49.

Ammenwerth, E., Rauchegger, F., Ehlers, F., Hirsch, B., & Schaubmayr, C. (2011). Effect of a nursing information system on the quality of information processing in nursing: an evaluation study using the HIS-monitor instrument. *International Journal of Medical Informatics, 80*(1), 25-38. https://doi.org/10.1016/j.ijmedinf.2010.10.010.

Arduser, L. (2017). *Living chronic: Agency and expertise in the rhetoric of diabetes.* Columbus, Ohio: Ohio State University Press.

Baker, E. (2023, January 24). Deep fake voice: Everything you should know in 2023. *Veritone Voice.* https://www.veritonevoice.com/blog/everything-you-need-to-know-about-deepfake-voice/

Batistatou, A., Doulis, E. A., Tiniakos, D., Anogiannaki, A., & Charalabopoulos, K. (2010). The introduction of medical humanities in the undergraduate curriculum of Greek medical schools: Challenge and necessity. *Hippokratia, 14*(4), 241–243. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3031316/

Bennett, K.C. (2022). Prioritizing access as a social justice concern: Advocating for ableism studies and disability justice in technical and professional communication. *IEEE Transactions on Professional Communication, 65*(1), 226-240. https://doi.org/10.1109/TPC.2022.3140570

Bivens, K.M., Arduser, L., Welhausen, C.A., & Faris, M.J. (2018). A multisensory literacy approach to biomedical healthcare technologies: Aural, tactile, and visual layered health literacies. *Kairos: A Journal of Rhetoric, Technology, and Pedagogy, 22*(2). http://kairos.technorhetoric.net/22.2/topoi/bivens-et-al/index.html

Blake, S.J., Longo, B., & Wills, K.V., (Eds.). (2006). *Critical power tools: Technical communication and cultural studies.* Albany: State University of New York Press.

Blakeslee, A., & Fleischer, C. (2019). *Becoming a writing researcher,* 2nd edition. Routledge.

Blythe, S., Grabill, J.T., & Riley, K. (2008). Action research and wicked environmental problems: Exploring appropriate roles for researchers in professional communication. *Journal of Business and Technical Communication, 22*, 272–298. https://doi.org/10.1177/1050651908315973

Böhlen, M. (2002). The Open Biometrics Initiative. *Real Tech Support*. http://www.realtechsupport.org/pdf/OpenBiometrics.pdf.

Brignull, H. (2023). Deceptive design. Retrieved from https://www.deceptive.design/

Browne, S. (2015). *Dark matters: On the surveillance of blackness.* Duke University Press.

Buolamwini, J. (2017). Gender shades: Intersectional phenotypic and demographic evaluation of face datasets and gender classifiers. Technical report, *MIT Media Lab*, 01.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM 31*(5), 498-512. https://doi.org/10.1145/42411.42413

Cook, C., Howard, J., Sirotin, Y., Tipton, J., & Vemury, A. (2019). Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science.* https://doi.org/10.1109/TBIOM.2019.2897801

Dorpenyo, I. (2019). Risky election, vulnerable technology: Localizing biometric use in elections for the sake of justice. *Technical Communication Quarterly, 28*(4), 361-375. https://doi.org/10.1080/10572252.2019.1610502

Edbauer, J. (2005). Unframing models of public distribution: From rhetorical situation to rhetorical ecologies. *Rhetoric Society Quarterly, 35*(4), 5–24. https://doi.org/10.1080/02773940509391320

Elmore, K. (2013). Embracing interdependence: Technology developers, autistic users, and technical communicators. In L. Meloncon (Ed.), *Rhetorical Accessibility: At the Intersection of Technical Communication and Disability Studies,* (pp. 15-38). New York, NY: Baywood.

Fadahunsi, K.P., Akinlua, J.T., O'Connor, S., Wark, P.A., Gallagher, J., Carroll, C., Majeed, A., & O'Donoghue, J. (2019). Protocol for a systematic review and qualitative synthesis of information quality frameworks in eHealth. *BMJ Open*, *9*(3), e024722. https://doi.org/10.1136/bmjopen-2018-024722.

Frost, E.A. (2016). Apparent feminism as a methodology for technical communication and rhetoric. *Journal of Business and Technical Communication, 30*(1), 3–28. https://doi.org/10.1177/1050651915602295

Garvie, C., Bedoya, A., & Frankle, J. (2018). The perpetual line-up: Unregulated police face recognition in America. Technical report, Georgetown University Law School, Washington, DC, 10.

Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Green, M. (2021). Risking disclosure: Unruly rhetorics and queer(ing) HIV risk communication on grindr. *Technical Communication Quarterly*, *30*(3), 271-284. https://doi.org/10.1080/10572252.2021.1930185

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *NISTIR.* https://doi.org/10.6028/NIST.IR.8280

Guyan, K. (2022). *Queer data: Using gender, sex and sexuality data for action*. London: Bloomsbury Publishing.

Hannah, M.A., & Arduser, L. (2018) Mapping the terrain: examining the conditions for alignment between the rhetoric of health and medicine and the medical humanities. *Technical Communication Quarterly, 27*(1), 33-49. https://doi.org/10.1080/10572252.2017.1402561

Jensen, R.E. (2015). An ecological turn in rhetoric of health scholarship: Attending to the historical flow and percolation of ideas, assumptions, and arguments. *Communication Quarterly, 63*(5), 522-526. https://doi.org/10.1080/01463373.2015.1103600

Joint Commission. (2022, May). Quick Safety 12: Speech recognition technology translates to patient risk. https://www.jointcommission.org/resources/news-and-multimedia/newsletters/newsletters/quick-safety/quick-safety--issue-12-transcription-translates-to-patient-risk/transcription-translates-to-patient-risk/

Joseph, J. (2022, August 31). Data privacy truly matters to your customers. It's time to make it a core business value. *VentureBeat*. https://venturebeat.com/security/data-privacy-truly-matters-to-your-customers-its-time-to-make-it-a-core-business-value/

Katz, S. B. (1992). The ethic of expediency: Classical rhetoric, technology, and the holocaust. *College English, 54*(3), 255–275.

Katz, S.B., & Miller, C.R. (1996). The low-level radioactive waste siting controversy in North Carolina: Toward a rhetorical model of risk communication. In C.G. Herndl & S.C. Brown (Eds.), *Green culture: Environmental Rhetoric in Contemporary America* (pp. 111-140). Madison, WI: University of Wisconsin Press.

Klare, B.F., Burge, M.J., Klontz, J.C., Vorder Bruegge, R.W., & Jain, A.K. (2012). Face recognition performance: Role of demographic information. *IEEE Transactions on Information Forensics and Security, 7*(6), 1789-1801.

Krishnapriya, K.S., Vangara, K., King, M.C., Albiero, V., & Bowyer, K. (2019). Characterizing the variability in face recognition accuracy relative to race. *CoRR*. https://doi.org/10.48550/arXiv.1904.07325

Larson, S. (2018, March 18). Beyond passwords: Companies use fingerprints and digital behavior to ID employees. *CNN Business*. https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html

Manolev, J., Sullivan, A., & Slee, R. (2019). The datafication of discipline: ClassDojo, surveillance and a performative classroom culture. *Learning, Media and Technology, 44*(1), 36-51. https://doi.org/10.1080/17439884.2018.1558237

McCartney, P.R. (2013). Speech recognition for nursing documentation. *Am J Matern Child Nurs., 38*(5), 320. https://doi.org/10.1097/NMC.0b013e31829c0ae0.

Monahan, T. (2010). *Surveillance in the time of insecurity*. New Brunswick, NJ: Rutgers University Press.

Nakamura, L. (2008). *Digitizing race: Visual cultures of the internet*. Minneapolis: University of Minnesota Press.

Nakasone, H., & Melvin, C. (1989). C.A.V.I.S. https://www.ojp.gov/pdffiles1/Digitization/126675NCJRS.pdf

Ortiz, K. (2023, February 12). Police violence persists even after 3 decades of video. *Axios.* https://www.axios.com/2023/02/12/police-violence-persists-even-after-3-decades-of-video

Pagliery, J. (2015, September 23). Hackers stole 5.6 million government fingerprints - more than estimated. *CNN Business*. https://money.cnn.com/2015/09/23/technology/opm-fingerprint-hack/index.html?iid=EL

Peivandi, S., Ahmadian, L., Farokhzadian, J., & Jahani, Y. (2022). Evaluation and comparison of errors on nursing notes created by online and offline speech recognition technology and handwritten: an interventional study. *BMC Medical Informatics and Decision Making, 22*(1), 96. https://doi.org/10.1186/s12911-022-01835-4.

Piepzna-Samarasinha, L.L. (2018). *Care work: Dreaming disability justice.* Vancouver, Canada: arsenal pulp press.

Raji, I., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. *In Conference on AI, Ethics and Society,* 429-435.

RevealMedia. AI Enabled Body Cameras. *Reveal.* https://www.revealmedia.co.uk/ai

Sava, J.A. (2022, December 12). Biometric technologies - Statistics & Facts. *Statista.* https://www.statista.com/topics/4989/biometric-technologies/

Savytskyi, T. (2022, September 22). Research vs Vision: the origin story of Sony Walkman, Mini Cooper, and the iPhone. *UX Collective.* https://uxdesign.cc/research-vs-vision-the-origin-story-of-sony-walkman-mini-cooper-and-the-iphone-e5c8623968bc

Scott, J.B., Longo, B., & Wills, K. (2007). *Critical power tools: Technical communication and cultural studies.* SUNY Press.

Skinner, D., & Franz, B. (2018). From patients to populations: Rhetorical considerations for a post-compliance medicine. *Rhetoric of Health & Medicine, 1*(3/4), 239-268.

Song, D. (2019, September 23). A short history of deep fakes. *Medium*. https://medium.com/@songda/a-short-history-of-deepfakes-604ac7be6016

Stimson, G.V. (1974). Obeying the doctors' orders: A view from the other side. *Social Science & Medicine, 8*(2), 97-104.

Tsai, P. (2018, March 12). Data snapshot: Biometrics in the workplace commonplace, but are they secure? *Spiceworks.* https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure

Urquhart, C., Currell, R., Grant, M.J., & Hardiker, N.R. (2009). Nursing record systems: effects on nursing practice and healthcare outcomes. *Cochrane Database Syst Rev.* https://doi.org/10.1002/14651858.CD002099.pub2

The U.S. Bureau of Justice Statistics. (2022, January 7). Research on body-worn cameras and law enforcement. *NIJ.* https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement#:~:text=Body%2Dworn%20cameras%20are%20widely,direct%20contact%20with%20the%20public.

Waddell, C. (1996). Saving the Great Lakes: Public participation in environmental policy. In C. G. Herndl & S.C. Brown (Eds.), *Green Culture: Environmental Rhetoric in Contemporary America* (pp. 141-165). Madison, WI: University of Wisconsin Press.

Waitzkin, H. (1993). *The politics of medical encounters: How patients and doctors deal with social problems.* New Haven, CT: Yale University Press.

Walton, R., Moore, K.R., & Jones, N.N. (2019). *Technical communication after the social justice turn: Building coalitions for action*. New York, NY, USA: Routledge.

Youngblood, S.A. (2012). Balancing the rhetorical tension between right-to-know and security in risk communication: Ambiguity and avoidance. *Journal of Business and Technical Communication, 26*(1), 33-62. https://doi.org/10.1177/10506519114211.

Zuckoff, A. (2012). Why won't my patients do what's good for them? Motivational interviewing and treatment adherence. *Surgery for Obesity and Related Diseases, 8*(5), 514–521.

Chapter 5

Concluding Takeaways: A Move towards Advocacy, Awareness, and Transparency

The previous chapter, Chapter 4, is a compilation of the data from the methods, where interlocking surveillance is applied as a methodological framework to analyze healthcare as a site of surveillance based on the collected information from the textual corpus analysis, screening surveys, and interviews. The analysis done in Chapter 4 identifies themes that link the initial communication of biometrics to consumers and institutions, to those who use the technology in healthcare (neonatal nurses), and individual accounts (those interviewed). The themes of compliance, security, and efficiency lead to understandings of the ways technical communicators may resist and intervene in communication practices to determine awareness, advocacy, and transparency in the site of surveillance: healthcare.

This chapter (Chapter 5) focuses on how neonatal nurses can (and do) have a role in the design of communication materials, particularly with patient choice in opting in/out. This chapter discusses implications of security, efficiency, and compliance in healthcare and how technical communicators may intervene. The goal of the technical communicator is to identify how technologies intentionally or inadvertently reinforce structures that produce, reproduce, or maintain inequality. Historically, biometric technologies reinforce structures that maintain inequality. The following sections outline concluding takeaways for technical communicators to consider such as coalitional work, questioning and revising normalized surveillance including ethics of biometric use, and further localization of community input with impacts to privacy including opting out procedures.

5.1 Security, Efficiency, Compliance: Localizing Efforts

Ultimately this study led to better understanding of the "trickle down" effect: biometric companies communicate their solutions with language that emphasizes security/safety, compliance, and efficiency. From there, nurses are trained or taught to use specific biometric solutions, again with the same language the companies are employing to consumers. Nurses adopt this language to communicate with patients. It's almost like a script: I was taught this technology will be more efficient and convenient for my role, and therefore when patients ask why or how I am using the technology, I'll explain it is to help me in my job. Every single nurse interviewed can be summarized by this thought process. Technical communicators have the ability to intervene in this exchange: they can influence the ways biometric solutions are communicated at the source (the companies creating the materials); they can focus on communication between nurses and companies (training materials); and they can influence the patient and nurse exchange (verbal and written communication).

Carolyn Rude (2009) reminds technical communicators that they have the potential to both function as "agents of knowledge making, action, and change" for some and function as agents of oppression albeit often unwittingly for others (p. 176). As public intellectuals, knowledge workers, and advocates for users, technical communicators have a responsibility to "advocate for equity and local and global networks of scientific, technical, and professional communication" (Haas & Eble, 2018, p. 4). Based on the textual corpus, screening surveys, and interviews in this study, scholars and practitioners can and should contribute to the ways that healthcare (broadly defined) understands issues of security, efficiency, and compliance.

I call in neonatal nurses *and* technical communicators because oftentimes neonatal nurses are not responsible for the creation of and distribution of healthcare communication materials.

Even so, neonatal nurses *are* technical communicators: they communicate and negotiate specialized information, *with* and *to* a particularly vulnerable audience. A participatory approach between those who create communication materials, and those who implement it, is necessary to attend to issues of security, compliance, and efficiency in healthcare. Jones (2016) discusses "participatory approaches [that] engage empathy as a conduit to understanding and advocacy" (p. 356). This participatory advocacy work, however, must be localized. Communication in one hospital likely won't look the same in another, despite the similarities in responsibilities and technologies. Agboka (2013) redefines localization as a user-driven approach, in which a user "identifies a need and works with the designer or developer to develop a mutually beneficial product that mirrors the sociocultural, economic, linguistic, and legal needs of the user" (p. 44). Further, Haas (2012) views located accountability as our worldview being "based in an embodied, and therefore partial, perspective—that makes us personally responsible for it. The only possibility for the creation of effective technologies, from this perspective, is through collective knowledge of the particular and multiple locations of their production and use" (p. 293). The takeaways from this study, therefore, *must* be localized. Technical communicators may adapt the general discoveries as they see fit within their own context and embodied perspective.

Dorpenyo (2019) notes that overall, localization scholars will begin to care not only about how to include user knowledge into technology design, but also how to talk to biometric and technology designers. Dorpenyo urges designers to focus on the "limits" of technology; that is, the various "ways technology fails and the nature of the failure and not so much fixation on looking at ways to incorporate user knowledge into design situations" (2019, p. 372-373). Hart-Davidson (2018) posits that, "We have long recognized the perils of a rhetorical education for humans that is devoid of ethical reasoning, but we now must take seriously a new set of

responsibilities to teach machines what to do and what not do with powerful rhetorical strategies" (p. 248). Institutions *should* use elements of interlocking surveillance to engage in awareness, advocacy, and transparency for the means data is collected, stored, and distributed as well as furthering considering ethics of opting out, language use, and communication materials. Technical communicators can help to guide institutions (companies, sites of surveillance, and so on) in making this shift. For example, a recent surveillance tech law, the 2020 Public Oversight of Surveillance Technology (POST) Act, is an example of the ways in which efforts can begin as localized. In this instance, the Act has been used to hold the New York Police Department accountable for disclosing the surveillance technologies that they use—for, you guessed it, safety. Interestingly, an article by Seitz (2023) reported that the New York Office of the Inspector General for the New York Police Department (OIG-NYPD) said the following:

> NYPD was not in compliance with the POST Act orders to publish Impact and Use Policies (IUPs)[84] for existing surveillance tech 180 days after the Act was signed and new IUPs at least 90 days before the use of any new surveillance tech.

The notion of *compliance* is fascinating here, especially as it engages with principles of sousveillance, or watching the watchers. According to Seitz (2023), among the recommendations the OIG-NYPD says the NYPD rejected were reports on the "potential disparate impacts on protected groups of the use and deployment of surveillance technology," disclosing what *external agencies* the NYPD shared data with, and two relating to how it *used* and *audited* its facial recognition technology. The POST Act is one example of ways that technical communicators can advocate for more states to adopt similar approaches to holding institutions (and systems) accountable. Dorpenyo (2019) posits that our role as technical communicators and

[84] The IUPs were supposed to "describe the capabilities of surveillance technology, and include any rules, processes, and guidelines that regulate access to or use of the technology, and any prohibitions or restrictions on its use, and any potential disparate impacts" (Seitz, 2023).

social justice advocates is to inform biometric production companies about how the technologies they design discriminate against certain people (p. 370). Furthermore, the lived experiences of these users (patients, nurses, and more) enables technical communicators to advocate for more transparency and awareness, intervening in those who create biometric solutions to ensure that their technologies are designed to serve every individual in the society. Biometric designers should "conscientiously employ...methods to engage purposefully with issues of social justice and deliberately make more just and equitable design an end-goal" (Jones, 2016, p. 477). As Banks (2006) notes, "Without systematic study of our relationships with technologies and technological issues, we remain subject to those technologies and the larger patterns of racism and racial exclusion that still govern American society" (p. 10). It is important to continue to consider "individual positions within the matrix of domination, oppression, and injustice in addition to institutional, structural, and cultural power relations" (Walton, Moore, Jones, & 2019, p. 126). When all is said and done, at the core of the study is the urgency to recognize and change systems. In fact, we really need regulatory efforts, though this is likely part of a larger study and/or research trajectory outside of the scope of this specific project. Even so, what can be done from this project is to intervene in training and communication materials *about* biometrics *for* those who employ such technologies (and have the technologies implemented *on* them).

Authentication measures, such as biometrics, are an invasion, and prevent individuals from having control over their data. Essentially, patients and nurses as discussed in this study, trade the right to "security" and "privacy" for alleged "convenience" and to "comply," ultimately providing access to the body and potential future harm. The focus should shift from the individual, to the collective, a focus on the assemblage of various connected publics, data, and

the impact of the ubiquity of surveillance and biometrics in healthcare, specifically. For example, Popescu & Brauh (2018) state that current privacy regulations need to change:

> Information privacy imagines the individual as isolated and autonomous; regulating privacy means regulating data collection practices as they pertain to that individual. As we have seen, [recommender systems] RSs rely instead on networks in which the individual is but a node in the larger assemblage of peers, consumed goods, cultural preferences, various connected publics, context signals, and other artifacts. Doing violence to an individual's privacy is violence against an entire network with whom the individual is connected through data transactions (p. 287).

One of the major problems associated with surveillance technologies is how invisible and normalized (or routine) they have become. What will be later discussed throughout this chapter, are concluding takeaways for technical communicators. The following list summarizes some of the main takeaways from this study:

- I call in neonatal nurses *and* technical communicators because oftentimes neonatal nurses are not responsible for the creation of and distribution of healthcare communication materials. Even so, neonatal nurses *are* technical communicators: they communicate and negotiate specialized information. A participatory approach between those who create communication materials, and those who implement it, is necessary to attend to issues of security, compliance, and efficiency in healthcare.
- To fully advocate for patients, and in this study, neonatal nurses, technical communicators and designers of biometric technologies should articulate cultural, political, and biomedical realities in its activist discourse.
- Technical communicators can intervene in the tradeoff fallacy and privacy paradox through the creation and design of materials that communicate transparently (through localizing knowledge) about privacy, data, and surveillance concerns.

Takeaways from this study also build off Popescu & Baruh's (2018) analysis of Recommender Systems (RS) and "their surveillance mechanisms in the flow of culture in order to uncover some of the challenges that recommender systems pose to privacy theory" (p. 280). I include information about Recommender Systems[85] here because of their similarities to how biometric solutions are built. While biometrics are not created with the intention to recommend additional products to consumers, the part of RS that overlaps with the goals of biometrics are through sorting and categorizing based on predetermined categories and characteristics. Ultimately:

> data mining these ever-increasing databases of expressed and implied cultural preferences may contribute to bringing RSs closer to the rhetorically powerful ideal of the personal assistant who knows you better than you know yourself, but also poses significant privacy risks for users whose non-public personal information can be inferred with a high degree of accuracy (Popescu & Baruh, 2018, p. 284).

These Recommender Systems create the illusion that the algorithm *knows* you better than you know yourself; just as biometric solutions create the illusion that they can confirm people are who they say they are.

The following sections focus on usability and user-design of biometric technologies, understanding precarious publics and patient advocacy, and how technical communicators can lay the groundwork for coalitional work (we can't do this alone!).

5.2 Questioning and Revising Norms: Patient Advocacy

Some of the concluding results from the surveys and interviews with neonatal nurses led to questioning of the way security, efficiency, and compliance have "norms" or expected standardized measures. As Chapter 4 uncovered, what personal information or privacy means to

[85] Recommendation system: an artificial intelligence or AI algorithm, usually associated with machine learning, that uses Big Data to suggest or recommend additional products to consumers. These can be based on various criteria, including past purchases, search history, demographic information, and other factors (NVIDIA, 2023).

one person, is not necessarily the same for all. This makes sense: we all approach the world based on our lived experiences and knowledge set. Since technical communicators are involved in decision-making protocols, especially as they relate to the creation of communication materials, this has a large impact on anything public facing. In this study, for example, even if technical communicators are not involved in the actual design process of biometric technologies (though they should be), they can create materials that explore *all* the potential effects of using the technology (re: technologies are not neutral (Noble, 2018; Haas, 2012)). If a company were to disclose or be transparent about the device they are creating (or have created), this would have potential advocacy effects. How so? Say if one of the voice/facial/fingerprinting companies from the study disclosed the helpful *and* harmful effects of their technology. Other companies are not doing this. Rhetoricians would argue that this would appear to be a move towards transparency on the company's end. This shift could increase business, or decrease; however, when users trust a company, that trust relies on the perception of transparency. It reminds me of the commercials for pharmaceuticals: listed (or spoken) very quickly are all the potential side effects of a medication. In essence, the ways technical communicators could intervene are through urging for all the "side effects" of emerging technologies to be public facing. In fact, though the commercial is a metaphor for the ways technical communicators *could* intervene and communicate, companies such as Veridium (2019) have traced examples of biometric authentication through commercials (examples include Olay and WeatherTech, used in Superbowl ads).

When we consider how emerging technologies may be public facing, this study focuses on two populations: patients and neonatal nurses. Not only does this study have implications for patient advocacy, but also the ways neonatal nurses understand and use the technologies that are

required in their roles. Further, as Novotny (2015) notes, feminist approaches to designing public stakeholder input are vital to upholding technical communication's commitment to advocacy. Biometric companies *should* invite users to participate in the creation of the technologies. These technologies aren't going away; in fact, they are increasing more than anything. Because of this, ethical design instead of deceptive design should occur. And calling in precarious publics can help.

To involve users in decision-making protocols takes time and intent. For example, Teston et al. (2019) caution researchers about involving participants in health-related surveying. This notion, however, extends past health-related surveys. When we involve participants in our data collection and as informants, oftentimes they will occupy an added layer of precarity based on not just intersectionality, but also ethics of disclosure. Teston et al. (2019) refers to participants who might be characterized as inhabiting one or more precarious positionalities as those who self-identify as one or more of the following: "racial and/or linguistic minority, economically disadvantaged, disabled, former or current drug user, undocumented, un(der)educated, oppressed, sexualized, disenfranchised, criminalized, and/or colonized" (p. 326). There are complexities inherent with involving people such as ethical concerns, as well as inclusion criteria, privacy, stigmatized and misleading language, accessibility, and liability. Despite the long list of complexities, involving participants is necessary to designing a technology that is usable, and does more help than harm. Ideally, biometrics would not cause any harm at all, but as we've learned, their training and usage to uphold systemic oppression contributes greatly to their usage and implementation now. Technology, as Durack (1997) writes, refers equally to "knowledge, actions, and tools" (p. 258). Technology, as applied to biometric technologies, are a network of constructed assemblages, the knowledge of such technology (including data

dissemination), and design (remember, created *by* people). These findings, uncovered by my methodological framework (interlocking surveillance), call attention to the ways in which biometric technologies are *intended* to be used, how they *justify standardization* and *technological use* by corporations creating the solutions, *categorize* people, how people are *informed* about the capabilities, and how the technology is *poised* (efficiency, safety, compliance). The framework can guide technical communicators in applying such questioning to various sites of surveillance, leading to ways they may intervene and resist specific aspects of the site. This could range in advocacy for transparent communication, for example, or leading training(s) or workshops for specific groups, creating more awareness about the tools and technologies used on them (and others, such as patients).

Furthermore, other than considering how to engage with the public, it is also helpful to understand what public perceptions are of how their data is used and collected. For example, as mentioned in Chapter 1, Lupton & Michael (2017) document how "post-Snowden," participants in the study tended to veer between "recognizing the value of both personal data and the big, aggregated data sets that their own data may be part of, particularly for their own convenience, and expressing concern or suspicion about how these data may be used by others" (p. 254). This aligns greatly with how neonatal nurses responded to issues of privacy and personal information. While nurses recognized the importance of using biometric technologies for ease of use and convenience, they also were concerned about the back end of the product: where did that data really go? Personal digital data is messy. There is a tension between individual role and responsibility; for example, with neonatal nurses there was a concern with their own personal data and biometric usage. However, when they were asked about patients and biometric usage, they claimed that the technologies were secure and more convenient for their jobs. How do we as

technical communicators move towards the same awareness and advocacy for personal protection, for those we influence or who might be part of a precarious public? Two Pew Research Center reports found that most respondents felt that their online privacy was challenged (Madden, 2014; Madden & Rainie, 2015). In fact, very few respondents felt they had much control over the types of data collected on them and how these data are used. Despite the expression of how important preserving personal data privacy is to those in the United States, companies and those implementing biometric technologies do not discuss with patients specifics related to data privacy.

When we consider patient rights and advocacy efforts, technical communicators may also consider what appeals to patients (and consumers) in the first place with biometrics. For example, it's easy to conceptualize the possible benefits of using digital technologies to engage in self-surveillance or complying with "professionals." As patients, (generally speaking) we trust in healthcare professionals and want to remain "in compliance" to help them diagnose, and overall complete their job. Lupton and Michael (2017) write about how participants in their study saw the importance of collecting personal data to promote their health, well-being and productivity (p. 266). It is the assumption that since someone is a nurse, that they are "well-educated" and a figure of "authority." Despite this assumption, it's important to remember that such nurses or even patients who are historically excluded and/or do not have access to education and employment opportunities are at a higher risk for discrimination and breach of privacy. This is exacerbated by not just the overall access to digital technologies, but also the knowledge about how to use these technologies, which increases vulnerability when interacting with digital technologies (Gangadharan, 2015; Rosenblat et al., 2014).

Technical communicators understanding vulnerability in relation to emerging technologies such as biometrics helps to situate communication about patient rights and advocacy. Herman and Chomsky (1988) might associate nurse usage of biometrics with manufacturing consent or creating the appearance of personal agency by leveraging public opinion through propaganda. Bellwoar (2012) explores patients' use of technical health care texts to produce knowledge and design their choices related to their bodies and health. Similarly, neonatal nurses and technical communicators can collaborate to compose documents that produce knowledge about emerging technologies and involve patients in opting in/out procedures. Patients are often not seen as participants or makers of knowledge in the production of healthcare texts, despite their expected "compliance." Bellwoar (2012) argues that approaches to technical communication have focused on issues of "advocacy in community organizations and civic and public discourse as well as everyday life spaces, a focus that is laying a groundwork for further studies of technical communication in everyday life" (p. 329). One focus of technical communication in everyday life is through patient and nurse health literacies.

DeTora (2018) provides a parallel (yet not the same) example of patient advocacy and rights that technical communicators may consider. For example, DeTora (2018) explores the "Right to Try" discourse and argues that it eliminates certain "material considerations—the bodies of sick patients and the realities of biomedical research—in favor of theories of constitutional rights and of limiting corporate liability" (p. 54). This can be linked to the ways in which biometric technologies are enacted "on" patients where there is limiting corporate liability despite the language and expectations that corporations promote. To fully advocate for patients, technical communicators and designers of biometric technologies should articulate cultural, political, and biomedical realities in its activist discourse. This activist discourse, as determined

by my methodological framework, could look like technical communicators (in their various roles) creating and disseminating information about biometrics. This could also look like neonatal nurses questioning opt in/out procedures in their specific healthcare site. Activist discourse could even (and should) look like coalitional work, which will be discussed further in the next section. What would it look like if a collective of technical communicators (in their various roles) questioned the "norms" within the healthcare site? We've witnessed nurses lead protests (re: the 2020+ COVID-19 pandemic): Would this be feasible? Would they *care* enough? Technical communicators are advocates (Jones, 2016) who move from critical analysis to critical change and action. The change or action doesn't *need* to be as drastic as a protest, but it *could* be. This is contextual and should be localized; change will depend on what people want. But if the consensus is that Americans value privacy (Madden, 2014; Madden & Rainie, 2015), then to what extent will technical communicators such as neonatal nurses intervene in the most important aspect of their jobs: protecting their patients?

Despite the seemingly scripted communication materials (by biometric companies to the public; training materials for nurses; and then nurses' scripts for patients), technical communicators can assist in intervening in diverging from scripted practices of medical care for patients. Bellwoar's (2012) study suggests that to diverge from the script, patients should "collaborate with others, resist and transform scripted behavior, and use a variety of texts with varying levels of 'official-ness' to navigate and negotiate seemingly fixed systems of health" (p. 343). Gouge (2018) considers the idea of agency and autonomy in "the patient-centered care movement's emphasis on the patient," and furthermore, biomedicine's tendency to treat evidence-based knowledge as fixed (p. 536). As noted, scholarship about patient communication has led to studies that use compliance and patients' ability to recount what they have been told as

metrics for whether or not communication is effective (Engel et al., 2009; Makaryus & Friedman, 2005; Waisman et al., 2003). As technical communicators know, this is not an accurate measure of effective communication.

As Gouge (2018) discusses, "treating biomedical knowledge as self-evident discounts the ways that knowledge and persuasion in health and medicine are embodied, produced in, and mediated by much more than a concern about what constitutes expert knowledge" (539). Technical communicators have long discussed what legitimizes knowledge and expertise. For example, Segal notes that patient advocacy should shift from compliance and "following doctor's orders," to communication involving "shared decision-making and consensual agreement" (2007, p. 95). Miller (1979) marks one of the first articles to emphasize technical communicators as involved in the knowledge-making and design process, rather than as an end point or part of the production end. That is, power is especially central to the history of the field, not just the role of technical communicators now and moving forward. Power may be exerted throughout the knowledge making process through the influence that technical communicators have in ensuring that those within the process are heard, but mostly those who are affected are privileged. This attention to power is what Frost and Eble (2015) advocate for in asking technical communicators to "resist, subvert, and intervene" (p. 6). These scholars define attributes to the role of a technical communicator and how they may wield the power the field has sought to legitimize for decades.

Patient advocacy and legitimization further comes into consideration with the breach of patient information and data. For example, since biometric technologies are personal identifiers of the body, documents such as driver's licenses and passports are examples of specific personal identifiers. Often during breaches, companies will place responsibility on patient/user to self-

monitor or surveil their data. This usually happens through “free credit monitoring” as witnessed through many examples, but one most recently in California. According to Toulas (2023), the medical breach included “Full name, Social Security Number (SSN), Date of birth, Address, Medical diagnosis and treatment, Laboratory test results, Prescription data, Radiology reports, Health plan member number, and Phone number.” What happens when biometric data is breached? How do we move past individuals to collective responsibility? How do we negotiate nonhuman and human actors in a context of care?

Another popular data breach comes with the rise of telemedicine. More concerning is the tracking and profiting of personal data for company gain. Telehealth has also become an increasingly popular option to expand access to health care for rural and underserved patient communities (Wilkerson, 2023). For example, Wilkerson (2023) cites how a bipartisan group of senators criticized several telehealth startups for failing to protect their patients’ sensitive health information. In an investigation by The Markup and STAT, dozens of telehealth companies shared patient data with Facebook, Google, and other major advertising platforms (Wilkerson, 2023). It’s important to remember that the digital health information shared by trackers is not protected by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA, now decades old, was created long before virtual care was an option; it is apparent that this Act needs to be revised/updated/amended. The Federal Trade Commission has begun to leverage their authority to hold companies accountable for their violations of patient privacy, for entities *not* covered by HIPAA; recent enforcement also includes companies such as BetterHelp (Davis, 2023) and GoodRx. Patient advocacy is complex; this work requires a collective and it requires a push for transparency and awareness across all communication materials.

5.3 Coalitional Work

A major aspect of the discourse in privacy studies is the illusion of personal responsibility. What can *I* do? Rather, what can *we* do as a collective? Change needs to happen with the language surrounding biometric usage, especially in healthcare. This work is coalitional.

One example of recent work rhetoricians and privacy/surveillance scholars have engaged in is the creation of The Digital Rhetorical Privacy Collective (DRP Collective)[86]. The DRP Collective is a coalitional action undertaken to continue to better understand how important digital privacy is not only to dismantling oppression in American society, but also to building an equitable future for all. I am a member of this Advisory Board and find that this is one (of many) collectives and nonprofits engaging in work that spread awareness about technology and privacy/surveillance. The DRPC is an interactive, coalitional resource which features activities, assignments, lesson plans, and other teaching materials for teaching about digital privacy and surveillance in writing classrooms. I am specifically focusing on this example of coalitional work not just because I am a member, but also because this is the first collective engaging in privacy and surveillance work that is situated within the large umbrella of rhetoric and composition.

This coalitional work also extends past the Collective. In fact, technical communicators should employ interlocking surveillance to various sites of surveillance to contend with issues of compliance, convenience, and security. It is important to note that in building a coalition, labor must be distributed in equitable ways. As Jones et al. (2021) suggest, the work must be coalitional, iterative, and it should harness the labor of those with more privilege and power (p. 33). Participatory health intervention projects are one-way technical communicators can engage in coalitional efforts. Participatory localization refers to "user involvement, not as isolated user

[86] https://drpcollective.com/

participation but as user-in-community involvement and participation in the design phase of products" (Agboka, 2013, p. 42). For example, Novotny (2015) calls upon technical communicators to continue to develop methodologies to facilitate stakeholder participation in health policymaking practices as a response to Scott's (2003) ethic of responsiveness. One way that interlocking surveillance furthers Novotny's (2015) call for more feminist intervention is through analyzing communication tactics at the source or site, while also recognizing the surveillance assemblage. For example, scholars such as Snorton (2017) and Gill-Peterson (2018) examine how contemporary medical advances used to provide gender-affirming care for trans people were borne from "centuries of white supremacist abuse" which was enacted by white doctors and their enablers who "targeted, enslaved, incarcerated, institutionalized, and/or kidnapped Black, Brown, immigrant, intersex, disabled, and poor people for the purpose of coerced, nonconsensual, and unnecessary medical experimentation" (and violence) (Frost et al., 2021, p. 224-225). Feminist interventions also require collaboration to call attention to and intervene in the ways research and policies continue to uphold systemic oppression; one way this happens is through categorizing people, as interlocking surveillance suggests. Coalitional efforts as opposed to individual efforts are needed so that technical communicators can engage in participatory health intervention that continue to contribute to work that activists, communities, and scholars have enacted such as (but *certainly* not limited to) resisting the image of an "ideal" candidate for clinical research (George, Duran, & Norris, 2014) and policies that intentionally underfund groups of people, such as that of the Indian Health Services (Jaramillo & Willging, 2021).

By honing in on specific sites of surveillance, intervention may manifest through awareness, advocacy, and/or transparency. How might this coalitional work extend to technical

communicators (such as designers and writers) collaborating with specialists (like neonatal nurses) to bring about change to designs, documentations, or scripts? That's the million-dollar question. If coalitional work is the answer to resisting the technologies, it's going to take a collective to consider how to do this work in a way that protects vulnerable populations and isn't sanctioned by the companies that produce the technology. Technical communicators, traditionally the designers and writers, need to insist on *engaging users* in this coalitional process. If the communication materials from biometric companies are informing training materials for nurses using the technologies, then incorporating neonatal nurses as the users within the design process will ensure all perspectives can be involved and addressed. Further, parents should be involved in the design of training materials too—what do parents value; what do they need to know; what might they expect nurses to communicate or know? For example, Garrison-Joyner and Caravella (2020) explore the usage of graphics as a way to mediate health communication. Though they refer to comics in their discourse, multimodal components should be considered as one way to create accessible training and communication materials. Technical communicators may engage in creating such documents, in conjunction with parent and healthcare provider input, to help "navigate the healthcare system, understand their treatment options, and make decisions regarding their care" (Garrison-Joyner & Caravella, 2020, p. iii). The coalitional and participatory approaches also work towards combating health inequity: as research suggests (Howard, Sentell, & Gazmararian, 2006; Sedore et al., 2006), disparities in health are often caused/exacerbated by low health literacy (see Chapter 2.7). A multimodal approach to creating communication and training materials is one way to address "low" health literacy.

Encompassing different stakeholders and their needs in the design process is one way of working through and addressing varied values and potential tensions. This sharing of knowledge is intentional. Resistance doesn't need to be a coup of an entire system (don't we sometimes wish). Rather, resistance is *intentional.* It is *thoughtful.* Resistance can be something small, like creating scripts for neonatal nurses to read and share with their patients. Or perhaps attending nursing conferences, joining organizations, co-teaching nursing communication courses or guest lecturing, partnering with nonprofits already doing this work (or a version of it)[87], and more. There is a severe tension between biometric solution companies and employers: of course, companies want their product to be purchased, and employers want to maximize efficiency (solely in reference to time and "ease"). The focus, however, can be on the "doers." The doers can be the people such as neonatal nurses and technical communicators as writers and designers, who can inform the larger system by what they *do*. Coalitional work could also look similar to Dautermann's (1993) study, where significant organizational change was attempted by "writers with relatively little power within the hospital, but who were directly involved in the activities regulated by the documents at stake" (p. 98). Here's the thing: if people became just as invested and outraged by biometrics as they are about AI text-generators such as ChatGPT,[88] meaningful change would be far more likely to occur. Overall, resistance involves "ethically evaluating scenarios, teaching others how to identify those scenarios, and considering where and how one can even resist, reject, and replace spaces of surveillance" (Young, 2023, p. 237). Resistance looks different depending on the site.

[87] Again, localized, but I think of organizations such as the Algorithmic Justice League, Data and Society, S.T.O.P, and many more.

[88] This dissertation is being defended during the 2023 rise of AI text generators by Open AI. This outrage also extends to plagiarism detectors like Turnitin attempting to implement "AI detection" to further police students.

Healthcare as a site of surveillance, for example, specifically attends to concerns that interlocking surveillance exposes, including stakeholder (patient and neonatal nurse) input in upholding technical communication's commitment to advocacy and an ethical feminist commitment to facilitating spaces for all citizens to contribute as public intellectuals (Novotny, 2015, p. 61). Since patients, and nurses, are impacted by biometric usage and implementation, it should be practice for participants who are impacted to not only engage in informed consent but also in design choices. This is one example of the ways in which interlocking surveillance attends to levels of informedness or awareness. In a special issue focused on conceptualizing communities who have been historically excluded and ignored in healthcare and medical communication, Frost et al. (2021) reference a long list of scholars engaging in coalitional work. This includes scholars engaging in work that focuses on multiply-marginalized individuals and collectives—particularly Black people—which have long engaged "methods and strategies designed to navigate (and resist) structural oppression in healthcare" (Jones & Williams, 2020 as cited in Frost, 2021, p. 224). Though often not explicit, this is one example of the ways biometrics are poised as determined by interlocking surveillance, and how they are communicated in their *intended* use.

Coalitional work can happen cross-institutionally, as with the DRPC. The goal of this work, of course, is to extend public facing. To do this, collaboration with nonprofits and groups already engaging in advocacy work is crucial. Collaboration and coalition *looks* different depending on the goal. For example, recent popular news articles engage in the "tradeoff fallacy." That is, misrepresentation of consumers by marketers. In studies published about United States consumers regarding privacy, oftentimes consumers are largely misrepresented, and research focuses on a small (and selective) portion of the population. Turow, Hennessy, &

Draper (2016) for example, indicate that marketers are misrepresenting a large majority of Americans by claiming that Americans give out information about themselves as a tradeoff for benefits they receive (p. 3). To the contrary, the survey reveals most Americans do not believe that 'data for discounts' is a square deal. Turow et al. (2016) report that marketers justify their data-collection practices with the notion of tradeoffs, "depicting an informed public that understands the opportunities and costs of giving up its data and makes the positive decision to do so" (p. 3). For example, a Yahoo report (2014) concluded that online Americans "demonstrate a willingness to share information, as more consumers begin to recognize the value and self-benefit of allowing advertisers to use their data in the right way." Coalitional work can address the tradeoff fallacy: the false misconception that Americans are aware of their data collection, especially as it relates to surveillance in healthcare. The end goal of this "tradeoff" illusion, according to Turow et al. (2016) is to claim to policymakers and the media that "Americans accept widespread tracking of their backgrounds, behaviors, and lifestyles across devices, even though surveys repeatedly show they object to these activities" (p. 3). Technical communicators can intervene in the tradeoff fallacy and privacy paradox through the creation and design of materials that communicate transparently (through localizing knowledge) about privacy, data, and surveillance concerns. As Dorpenyo and Fernandez (2022) note, technical communicators can engage in coalitional work in their own practice, but also in the classroom to equip students with the tools to dismantle unjust and oppressive practices.

In some ways, this study is an example of resistance, or intervention. Months after I interviewed the 10 neonatal nurses, I reached out to ask them if since our interview, they had thought differently about biometrics and/or privacy. One nurse mentioned that without thinking through the scenarios I provided in the interviews they would not have thought about the ways

they communicate with their patients about new technologies. Another nurse responded: "Since our interview, you have expanded my knowledge on how biometrics will serve healthcare. I feel cautious about new technology but excited that healthcare is making it easier to apply. Thank you for the interview." This is where coalitional change can occur: through the ways in which technical communicators can influence who we research with, and for. Another nurse stated:

> Since our interview, I have become more mindful of the implications of biometric technology on patient privacy and security. I have become increasingly aware of the need for organizations to take a proactive approach to protecting patient information and ensuring that biometric data is stored and used in a secure manner. I am determined to ensure that any biometric data used in a healthcare setting is done so in a secure and respectful manner that is in line with patient privacy laws.

I'm determined, too, to ensure that patients are protected from the invisible forms of harm that occur when they don't have the opportunity to opt out of technologies.

To reiterate, from this study, I have found that technical communicators have the ability to influence the ways biometric solutions are communicated at the source (the companies creating the materials); they can focus on communication between nurses and companies (training materials); and they can influence the patient and nurse exchange (verbal and written communication). To summarize thus far, suggestions for technical communicators have included the following:

- Redefining what it means to *be* a technical communicator. Neonatal nurses *are* technical communicators: they communicate and negotiate specialized information. A participatory approach between those who create (design) communication materials, and those who implement them, is necessary to attend to issues of security, compliance, and efficiency in healthcare.
- To fully advocate for patients, technical communicators (in all their roles) and designers of biometric technologies should articulate cultural, political, and biomedical realities in

its activist discourse. Such discourse is contextual and should be localized yet may provide *awareness* through creating and disseminating information about biometrics; *advocacy* for opt in/out procedures; and *transparency* about the ways in which biometric solutions politicize categorizing people.

- Technical communicators can intervene in the tradeoff fallacy and privacy paradox through the creation and design of materials that communicate transparently (through localizing knowledge) about privacy, data, and surveillance concerns.

The following section discusses usability and design concerns with biometric technologies. Of course, much of this has been analyzed throughout this study, but it is an important takeaway. Further, we should remember that biometric technologies are biopower, or the discursive control and regulation of the perceived choice individuals have in making decisions in regard to their health. This perceived choice is often due to deceptive design.

5.4 Usability, Design and Ethics

As mentioned, this study shows how there needs to be a shift from deceptive design of biometric technologies to ethical design. As I, and other scholars such as Dorpenyo (2022) and Haas (2012) have noted, [biometric] technology is often viewed as an objective, neutral, and powerful technology which authenticates and verifies the identity of individuals accurately. Barnum's (2001) definition of usability indicates a focus on the user and not the product, she also stated that her book is about ''the place that usability testing...holds within the process of *developing products* [emphasis added] that work for users'' (p. 2). Further, scholars such as Gilson (2021) and Sun (2012) posit that in the classroom setting, students' interactions with users and user-testing are explicitly intended to "counteract the ethic of expediency associated with the engineering model of usability" and instead, focuses on increased user involvement,

knowledge legitimization, and reframing users as participants instead of subjects (Sun, 2012, p. 36-37; Gilson, 2021, p. 179). Technical communication health care documents are studied primarily as they are produced in medical settings (Dautermann, 1997; Spafford, Schryer, Mian, & Lingard, 2006). There is ample opportunity for technical communicators to intervene in not just the documents created for biometric technologies, but also the design process and neonatal nurse interaction with patients. Participatory methods, however, do not necessarily render the design process or its products just. As my methodological framework suggests, interlocking surveillance, technical communicators should take an advocacy perspective in design. As Rose (2016) similarly expresses, advocacy in design is particularly crucial for systems and policies (such as healthcare) that are designed for a broad swath of users (p. 442). This study is foundational for questioning: what does it mean to design for opting out? As I referenced in Chapter 5.3, this work is coalitional and would need to involve many different stakeholders in the design process. This participatory approach is a valuable model, though, for how companies can "prove" they are committed to engaging in inclusive and equitable design. To involve all stakeholders in the process, though time consuming, would be one step towards a more humanistic world. For example, what would it look like for companies to have a "privacy" score? Better yet, what would it look like for companies to have a "humanistic" score? Think of this as similar to walking into a restaurant in the United States and seeing the health rating on the wall. The score might also be similar to what many companies currently have—security ratings—but this is not standardized across companies (Holmes, 2023). Nor does the security rating remain consistent for what it's measuring within the company. Components that may determine a privacy score could be the communication materials, such as training materials, for nurses. The criteria could also include who is involved within the design process, and what

"occurs" during the training procedures. How do we make the "scripts" neonatal nurses communicate with patients more humanistic? How do we give parents the language to opt out? How do we honor and incorporate the knowledge and expertise that neonatal nurses have in these scenarios?

According to Light and Luckin (2008) we can design *for* social justice. And we can do this with biometrics. It's important to return to the beginning of this chapter: design is going to look different depending on context. We can localize design, and we can also include local communities in decision-making protocols. This looks different depending on the biometric solution, company, people, goals, and site of surveillance (or implementation). Light and Luckin (2008) mention that "participative design" approaches in which users and professional designers have a more equal say in taking design decisions is a potential effective approach to the design process, agency, and informed consent. Despite the length of time contributing to concerns with participatory design, this process can be more efficient instead of creating a product that does not involve "non-specialists" in the design process. Fleck (1993, 1994) and Stolterman (2001) make a point that the distinction between the designer and the user can become blurred at the time of use, as the user alters the design by the very act of using it (Light & Luckin, 2008, p. 15). If participants cannot give insights into the design process of biometrics themselves, then another starting place is with the communication materials. Perhaps this is through the website, consent documents, instructional sets and training, and more. None of these documents or aspects of biometrics are useful until topics such as how the technology impacts people, usability, content, as well as access, have also been considered.

Parvin (2023) furthers the conversation of social justice in design through considering ethics: "Ethics is intrinsic, if not assumed, in formal definitions and cultural assumptions about

design, either through recognizing design's purposeful nature or more directly by asserting its role to serve people and communities." As I mentioned in my study, efficiency is often discussed in terms of output (speed and time), for both the emerging technology (such as biometrics) and for the usage/perception of the technology's role in the site of surveillance (healthcare). Efficiency has often been a design concern as it relates to the production of material goods. As Parvin (2023) notes, it is crucial to be attentive to the "intersectional workings of power and privilege" and the "positionality of designers, design teams, and design organizations" especially since we do live and engage in a "world built by and for economically privileged, white, cisgender, male bodies." An example of design concerns with biometrics occur in Keshavarz (2018) scholarship, which draws attention to technologies that reinforce national hegemonies such as borders and passports. Keshavarz (2018) argues that not only Black and Brown bodies are framed as "illegal travelers across the artificial constructs of borders"; but also, that ideas, languages, and ways of being and knowing are rendered "illegitimate, ill-formed, incomprehensible, and even nonsensical" (Schultz et al., 2018, p. 87–89). Technical communicators should consider *who* designs and *for* whom.

Effective participative design can lead to a greater understanding of the design process by all, with participants becoming more skilled in design processes, and, through their participation, learning more about their own potential agency. This is the goal: engaging in the design process through participation and informing biometric companies about the ways they may actually communicate informed consent, even if "opting out" is not an option. Biometrics are not neutral, and user design and usability studies can disrupt this notion. The notion of informed consent comes from medical ethics, to protect patients' autonomy. As Véliz (2022) notes, while the medical profession is intended to aid patients, companies are typically wanting to profit from

their users. This means that terms and conditions are written to protect companies—not people—from liability. Terms and conditions are usually unreasonably long, non-negotiable, and can change at any time without previous warning. Even if the terms and conditions were short, and "easily" readable, there is arguably no such thing as informed consent in the context of the data economy. And though in the healthcare context, we may be able to justify the collection of some personal data (i.e., clinical tests, a list of symptoms, etc.), justification of ubiquitous surveillance and trading personal data for care should not occur. Collecting data in medical contexts is justified; selling or distributing that data might not be.

As we become more reliant on technologies, we need feminist and social justice methodologies to guide technical communicators in intervening in the ways technologies "determine important aspects of who we are" (Koerber, 2000, p. 66). Murray (2007) reveals that the biometric technology cannot "read all bodies equally" (p. 347), and that the biometric produces "illegible biometric bodies" (p. 348). The data collected in this study suggests that biometrics are believed to be credible, safe/secure, convenient and efficient, and remain in compliance. This tension between what the biometric *is* versus how it is communicated and perceived is stark. How do we move toward understanding technologies for what they are and who they impact? Perhaps it is through the ways such solutions are communicated and trained.

Technical communicators also need to approach emerging technologies through social justice and feminist methodologies. As interlocking surveillance suggests, we can understand sites of surveillance and technical communicators' role in decision-making processes through the promotion of awareness, advocacy work, and transparent language/practices. How do we ensure that the site is contributing to increasing awareness, transparent practices, and advocating for

ethical design and practices? I apply the following questions to sites of surveillance to better understand where technical communicators may intervene, resist, and inform:

- What are the intended purposes of the technology?
- How does the corporation justify its standard usage?
- How does it categorize people and into what categories (and for what purpose)?
- How does the corporation justify its technological usage?
- How are people informed about the capabilities, data collection, and more?
- Is the technology poised for efficiency purposes, or implemented during a time of "urgency"?

These questions, as a heuristic, may be applied to *any* site of surveillance. Sites extend from healthcare to popular surveillance sites such as the classroom, airport, and other workplaces outside of higher education (among *many* more). The guiding questions, once answered, may assist technical communicators in determining *where* their interventions need to occur. For example, if they determine that people are not informed about the biometric capabilities, then technical communicators can intervene as they see fit for the specific site. How *should* people be informed? *What* do they need to be informed of (is this *everything* about biometrics, or something specific such as what information is being collected from people, or ways to opt out)? My methodological framework expands feminist observations and definitions of technology (Koerber, 2000, p. 60); however, it also extends past the ways that technologies have not only excluded the historical contributions of women, but also historically excluded populations such as those who are Black, people of color, Indigenous, disabled, and LGBTQIA+. And though feminist scholars can and should "move beyond the design and development phases of technology," interlocking surveillance's goal of intersecting feminist concerns as applied to

technical communication and surveillance studies affords the care and attunement to the ways we can collaborate with and ethically design technologies (Koerber, 2000, p. 60). Technical communicators can, as I'll discuss further in the next section, attempt to determine what we can learn about the political effects and consequences of technology from observing the design and development phases of new technologies to promote awareness, advocacy, and transparency. As my study outlines, we can holistically chart the impacts of communicating about technologies to implementation, alongside usages and perceptions of such. Feminist interventions need to happen as technologies are designed, produced, and communicated, because such technologies, as we've witnessed with biometric technologies, are "typically incorporated into existing institutions and practices, which cause them to reinforce status-quo meanings of phenomena such as race and gender rather than foster new meanings" (Koerber, 2000, p. 68). Further, as the takeaways from this study suggest, technical communicators can recognize the challenges of creating "technical documents that support increased health literacy for vulnerable patient populations" as an opportunity to practice "socially just community-engaged research, design, and communication" (Garrison-Joyner & Caravella, 2020, p. viii).

5.5 Advocacy, Transparency, Awareness: Calling in and Future Research

As Dorpenyo (2019) notes, there are various ethical implications of the design of biometric technology. Who gets accepted or rejected by a design is a matter of ethics (Katz, 1992; Rose, 2016) and access (Banks, 2006; Haas, 2012). Technology communicators or designers may overzealously make a case for the objective nature of the technology while neglecting other moral or social consequences. As technical communicators and social justice advocates, we may be complicit in unethical behavior if we "glorify the technical prowess of the biometric or any technology and stand aloof to concerns that the biometric rejects specific groups

of people" (Dorpenyo, 2019, p. 371). This section further documents resistance tactics through promoting awareness and advocating for transparency. Is transparency an achievable goal? I think so, and here's why.

Transparency often involves the efforts to "uncover" state and corporate surveillance tactics (Monahan, 2022). As I wrote throughout Chapter 3.3, transparency can be a goal while also acknowledging that approaches to transparency are contextual and need to be critically examined. Transparency must be *intentional.* For example, transparency can look like glimpses into a system, a means to see the often invisible "controlling logics of institutional surveillance" (Monahan, 2022, p. 50). As Wajcman reminds us, technologies are always "inextricably linked to particular institutionalized patterns of power and authority" (1991, p. 63), meaning that they never act independently of humans, even if biometrics are often touted or communicated as rhetorical agents. Algorithmic usage in healthcare has shaped life in largely invisible and unequal ways (Barocas & Selbst, 2016): such systems dictate what "resources and services one has access to based upon assessments of one's relative risk or value" (Monahan, 2022, p, 55). I think about, for example, Alexander and Edenfield's (2021) article about accessing medical resources in marginalized communities. This article specifically addresses a series of barriers trans African American patients experience, and further documents how technical communicators can help healthcare practitioners "address social stigmas, social injustice, and social barriers to medical resources, as well as tactics that destabilize those barriers" (p. 245). This article, in combination with my financial and access barriers in this study, led me to consider the ways academics engage with multiply marginalized populations. Alexander and Edenfield (2021) urged scholars for better research in assisting marginalized communities. Part of this research is pushing against and intervening in the institutionalized oppression that creates such barriers. I saw this in my

research: how do we, as technical communicators and scholars, break down the walls that prevent or seek to prevent access to communities who are most impacted by the research that we do? Alexander and Edenfield (2021) cite astounding statistics about medical harassment and discrimination; much of this accounts for why, I can only assume, a select population took my screening questionnaire, and an even lower number elected to be interviewed. Though Alexander and Edenfield (2021) specifically focus on African American and trans populations, their takeaways help contribute to understandings of a much larger public safety issue. Academics and the local community *need* to collaborate to attend to issues of safety and security especially as they relate to healthcare. And as Agboka (2013) identifies, we cannot take a universalizing approach to localization because this can further marginalize users.

Biometric technologies contribute to the oppressive nature of the healthcare institution; but who will hear this? We need to create and sustain community, corporation, and organizational relationships to respond to and intervene in what is harming so many vulnerable populations. We need a coalition. If, as the nurses in my study claim, that their role and responsibility is to care for the whole person/patient, then it should be deduced that part of the whole person are the invisible ways they may be caused harm due to the multitude of implications of using biometric technology. Sustainable collaboration is a form of resistance. This form of resistance, however, is much larger than some of the smaller, tangible claims that I referred to before (5.3). This collaboration responds to a tension that is key to *why* the United States hasn't seen policies in place regulating privacy, and biometrics broadly construed. One out of many reasons: we live in a neoliberal society. Neonatal nurses and technical communicators (as designers, writers, instructors) may resist the ways biometrics are communicated by becoming the designers (working for the companies). Easier said than done, right? But it is true

that technical communicators *are* designers and *do* write the content for the biometric solution pages. Further, for many of us, we are also instructors dedicated to teaching current and future technical communicators. Technical communicators can also work on motivating companies to *be* transparent and change their protocols through collaborating with lobbyists, politicians, and others who are in positions of power. Change *can* happen; we've witnessed it with some of the General Data Protection Regulation (GDPR)[89] legislature. Creating a community that is invested and cares is the first step. Communities can solve problems together: "communities collect data about problems, test ideas for change, organize pressure campaigns, and take civic action" (Matias, 2023). As Matias (2023) describes, equitable technology governance will occur through community networks who have "relationships of reciprocity with scientists, journalists, and NGOs." There are groups already doing the work, reciprocal work with communities, that technical communicators can further build.

Part of the issue with community-engagement is that scholars need to understand communities engage in very different ways, especially in healthcare. Scholars in technical and professional communication have discussed strategies for engagement (or lack of) with communities. For example, Alexander and Edenfield (2021) discuss one approach to understanding, which is tactical technical communication: a means of documenting one way of doing something (p. 243). Tactical technical communication is extra-institutional communication that takes place "outside, between, and through corporations and other institutions," and "in the gaps between" institutions (Kimball, 2006, p. 67-68). Kimball (2006) marks tactical technical communication as a means by which "users have appropriated technology to increase their freedom of agency" (p. 68). Agency, autonomy, and informed consent are all topics that arise

[89] General Data Protection Regulation: Regulation in European Union (EU) law on data protection and privacy in the EU and the European Economic Area.

when we discuss the relationship between patients and technology. I therefore propose the following research questions for readers, technical communicators, and scholars to consider:

- How do technical communicators such as neonatal nurses advocate for or engage in informed consent of biometric technologies?
- How do technical communicators communicate the potential harms to already vulnerable populations, many of which delay receiving medical care because of the systemic oppression and discrimination in healthcare?
- How do technical communicators advocate for a shift in language surrounding privacy and security as personal responsibility, to collective?

Biometrics are not going away any time soon. In fact, their presence is increasing. Durack (1997) expresses that technical writing exists to accomplish something, and is a form of social action (Cooper, 1996, p. x). We, as technical communicators, need to engage in the ethical design of the technology, but we also need to advocate for awareness (through proper informed consent) and transparency of data collection practices. This responsibility largely falls on the corporations creating and distributing the biometric solutions. But this can also be a responsibility of technical communicators. The way technical communicators, such as neonatal nurses, communicate with patients (and other stakeholders) about privacy, ability to opt out, and biometrics in general can be different. Neonatal nurses can allow for opting out, even if this leads to making our jobs less "easy." Technical communicators can urge biometric companies to disclose their practices more fully. It is not enough anymore to place a privacy policy on a website. For example, Turow et al. (2023) writes how current privacy law still relies on industry self-regulation and individual privacy self-management: "companies post privacy policies that detail the information they collect and individual consumers are tasked with reading and

understanding these policies and making decisions about whether to use a website. This regime is known as 'notice-and-consent'" (p. 3).

Furthermore, technical communicators need to be aware of the ways communication about technology could potentially marginalize local, nondominant knowledge systems whereas it privileges global, dominant knowledge systems (Dorpenyo, 2022). Current representation of the biometric technology as documented through my corpus analysis, screening surveys, and interviews displays how technical communicators can become complicit in silencing, excluding, and marginalizing local voices. As Dorpenyo (2022) notes, technical communicators can "call attention to how communication that focuses on dominant narratives obscures and delegitimizes the knowledge of disenfranchised and less privileged groups" (p. 291). In fact, one of the major takeaways of this study is that through examining the corpus of communication materials collected from biometric solutions companies, technical communicators need to intervene in the design of *both* texts and technologies.

Biometrics reflect a new world of interconnected technologies that are communicated and will influence and define people in new ways. For example, recent voice technologies can infer your emotional state by the sound of your voice. Imagine the impacts in healthcare: your voice state being used to decide how long to keep you waiting or to triage you to an agent who is successful at satisfying and even "upselling" people with your emotions and purchase history? (see Turow, 2021). Though possible, it is not easy to change your biometric data. Even so, people give opt-out or opt-in "consent" to the collection of their bodily data every day. As Kearns and Roth (2019) argue, understanding how opt-in/out data feeds automated decision-making systems, geolocation tracking, and biometric analyses, among other high-tech tools,

requires individuals to read about, process, and make decisions based on algorithmic information even many experts do not comprehend.

To summarize, from this study, technical communicators may take away the following main points:

- Technical communicators are not just those who create documents or design web content. Neonatal nurses *are* technical communicators: they communicate and negotiate specialized information. We can further redefine what it means to be a technical communicator.
- Technical communicators can engage in a participatory approach between those who create communication materials, and those who implement it. This is necessary to attend to issues of security, compliance, and efficiency in healthcare.
- Technical communicators and designers of biometric technologies should articulate cultural, political, and biomedical realities in its activist discourse.
- Technical communicators can engage in the design process through participation, and informing biometric companies about the ways they may actually communicate informed consent, even if "opting out" is not an option.
- Technical communicators can engage in the ethical design of the technology, but we also need to advocate for awareness (through proper informed consent) and transparency of data collection practices.
- Technical communicators can intervene in the tradeoff fallacy and privacy paradox through the creation and design of materials that communicate transparently (through localizing knowledge) about privacy, data, and surveillance concerns.
- Technical communicators can intervene in the design of *both* texts and technologies.

Technical communicators (Williams, 2022; Smith, 2000; Moore, 2017; Roundtree, 2019; Sackey, 2019) have researched the intersection of technical communication and public policy. Other than the provided bulleted list, other research and direction might focus on recent legislation regarding biometric identification especially as it relates to what "counts" as identification and explicit neglect of the impacts of biometrics on people. For example, according to LegiScan, in Nevada, New York, Rhode Island, North Carolina, and West Virginia, an act relating to drivers' licenses is requiring, under certain circumstances, that the Department of Motor Vehicles place a designation on a driver's license for certain persons with autism (NV AB161, 2023). Technical communicators can intervene in these ableist, racist, and sexist oppressive and violent systems. As I've stated before, biometrics are not going away. It would be nearly impossible to list *all* of the current biometric news. There are developments, integrations, and tools, updated weekly. At the time of writing this additional section (week of February 19, 2023), for example, the Biometric Information Privacy Act (BIPA) "White Castle" case took center stage, where Illinois Supreme Court held that a separate BIPA claim accrues for every biometric scan or transmission. According to the National Law Review, BIPA provides that a party may not, without consent, "collect, capture, purchase, receive through trade, or otherwise obtain" a biometric identifier (Kaltenbach & Zielinski, 2023). Further, a party may not "disclose, redisclose, or otherwise disseminate" a biometric identifier or biometric information without consent (Kaltenbach & Zielinski, 2023). As this example suggests, biometric legislation is and has been hitting the court system. Employers and others using biometric identifiers should take note to adopt consent and policy requirements, not just businesses in Illinois. A bill establishing consumer health data rights known as ESHB 1155,[90] or "My Health, My Data Act," has passed

[90] Washington Public Affairs Network

both chambers of the Legislature in Washington, United States. The rights allow Washingtonians the "right to access, delete, and withdraw consent from the collection, sharing, or selling of their consumer health data" (Zucco, 2023). The current moves towards regulatory protections for biometric and consumer health data have been on the rise in the United States (as I'm finishing this dissertation in April 2023). States should take notice of the increase in efforts towards introducing ways to protect people that extend into the digital sphere.

Future research could expand on this collected information by localizing biometric usage in a specific (and willing to collaborate) healthcare system to understand *precisely* how nurses are communicating issues such as undocumented status and insurance claims to vulnerable patients (re: section 4.6c). This would further the perception conversation to focus on communicative interaction, and could contribute to conversations about delivery, ethos, power dynamics, and so on. Technical communicators may also consider research into a comparative analysis across all stakeholders within a healthcare system. This might include expanding (or narrowing) a scope to focus on disclosure documents, as well as positioning of retention through acquiring emerging technologies such as biometrics, and what is considered "data" to stakeholders. As I mentioned in 4.3b, the stakeholders involved (for example, neonatal nurses) could have many systemic and infrastructural factors that influence their implementation of the most recent emerging technologies, such as biometrics. Technical communicators could also consider the ways in which the location (or type) of a facility impacts implementation of biometric technologies. Preliminary research from this study suggested that nurses interviewed believed implementation correlated to cost/finances, and overall incidentals. More research would need to be conducted in this area.

5.6 Chapter Summary

This Chapter (5) focuses on how neonatal nurses can (and do) have a role in the design of communication materials, particularly with patient choice in opting in/out. This chapter discusses implications of convenience, efficiency, and compliance in healthcare and how technical communicators may intervene. The Chapter documents several takeaways for technical communicators to consider such as coalitional work, questioning and revising normalized surveillance including ethics of biometric use, and further localization of community input with impacts to privacy and design including opting out procedures.

In the next chapter, I use the conclusions of this study to inform the ways technical communicators might engage this work in the classroom. Chapter (6) applies themes of security, efficiency, and compliance to programmatic application in the technical communication classroom through examining how a technical communication course may benefit from exploration of surveillance technologies in healthcare (and other sites of surveillance). As healthcare (and many other industries) become increasingly reliant on digital technologies, it is imperative for faculty (and students) to explore the ways pervasive technologies impact our agency, privacy, communication practices, and personal/professional lives and careers. The Chapter builds off this Chapter (5) by providing insights into the programmatic and pedagogical impacts of my dissertation study and its exigency in technical communication classes/programs.

REFERENCES

Agboka, G.Y. (2013). Participatory localization: A social justice approach to navigating unenfranchised/disenfranchised cultural sites. *Technical Communication Quarterly, 22*(1), 28-49. https://doi.org/10.1080/10572252.2013.730966

Banks, A.J. (2006). *Race, rhetoric, and technology: Searching for higher ground* (1st. ed.). Routledge, New York, NY.

Barnum, C. (2001). *Usability testing and research*. New York, NY: Longman.

Barocas, S., & Selbst, A.D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671-732.

Bellwoar, H. (2012). Everyday matters: Reception and use as productive design of health-related texts. *Technical Communication Quarterly, 21*(4), 325-345. https://doi.org/10.1080/10572252.2012.702533

Cooper, M. (1996). Foreword. In A.H. Duin & C.J. Hansen, *Nonacademic writing: Social theory and technology,* (ix-xii). Mahwah, NJ: Lawrence Erlbaum.

Dautermann, J. (1993). Negotiating meaning in a hospital discourse community. In R. Spilka, (Ed.), *Writing in the Workplace: New Research Perspectives* (pp. 98-111). Carbondale, IL: Southern Illinois University Press.

Dautermann, J. (1997). *Writing at Good Hope: A study of negotiated composition in a community of nurses.* Greenwich, CT: Ablex.

Davis, J. (2023, March 3). BetterHelp to pay FTC $7.8M for privacy failures, unfair practices. *SC Media: A Cyber Risk Alliance Resource.* https://www.scmagazine.com/news/privacy/betterhelp-pay-ftc-7m-privacy-failures-unfair-practices

DeTora, L. (2018). The dangers of magical thinking: Situating right to try laws, patient rights, and the language of advocacy. *Rhetoric of Health & Medicine, 1*(1) 37-57. https://www.muse.jhu.edu/article/710562.

Dorpenyo, I.K., & Fernandez, L. (2022). Towards a social justice agenda: Learning outcomes as a site for coalition building. *Programmatic Perspectives, 13*(1), 114-130.

Dorpenyo, I.K. (2022). Local knowledge as illiterate rhetoric: An antenarrative approach to enacting socially just technical communication. *Journal of Technical Writing and Communication, 52*(3), 291-315. https://doi.org/10.1177/00472816211030199

Durack, K.T. (1997). Gender, technology, and the history of technical communication. *Technical Communication Quarterly, 6*(3), 249-260. doi:10.1207/s15427625tcq0603_2

Engel, K.G., Heiser, M., Smith, D.M., Robinson, C.H., Forman, J.H., & Ubel, P.A. (2009). Patient comprehension for emergency department care instructions: Are patients aware of when they do not understand? *Annals of Emergency Medicine, 53*(4), 454-61.

Fleck, J. (1993). Configurations: crystallizing contingency. *International Journal of Human Factors in Manufacturing, 3*(1), 15-36.

Fleck, J. (1994). Learning by trying: The implementation of configurational technology. *Research Policy, 23*, 637-652.

Frost, E.A., & Eble, M. (2015). Technical rhetorics: Making specialized persuasion apparent to public audiences. *Present Tense, 4*(2). Retrieved from http://www.presenttensejournal.org/wp-content/uploads/2015/04/FrostandEble.pdf

Frost, E.A., Gonzales, L., Moeller, M.E., Patterson, G., & Shelton, C.D. (2021). Reimagining the boundaries of health and medical discourse in technical communication. *Technical Communication Quarterly, 30*(3), 223-229. https://doi.org/10.1080/10572252.2021.1931457

Gangadharan, S.P. (2015). The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. *New Media & Society.* https://doi.org/10.1177/1461444815614053

Garrison-Joyner, V., & Caravella, E. (2020). Lapses in literacy: Cultural accessibility in graphic health communication. *Technical Communication Quarterly, 29*(3), iii-xxv, https://doi.org/10.1080/10572252.2020.1768295

George, S., Duran, N., & Norris, K. (2014). A systematic review of barriers and facilitators to minority research participation among African Americans, Latinos, Asian Americans, and Pacific Islanders. *American Journal of Public Health, 104*(2), 16–31. https://doi.org/10.2105/AJPH.2013.301706

Gill-Peterson, J. (2018). Trans of color critique before transsexuality. *Transgender Studies Quarterly, 5*(4), 606-620. https://doi.org/10.1215/23289252-7090073

Gilson, O.A. (2021). An intersectional feminist rhetorical pedagogy in the technical communication classroom. In R. Walton & G.Y. Agboka (Eds.), *Equipping Technical Communicators for Social Justice Work: Theories, Methodologies, and Pedagogies* (pp. 178-194). University Press of Colorado. http://www.jstor.org/stable/j.ctv1mjqtfr.13

Gouge, C. (2018). Getting the knowledge right: Patient communication, agency, and knowledge. *Journal of Medical Humanities, 39*(4), 535-551. https://doi.org/10.1007/s10912-016-9389-1

Haas, A. (2012). Race, rhetoric, and technology: A case study of decolonial technical communication theory, methodology, and pedagogy. *Journal of Business and Technical Communication, 26*(3), 277-310. doi:10.1177/1050651912439539

Haas, A.M., & Eble, M.F. (Eds.). (2018). *Key theoretical frameworks: Teaching technical communication in the twenty-first century.* Logan, UT: Utah State University Press.

Hart-Davidson, W. (2018). Writing with robots and other curiosities in the age of machine rhetorics. In J. Alexander & J. Rhodes. (Eds.). *The Routledge Handbook of Digital Writing and Rhetoric* (pp. 248-257). Routledge.

Herman, E.S., & Chomsky, N. (2002). *Manufacturing consent: The political economy of the mass media.* New York: Pantheon.

Holmes, R. (2023, March 24). What are security ratings? A complete and authoritative guide. *BitSight*. https://www.bitsight.com/blog/what-is-a-security-rating

Howard, D.H., Sentell, T., & Gazmararian, J.A. (2006). Impact of health literacy on socioeconomic and racial differences in health in an elderly population. *Journal of General Internal Medicine, 21*(8), 857-861. https://doi.org/10.1111/j.1525-1497.2006.00530.x

Jaramillo, E.T., & Willging, C.E. (2021). Producing insecurity: Healthcare access, health insurance, and wellbeing among American Indian elders. *Social Science & Medicine, 268*(113384), 1-8. https://doi.org/10.1016/j.socscimed.2020.113384

Jones, N.N. (2016). The technical communicator as advocate: Integrating a social justice approach in technical communication. *Journal of Technical Writing and Communication, 46*(3), 342-361. https://doi.org/10.1177/0047281616639472

Jones, N.N., & Williams, M.F. (2020). The just use of imagination: A call to action. *ATTW Blog.* Retrieved from https://attw.org/blog

Jones, N.N., Gonzales, L., & Haas, A.M. (2021). So, you think you're ready to build new social justice initiatives?: Intentional and coalitional pro-Black programmatic and organizational leadership in writing studies. *Writing Program Administration, 44*(3), 29-35.

Kaltenbach, B., & Zielinski, R. (2023). The $17 Billion Slider? Illinois Supreme Court Decides White Castle BIPA Case. *The National Law Review.* https://www.natlawreview.com/article/17-billion-slider-illinois-supreme-court-decides-white-castle-bipa-case

Kearns, M., & Roth, A. (2019). *The ethical algorithm*. Oxford UK and New York: Oxford University Press.

Keshavarz, M. (2018). *The design politics of the passport: Materiality, immobility, and dissent.* London: Bloomsbury.

Koerber, A. (2000). Toward a feminist rhetoric of technology. *Journal of Business and Technical Communication, 14*(1), 58–73. https://doi.org/10.1177/105065190001400103

NV AB161 | 2023 | 82nd Legislature. (2023, February 15). LegiScan. Retrieved March 14, 2023, from https://legiscan.com/NV/bill/AB161/2023

Light, A., & Luckin, R. (2008). Designing for social justice: People, technology, learning. *Futurelab*. Retrieved from https://www.nfer.ac.uk/publications/FUTL53/FUTL53.pdf.

Lupton, D., & Michael, M. (2017). 'Depends on who's got the data': Public understandings of personal digital surveillance. *Surveillance & Society, 15*(2), 254-268. https://doi.org/10.24908/ss.v15i2.6332

Madden, M. (2014, November 12). Public perceptions of privacy and security in the post-snowden era. *Pew Research Center.* https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/

Madden, M., & Rainie, L. (2015, May 20). Americans' attitudes about privacy, security and surveillance. *Pew Research Center.* https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Makaryus, A.N., & Friedman, E.A. (2005). Patient understanding of their treatment plans and diagnosis at discharge. *Mayo Clinic Proceedings, 80,* 991-994.

Matias, J.N. (2023, March 26). To hold tech accountable, look to public health. *Wired*. https://www.wired.com/story/tech-governance-public-health/

Miller, C.R. (1979). A humanistic rationale for technical writing. *College English, 40*(6), 610-617.

Moore, K.R. (2017). The technical communicator as participant, facilitator, and designer in public engagement projects. *Technical Communication, 64*(3), 237–253.

Monahan, T. (2022). *Crisis vision: Race and the cultural production of surveillance.* Duke University Press.

Murray, H. (2007). Monstrous play in negative spaces: Illegible bodies and the cultural construction of biometric technology. *The Communication Review, 10*(4), 347-365. https://doi.org/10.1080/10714420701715415

Noble, S.U. (2018). *Algorithms of Oppression*. New York: New York University Press.

Novotny, M. (2015). reVITALize gynecology: Reimagining apparent feminism's methodology in participatory health intervention projects. *Communication Design Quarterly, 3*(4), 61-74. https://dl.acm.org/doi/pdf/10.1145/2826972.2826978

NVIDIA. (2023). Recommendation System. *NVIDIA Corporation.* https://www.nvidia.com/en-us/glossary/data-science/recommendation-system/#:~:text=A%20recommendation%20system%20is%20an,demographic%20information%2C%20and%20other%20factors

Parvin, N. (2023). Just design: Pasts, presents, and future trajectories of technology. *Just Tech. Social Science Research Council.* https://doi.org/10.35650/JT.3049.d.2023

Popescu, M., & Baruh, L. (2018). Privacy as cultural choice and resistance in the age of the recommender systems. In J. Alexander & J. Rhodes (Eds.). *The Routledge Handbook of Digital Writing and Rhetoric,* (pp. 280-291). Routledge.

Rosenblat, A., Wikelius, K., boyd, d., Gangadharan, S.P., & Yu, C. (2014). Data & civil rights: Health primer. *Data & Society Research Institute.* Retrieved from http://www.datacivilrights.org/pubs/2014-1030/Health.pdf.

Roundtree, A.K. (2019). Exploring public engagement in environmental rhetoric. In D.R. Gruber and L.C. Olman (Eds.), *Routledge Handbook of Language & Science* (pp. 279-294). New York, NY: Routledge. Retrieved from https://www.crcpress.com/The-Routledge-Handbook-of-Language-and-Science/Gruber-Walsh/p/book/ 9780815382683

Rude, C.D. (2009). Mapping the research questions in technical communication. *Journal of Business and Technical Communication, 23*(2), 174-215. https://doi.org/10.1177/1050651908329562

Sackey, D. (2019). One-size-fits-none: A heuristic for proactive value sensitive environmental design. *Technical Communication Quarterly, 29*(1), 33–48. doi:10.1080/10572252.2019.1634767

Schultz, T., Abdulla, D., Ansari, A., Canlı, E., Keshavarz, M., Kiem, M., Prado de O. Martins, L., & J.S. Vieira de Oliveira, P. (2018). What is at stake with decolonizing design? A roundtable. *Design and Culture, 10*(1), 81–101. https://doi.org/10.1080/17547075.2018.1434368.

Scott, J.B. (2003). *Risky rhetoric: aids and the cultural practices of HIV testing*. Southern Illinois University Press.

Segal, J. (2007). Compliance to concordance: A critical view. *Journal of Medical Humanities, 28*(2), 81-96. https://doi.org/10.1007/s10912-007-9030-4.

Seitz, J. (2023, March 30). NYPD is refusing to comply with NYC's new surveillance tech laws. *Daily Dot.* https://www.dailydot.com/debug/nypd-violating-post-act-inspector-general/

Smith, C.F. (2000). Writing public policy: A practicum. *Technical Communication Quarterly, 9*(1), 77–92. https://doi.org/10.1080/10572250009364686

Snorton, C.R. (2017). *Black on both sides: A racial history of trans identity*. Minneapolis: University of Minnesota Press

Spafford, M.M., Schryer, C.F., Mian, M., & Lingard, L. (2006). Look who's talking: Activity mapping in pediatric clerkship case presentations. *Journal of Business and Technical Communication, 20*(2), 121–158.

Stolterman, E. (2001). Creating community in conspiracy with the enemy. In L. Keeble & B. Loader (Eds.), *Community Informatics: Shaping Computer-Mediated Social Relations* (pp. 43-52). London: Routledge.

Sudore, R.L., Mehta, K.M., Simonsick, E.M., Harris, T.B., Newman, A.B., Satterfield, S.,...Yaffe, K. (2006). Limited literacy in older people and disparities in health and healthcare access. *Journal of the American Geriatrics Society, 54*(5), 770–776. https://doi.org/10.1111/j.1532-5415.2006.00691.x

Sun, H. (2012). *Cross-cultural technology design: Creating culture-sensitive technology for local users.* Oxford: Oxford University Press.

Teston, C., Gonzales, L., Bivens, K.M., & Whitney, K. (2019). Surveying precarious publics. *Rhetoric of Health & Medicine, 2*(3), 321-51. https://doi.org/10.5744/rhm.2019.1015

Toulas, B. (2023, February 10). California medical group data breach impacts 3.3 million patients. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/california-medical-group-data-breach-impacts-33-million-patients/

Turow, J., Hennessy, M., & Draper, N. (2016). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2820060

Turow, J. (2021). *The voice catchers.* New Haven: Yale University Press.

Turow, J., Lelkes, Y., Draper, N., & Waldman, A.E. (2023, February). Americans can't consent to companies' use of their data. *Annenberg School for Communication, University of Pennsylvania.* https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf

Véliz, C. (2022). The surveillance delusion. In C. Véliz (Ed.), *The Oxford Handbook of Digital Ethics*. https://doi.org/10.1093/oxfordhb/9780198857815.013.30.

Veridium. (2019, February 6). Biometric authentication hits primetime in Super Bowl ads. https://veridiumid.com/biometric-authentication-super-bowl-ads/

Waisman, Y., Siegal, N., & Chemo, M. (2003). Do parents understand emergency department discharge instructions? A survey analysis. *Israel Medical Association Journal, 5*(8), 567-70.

Wajcman, J. (1991). *Feminism confronts technology.* University Park: Pennsylvania State University Press.

Walton, R., Moore, K., & Jones, N. (2019). *Technical communication after the social justice turn: Building coalitions for action*. Routledge.

Washington Public Affairs Network. (2023, April 5). Senate floor debate. https://www.tvw.org/watch/?clientID=9375922947&eventID=2023041079

Wilkerson, J. (2023, February 7). Senators launch inquiry into telehealth companies for tracking and monetizing personal data. *The Markup*. https://themarkup.org/pixel-hunt/2023/02/07/senators-launch-inquiry-into-telehealth-companies-for-tracking-and-monetizing-personal-data.

Williams, M.F. (2022). Gun control and gun rights: A conceptual framework for analyzing public policy issues in technical and professional communication. *Technical Communication Quarterly, 31*(1), 33-43, https://doi.org/10.1080/10572252.2021.1963487.

Yahoo! (2014). Advertising, the balancing act: Getting personalization right. Retrieved from https://advertising.yahoo.com/Insights/BALANCING-ACT.html.

Young, S. (2023). *Working through surveillance and technical communication: Concepts and connections.* SUNY Press.

Zucco, E. (2023, April 6). Bill to strengthen privacy of health data passes state House, Senate. *King TV*. https://www.king5.com/article/news/politics/state-politics/bill-strengthen-privacy-health-data/281-527855ee-640a-4e80-b655-6f89c977fdc0

Chapter 6

Pedagogical and Programmatic Implementation[91]

The previous Chapter (5) focuses on how neonatal nurses, as technical communicators, can (and do) have a role in the design of communication materials, particularly with patient choice in opting in/out of biometric technology usage. The Chapter documents several takeaways for technical communicators to consider such as coalitional work, questioning and revising normalized surveillance including ethics and design of biometric use, and further localization of community input with impacts to privacy and design including opting out procedures.

This Chapter (6) applies themes of security, efficiency, and compliance to programmatic application in the technical communication classroom through examining how a technical communication course may benefit from exploration of surveillance technologies in healthcare (and other sites of surveillance). As healthcare (and many other industries) become increasingly reliant on digital technologies, it is imperative for faculty (and students) to explore the ways pervasive technologies impact our agency, privacy, communication practices, and personal/professional lives and careers. This chapter builds off the previous by providing insights into the programmatic and pedagogical impacts of my dissertation study and its exigency in technical communication classes/programs.

6.1 Problem Statement: Why Introduce Biometrics to TPC

The information collected from this study may be bridged to another site of surveillance: the college classroom. It is important to note that many parts of this chapter are pulled from previous chapter sections written for the dissertation: the literature and takeaways (Chapter 2 and

[91] As a condition of the grant received to pay nurses from the Council for Programs in Technical and Scientific Communication, this chapter focuses on programmatic and pedagogical impacts from the study. This chapter will be revised for publication in *Programmatic Perspectives*.

5), for example, inform how a TPC course "might" operate. I propose that upper-level Technical and Professional Communication courses across institutions would benefit from critically analyzing and studying biometric technologies as influential and integral to defining the role of technical communicators (and subsequently, the field of technical communication broadly construed). As Gilson (2021) explains, many students will enter professions that help shape who is able to "access, use, enjoy, contribute to, and interact with online material" (p. 179). These same students view technologies as neutral and unbiased, which is why curriculum should be developed as a "site for action and an area for enacting theory; it is a nurturing ground for critical, functional, and socially just technical communication" (Agboka & Dorpenyo, 2022, p. 60). Technical communication programs and curricula must be sites for engaging social justice issues and enabling students to critique and address systemic inequalities and disadvantages. The following outlines how surveillance studies may intersect with technical communication and social justice in the classroom, with the goal "to address issues of power and agency as they manifest in communicative practices and texts" (Jones, 2016, p. 343). This chapter adds to understandings of how instructors may expose students to "everyday issues of injustice that affect students or in which technical communication might play a role" (Agboka & Dorpenyo, 2022, p. 62). Further, social justice approaches to TPC are "practical and applied" not merely "theoretical or ideological stances," thus critically *analyzing* and creating *action* plans to address emerging technologies is a crucial component of the technical communication class and curriculum (Walton & Agboka, 2021). To reiterate, this study focuses on biometric technology usage and perceptions in healthcare. This topic and focus, however, has implications for surveillance sites for future study especially for addressing ethical concerns. Biometric

surveillance is not just enacted as routine surveillance, but also within other systems, contexts, and institutions including higher education.

Our role as technical communicators who function as knowledge-makers, creators, and instructors is to communicate with audiences regarding how surveillance impacts their daily lives. Since technical communicators are advocates (Jones, 2016; Walton, Moore, & Jones, 2019), then advocating for historically marginalized and multiply marginalized individuals and groups becomes an important part of a technical communicator's teaching. Surveillance is a key writing and thinking activity that impacts our day-to-day lives in a multitude of ways; this study translates across disciplines and institutions in its impact within the classroom space, especially if used as a case study. We should discuss with students how and why bodies are impacted by surveillance technologies. Programmatic and pedagogical impacts of surveillance activities include interdisciplinary texts, activities, and assignments that intersect with scientific writing and health and medicine.

As media scholars danah boyd and Kate Crawford have noted, "Data sets that were once obscure and difficult to manage–and, thus, only of interest to social scientists–are now being aggregated and made easily accessible to anyone who is curious, regardless of their training" (2012, p. 664). Licastro and Miller (2021) argue that "What's 'big' about big data, then, is not the information itself, but the number of people able to access and interrogate that data" (p. 4). Licastro and Miller (2021) discuss the ways that institutions and writing programs are increasingly using repositories for student data (amongst other data points); however, this may be applied to other structural institutions such as the government or corporations utilizing biometric identification. These institutions, corporations, and governing bodies lack transparency in the process of opting into participation in these systems, which further contributes to ethical

concerns about privacy and security. Such topics are apt for consideration when designing technical communication courses, especially since students are stakeholders in these systems (particularly in their future careers) and inform decision-making processes such as the ability to opt out.

For example, in higher education, the classroom is a place where instructors and technical communicators may analyze the way efficiency is monitored by biometrics. Efficiency and biometrics are most often seen in the classroom space with third-party applications, where instructors (and eventually employers) view speed and time as a measure of success. Measures of success, as often determined by "efficiency," manifest through monitoring in Learning Management Systems, or workforce software such as Kronos. They also manifest through remote proctoring such as Respondus and Proctorio, and other third-party software that's introduced within the institution. This monitoring is behavioral regulation or disciplinary power in action (Foucault, 1995). This monitoring, as it relates to the collection of biometrics, is also highly problematic (as briefly mentioned in section 6.2).

Furthermore, introducing students to issues of surveillance within technical and professional communication creates an opportunity to reflect, analyze, and interrogate students' digital literacies. Our identities are inextricably linked and tied to the digital age; digital spaces provide for world-making (Muñoz, 2009). Digital literacy is broadly defined as an individual's ability to search, find, evaluate, and compose clear information through typing, writing, tapping, and by using other mediums (i.e., multimedia videos, video calling, and messaging) on various digital platforms, which requires a basic level of computer competency (Bawden, 2008). Digital literacy is important to discuss since our bodies transcend physical boundaries through virtual existences. However, digital spaces can be at times fraught, confusing, or difficult to navigate.

These spaces can also be unsafe. As Beck et al., (2021) notes, digital literacy initiatives "foster navigation, examination, searching, composing, remixing, coding, designing, sharing, contributing, and protecting—or the skills needed to enable communication online" (p. 6). Understanding privacy and surveillance is a form of digital literacy. I view digital literacy as interlocking with data literacy. Laurie Gries (2017) defines data literacy as the "ability to gather, evaluate, visualize, draw conclusions from, and communicate data to form new knowledge." Privacy and surveillance as they relate to digital literacy are relevant across disciplines. While some of us might be directly affected, others may simply want to know what measures they *can* take to protect their communications and data from spying. Defining privacy has proven quite difficult as so many interactions have transitioned online (OHRP, 2013). For example, instructors working in educational settings rely on Family Educational Rights and Privacy Act (FERPA) to guide their interactions with students and the definition of privacy defined by the Human Subject Institutional Review Board (IRB) for their research. Conversely, people working in the medical and healthcare industry follow guidelines of the Healthcare Insurance Portability and Accountability Act (HIPAA). These variations in how people understand privacy represent one aspect of understanding digital literacy. I adopt the definition of privacy from Tham and Duin (2021), who define it as having control over the extent, timing, and circumstances of sharing oneself physically, behaviorally, or intellectually with others (Beck & Hutchinson Campos, 2021). Privacy is, however, a limited lens for thinking about surveillance, since it is a right not granted equally to all, a fact that needs to be considered in such investigations especially when talking with students about privacy as digital literacy. Privacy depends on context and is a sweeping concept. A common argument is that students don't care about

privacy. The thing is, they do. When introducing concepts, we must give examples and scenarios that don't just relate to students, but also impact them. What do they care about?

This dissertation study has pedagogical and programmatic implications for technical communication programs across the United States. The chapter includes example materials such as an assignment, reading list(s), and a case example that explores ethical considerations and technology as they manifest in sites of surveillance. In these courses or lessons, whichever instructors decide, students will be able to consider the ways surveillance is integral to many of our foundational structural systems, "ones that breed disenfranchisement, and that continue to be institutionalized" (Dubrofsky & Magnet, 2015, p. 7). Surveillance practices and technologies normalize and maintain whiteness, able-bodiedness, capitalism, and heterosexuality (see hooks, 1994). The study itself has practical application(s) especially as surveillance technologies such as biometrics have increased as a result of the COVID-19 pandemic, which makes it a useful and timely example to translate into technical communication classrooms across the United States.

6.2 In the Classroom

As I summarized in Chapter 1, our goal as educators and users is to empower ourselves and our students to be well-informed citizens. Technical communication administrators (broadly defined) may be interested in introducing topics of surveillance and privacy within technical communication programs especially as such topics relate to everyone through surveillance capitalism, the illusion of security, and our right-to-know (Zuboff, 2019; Reilly, 2021; Kerr, 2009; Youngblood, 2012). There are colonialist implications to the history of the definition of surveillance, and the connotations of surveillance are largely nefarious, complicated by the ways in which surveillance is poised as a "necessity" for "security" and "safety." Public response is often to dismiss issues of surveillance, security, and privacy; however, as writers, professional

and technical communicators, and members of society, it is important to understand how we may become more empowered citizens. One way we may become more empowered is by understanding the impact of surveillance technologies in our lives, in our writing, and in our practices. What is the purpose of implementing such technologies? Who do they protect and harm? What are the ethical implications?

Further, it is crucial to note the ways that, as Dorpenyo (2022) has noted, technical communication about technology has continued to maintain and reproduce "dominant narratives about technology while it obscures and delegitimizes the knowledge of unenfranchised/disenfranchised groups" (p. 292). When we, as instructors and technical communicators, teach about technical communication and social justice, we also need to address the ways in which emerging and past technologies (digital and not) have become complicit in injustice. Students will and should have an opportunity in the classroom to explore how certain groups are hyper-surveilled over others through the linguistic and rhetorical choices we make. In fact, from my study, I found that the ways biometric companies communicate their products to consumers emphasize efficiency, compliance, and safety, without ever accounting for a *person* on the other end of the technology. The neonatal nurses interviewed in my study adopted language based on the communication materials used for training(s) in the healthcare setting, which were very similar to the language on the biometric websites themselves. Similar to what Dorpenyo (2022) found in their analysis of documents, the corpus I collected also encouraged users to constantly engage the specific biometric solution, suggesting task-oriented instructions and language that in this study, would then be communicated to patients. These styles are adopted to enable users "to quickly and efficiently complete the task at hand" (Seigel, 2013, p.

71). Such documents ultimately make a case/argument for why it is necessary to adopt the biometric technology: convenience, safety, and/or compliance.

a. Design and Disability Justice as Advocacy for a Socially Just Classroom

Technical communication courses have increasingly incorporated issues of usability and accessibility into the classroom space. Despite this increasing incorporation, Rose (2016) expresses that it is crucial to focus on the needs of vulnerable populations; without such focus, designers are "in danger of creating technologies that reinforce existing inequities" (p. 442). We cannot talk about usability and accessibility, however, without discussing disability justice. Disability justice honors the "longstanding legacies of resilience and resistance which are the inheritance of all of us whose bodies or minds will not conform" and questions "how do we move together as people with mixed abilities, multiracial, multi-gendered, mixed class, across the orientation spectrum—where no body/mind is left behind" (Berne et al., 2018). As my study has displayed, emerging technologies such as biometrics have been used to hyper-surveil and harm historically excluded groups, especially those who are Black, LGBTQIA+, and disabled. Further, Rose (2016) contributes to how technical communicators engage in socially just design through examining the design of information and communication technologies and how they impact vulnerable populations. Berne et al., (2018) document ten principles of disability justice that I believe are a foundational starting point to social justice approaches in the technical communication classroom. Similarly, to my methodological framework of interlocking surveillance, Berne et al., (2018) also consider intersectionality to be critical to disability justice, as it is crucial to pay attention to the ways our students (and ourselves) have multiple identities that can be a site of privilege and/or oppression. Rose (2016) writes that, "designers have a responsibility and obligation to account for the ways in which their work can impact people" (p.

432). For example, human-centered design may shift from "user, use, and activity" to "humans being at the center of the design process" (Rose, 2016, p. 432; see also Buchanan, 2001). Other principles that are important to consider in approaching disability justice in the technical communication classroom are social justice elements such as amplification of historically excluded voices, as well as a critique of anti-capitalist politic. Berne et al., (2018) define this principle as an approach to understanding disabled people as whole, and further, a resistance to conforming to a capitalist "normative" level of production. The scholars critique a concept of "labor" as defined by able-bodied supremacy, white supremacy, and gender normativity, which is helpful when constructing a socially just course and curriculum.

Technical communicators have the opportunity to intervene in designing emerging technologies and we can teach this in the classroom through exploring how they are designed and how the design impacts people in need. We can teach students, as future technical communicators and designers, to ask different questions and therefore "bring about different, and more equitable, design solutions" (Rose, 2016, p. 443). Recent scholarship (Colton & Walton, 2015; Browning & Cagle, 2017; Smyser-Fauble, 2018; Hitt, 2018) has situated disability studies as integral to social justice goals, since technical communicators engage with discourse and design that may, unknowingly, marginalize disabled individuals. This extends to my study with biometrics, as well, and can be a point of entry for students interested in exploring emerging technologies and design. For example, Pons and Polak (2008) document how biometrics are used for "associating computer users with their computer behavior, linking employees to their workstation performance, managing user-resource usage and activity, and e-commerce" which are all aspects of students' current and future careers (p. 115). The usage of biometrics in higher education, for example, is a site of surveillance that all students will know and recognize. Pons

and Polak (2008) notes that at universities, where "the students are ultimately customers with a choice, implementations of biometric systems might be met with some level of resistance due to the sensitive nature of identification, storage, and usage of personal data, notwithstanding whether the 'sensitivity' is real or only perceived" (p. 118). Rodgers et al. (2022) argues that the way time is regulated and managed, or what technical communicators refer to as efficiency, within the neoliberal university is ableist. Efficiency, as documented in this study as well, fails to account for the crip temporalities by which disabled peoples live their lives. Rodgers et al. (2022) argue that in higher education, the concept of "crip" and "cripping time" in relation to disabled academics opens up new ways of thinking, doing, and being that are not constrained by normative (clock) time that marginalizes disabled academics.

Though discrimination certainly happens in healthcare, as this study has explored, examples of design discrimination with biometric technologies often occur with disabled students through lack of access and third-party proctoring applications. For example, one study by Butler et al., (2019) explored automatic speech recognition (ASR) programs that generate real-time speech-to-text captions. The article posited that the ASR can be provided as supplemental access technologies for deaf and hard of hearing (DHH) students in higher education classes. The ASR continued to generate errors, yet the authors cited an access issue: accuracy and readability. Tham and Verhulsdonck (2023) discuss the datafication of schools—which involves "a reimagining and reconfiguration of schools as data-based sites of real-time monitoring and measurement" (Williamson, 2015). This datafication includes implementation of biometric technologies, which students are able to critically examine. However, Tham and Verhulsdonck (2023) argue for a data-*informed* approach rather than data-*driven*; that is, a means

to share perspectives about the value of data privacy and ownership juxtaposed against the value of data-driven education in a situated context (Duin & Tham, 2020).

Further, materialist arguments note that the body is constituted along specific lines of race, class, gender, and nation, and that "when racialized, classed, gendered, and nationalized bodies lack 'material freedom' to engage in relations with other bodies, the theoretical affection for 'rhizomatic'" becomes problematic (Erevelles, 2011, p. 28). This occurs in the classroom space through the set normalization that is expected from proctoring companies (and other third-party applications). As disability activist sarah madoka currie writes in her forthcoming dissertation, *the mad manifesto* (2023), there are scholars such as Brier (2021) and Nielson (2021) who advocate for the intentional refusal of proctoring and other surveillance practices in the classrooms, else instructors are named complicit in creating a "burnout as destiny" (Neilson, 2021) structure for the most marginalized students in their classes. As currie writes, these are the students most likely to be identified as "at risk" or "struggling with resilience" in their relationship to online learning. currie's argument for access is one that technical communicators should engage with:

> When we fail to subvert systems that require students to disclose potentially unsafe work environments, work habits or coping mechanisms in their own work-from-home space using LMS analytics and digital proctoring, we consequently make the argument that their work-from-home space is "on campus" through policing it as though we are engaging with them in public space. But that's not public space, and the bodies interacting in that private space are private bodies (p. 98).

However, this study is not about proctoring services: that could be an entirely other dissertation (see sarah madoka currie's excellent work). Such biometric usage, however, should be noted in its applications in the classroom. We should thus follow Price's (2015) concluding thoughts, to teach students (and ourselves) to move with care. What this means is, according to Price (2015), to give "more when one has the ability to do so, and accepting help when that is

needed" as well as care for not "knowing exactly what another's pain feels like," but "respecting each person's pain as real and important" (p. 279). The harm that comes from usage of biometrics may not be understood by *everyone,* but technical communicators should take care to acknowledge and respect that such pain occurs disproportionately. Intervention begins in the classroom, and such harms should be addressed. Care work must be participatory in nature, that is, "developed through the desires and needs of all participants" (Price, 2015, p. 279).

Other than a special topics course, this study would be useful in an upper division writing intensive course and graduate course. What follows is an overview of an example assignment and reading lists, and a case study for a course that centers surveillance and social justice in technical communication. Despite varying backgrounds and interests, students may benefit from learning theories that are central to surveillance. Though this study specifically collects information from neonatal nurses who use biometric technologies in healthcare, and their perceptions, the broader conversation educators and administrators may focus on are exploring sites of surveillance. Further, it is important to explore with students how disability justice intersects with social justice: as Piepzna-Samarasinha (2018) describes, disability justice understands that oppressive forces like ableism, "racism … sexism, and queer- and transphobia" mutually influence and sustain each other (p. 22). The course assignments and practices challenge students to recognize and attend to diverse and interlocking needs, and to view feedback as essential to professional practice.

b Example Course Overview, Assignments, and Case Study

In the course—which can be adapted as needed for an undergraduate or graduate curriculum—we will examine sites of surveillance as they relate to professional and technical writing. Our examination of such sites of surveillance (such as healthcare, the classroom, and

other spaces we commonly occupy) will focus on the ways in which emerging (and past) technologies (digital and not) hyper-surveil bodies, predominantly those who are Black, people of color, Indigenous, disabled, and LGBTQIA+. We will read and respond to topics including (but not limited to), algorithmic bias, disability and AI, data mining, surveillance capitalism, privacy, and more. This course will emphasize critical reading, writing, and listening to scholarly and popular texts that center historically excluded and silenced voices. Assignments will include original research writing; responses to readings, case scenarios, and peer writing; collaborative discussions; and multimodal projects. Students will rhetorically analyze sites of surveillance as they relate to professional and technical writing and their career goals/trajectories, responding to them in socially relevant ways (including various modes/mediums of response, recognition of language other than Standard Written English, and more) for a range of audiences.

Some course/unit/lesson plans guiding questions may explore[92]:

- What is surveillance, and how does it impact technical communicators?
- How, as digital users and technical communicators, does surveillance (and tools, such as biometric technologies, impact professional writing?
- What are the implications of surveillance for historically excluded groups such as those who are marginalized due to race, class, gender, sexuality, and dis/ability?

Some of the ideas for course assignments were adapted from Beck, et al. (2021) who wrote about implementing critical digital literacy with undergraduate students. I highly recommend viewing a more comprehensive look at surveillance and digital literacy in the syllabus that Beck (2021) outlines. For example, it is important to note that what is included in this chapter are merely examples. Instructors can, and should, adapt the examples as they see fit.

[92] This could, and should, be an interdisciplinary course that reflects students' interests.

Instructors should implement readings and assignments that represent students and their positionalities, and interests. The following are some potential learning outcomes adapted from Torin Monahan's (2022) Technology & Social Justice Course syllabus.

Learning Outcomes[93]*:*

Students will…

- Learn how emerging technologies such as biometrics impact groups of *people* within specific sites of surveillance as they relate to students' future career paths and interests.
- Acquire a conceptual toolkit for analyzing issues related to technology, accessibility, and social justice, as they relate to technical and professional communication.
- Gain experience collaborating with other students to investigate the political, social, cultural, and economic impacts of emerging technologies.

The following are some potential readings that instructors may consider implementing in their courses. These readings were adapted from my own comprehensive exam reading list as a graduate student. It is important to note that this list is ***not*** extensive in its documentation of the multitude of scholars who research and teach technical communication and surveillance. This is a short sample reading list that may provide a foundation, and I highly recommend incorporating scholars who engage in work that is both representative of your current student population, while also exposing students to new insights and perspectives. For example, it would be useful to turn to some collected works for inspiration, such as:

- MMU Scholar Bibliography: https://www.itchuaqiyaq.com/mmu-bibliography
- Cox M. B., Faris M. J. (2015). An annotated bibliography of LGBTQ rhetorics. Present Tense: A Journal of Rhetoric in Society, 4(2), 1–161.

[93] (Adapted from Torin Monahan, 2022)

- NCTE CCCC Latinx Caucus Bibliography: https://cruzmedina.com/digital-projects/ncte-cccc-latinx-caucus-bibliography/
- Alternative Texts and Critical Citations for Antiracist Pedagogies: https://docs.google.com/spreadsheets/d/1ONAkDvuzGS4xAnqE0p-5kDseWS-5Hs_BDDwMy-wHUnk/edit#gid=0
- WPA/CompPile Research Bibliographies: https://wac.colostate.edu/comppile/wpa/
- Intersectional Research: http://womenintechcomm.org/resources/intersectional-research/
- Anti-Racist Pedagogy: https://ece.english.uconn.edu/reading-list-anti-racist-pedagogy/
- TPC OER: https://docs.google.com/document/d/1iP1xYbDbXYzx9njc8BTwb8ViZv6sOSOlsG5Ift0vOKM/edit#
- Surveillance Studies: Lyon, David. 2022. Reflections on FortyYears of "Surveillance Studies." Surveillance & Society, 20(4): 353-356. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

The readings will be assigned during thematic weeks, which may include sample topics such as: Power and Legitimacy; Disability and AI; Design and Usability; Healthcare Inequities; Surveilling the Classroom and more.

Assigned Readings[94]*:*

Technical Communication and Social Justice:

Agboka, G.Y. & Dorpenyo, I.K. (2022). The role of technical communicators in confronting injustice—everywhere. *IEEE Transactions on Professional Communication, 65*(1), 5-10. https://doi.org/10.1109/TPC.2021.3133151.

[94] These are solely suggestions and would shift based on the students' interests and goals.

Barnum, C.A., & Huilin, L. (2006). Chinese and American technical communication: A cross-cultural comparison of differences. *Technical Communication, 53,* 143–166.

Bowdon, M. (2004). Technical communication and the role of the public intellectual: A community HIV-prevention case study. *Technical Communication Quarterly, 13*(3), 325-340.

Colton, J. S., & Walton, R. (2015). Disability as insight into social justice pedagogy in technical communication. *Journal of Interactive Technology and Pedagogy, 8.* Retrieved from http://jitp.commons.gc.cuny.edu/disability-as-insight-into-social-justice-pedagogy-in-technical-communication/

Cox, M.B. (2019). Working closets: Mapping queer professional discourses and why technical communication studies need queer rhetorics. *Journal of Business & Technical Communication, 33*(1), 1-25.

Dorpenyo, I. (2019) Risky election, vulnerable technology: Localizing biometric use in elections for the sake of justice. *Technical Communication Quarterly, 28*(4), 361-375. https://doi.org/10.1080/10572252.2019.1610502

Dorpenyo, I.K. (2022). Local knowledge as illiterate rhetoric: An antenarrative approach to enacting socially just technical communication. *Journal of Technical Writing and Communication, 52*(3), 291-315. https://doi.org/10.1177/00472816211030199

Frost, E.A. & Eble, M. (2015). Technical rhetorics: Making specialized persuasion apparent to public audiences. *Present Tense, 4*(2). Retrieved from http://www.presenttensejournal.org/wp-content/uploads/2015/04/FrostandEble.pdf

Gonzales, L., & Turner, H. (2017). Converging fields, expanding outcomes: Technical communication, translation, and design at a non-profit organization. *Technical Communication, 64*(2), 126-140.

Haas, A. (2012). Race, rhetoric, and technology: A case study of decolonial technical communication theory, methodology, and pedagogy. *Journal of Business and Technical Communication, 26*(3), 277-310. https://doi.org/10.1177/1050651912439539

Haas, A.M., & Eble, M. F. (Eds.). (2018). *Key theoretical frameworks: Teaching technical communication in the twenty-first century*. Logan, UT: Utah State University Press.

Jones, N.N. (2016). The technical communicator as advocate: Integrating a social justice approach in technical communication. *Journal of Technical Writing and Communication, 46*(3), 342-361. https://doi.org/10.1177/0047281616639472

Piepzna-Samarasinha, L.L. (2018). *Care work: Dreaming disability justice.* Vancouver, Canada: arsenal pulp press.

Walton, R., Moore, K., & Jones, N. (2019). *Technical communication after the social justice turn: Building coalitions for action.* Routledge.

Surveillance Studies:

Amidon, T.R., Hutchinson, L., Herrington, T., & Reyman, J. (2019). Copyright, content, and control: Student authorship across educational platforms. *Kairos 24*(1). http://kairos.technorhetoric.net/24.1/topoi/amidon-et-al/index.html.

Beck, E., & Hutchinson Campos, L. (Eds). (2021). *Privacy matters: Conversations about surveillance within and beyond the classroom.* Utah State University Press.

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new jim code.* Cambridge, UK; MA: Polity Press.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498-512.

Dubrofsky, R.E. & Magnet, S.A. (2015). *Feminist Surveillance Studies.* Durham and London: Duke University Press.

Eubanks, V. (2011). *Digital dead end: Fighting for social justice in the information age.* MIT Press.

Moore, K.R., Jones, N., Cundiff, B.S., & Heilig, L. (2018). Contested sites of health risks: Using wearable technologies to intervene in racial oppression. *Communication Design Quarterly Review, 5*(4), 52-60.

Noble, S.U. (2018). *Algorithms of Oppression.* New York: New York University Press.

The following are example course assignments that technical communication instructors may adopt and/or implement.

Course Assignments[95]*:*

1. Keyword Report: From the reading list, students will select one concept or keyword to further explore. The report must: 1) succinctly define the concept, 2) offer an example of how it could be applied, 3) state how it relates to the course focus on technology, accessibility, and social justice, 4) provide a full citation, and 5) include a multimodal component (an audio description, visual, etc.).

[95] Course Assignments 1 and 3 have been adapted from Torin Monahan, 2022.

2. Case Studies: Case studies are similar to discussion boards. Each week, students will either have a discussion board or a case study to respond to. Case studies will explore a specific instance of surveillance and/or privacy concerns in the technical/professional workplace. Students will be responsible for utilizing assigned readings, alongside with outside research, to determine the best course of action given the scenario. This project will allow students to identify problems, audiences, and appropriate genres to write in to respond to a case.
3. Technology Justice Project: The final project will be a team-based research project, presentation, **and** reflection. Students will be asked to select a specific social justice concern with technology, formulate research questions, decide upon appropriate research methods to answer your questions, analyze collected data, and compose an accessible final deliverable (i.e., professional report, website, documentary video, podcast, community resources). Sample areas of inquiry might include labor automation/workplace surveillance, institutional surveillance (CCTV, etc.), algorithmic bias, healthcare inequities, (in)accessible spaces, borders and barriers (airport security, etc.), or other topics that appeal to you.

c Case Study Example[96]

My case study example contributes to the social justice implications of how different communities are surveilled. With the social justice turn in technical communication, students (regardless of major) should center social justice in their approaches to teaching, work, and being in the world. Social justice research in technical communication investigates how

[96] This Case Example has been piloted successfully in an undergraduate upper division writing intensive course called, Writing for Business and Industry.

"communication broadly defined can amplify the agency of oppressed people—those who are materially, socially, politically, and/or economically under-resourced" (Jones, 2016, p. 347). It is important to introduce students to feminist and social justice methodologies as approaches to reorienting their lens of how surveillance (and biometric technologies) pervades their lives and future careers; though surveillance is not solely understood as digital, many of the technologies that put bodies on visual display is not new and is rather associated with longstanding forms of oppression.

From implementing biometric technologies as a case study example of workplace surveillance, students will be able to demonstrate how surveillance is an embodied process, and how they may advocate for individual/user awareness. Because, as Ornatowski (1992) writes, technical writing is always rhetorical, the case example will also consider questions of ethics and responsibility. To further display the relationship between efficiency and surveillance in the workplace, I implemented a case study within an undergraduate course in the United States. This classroom activity is transferable across courses in higher education and institutions. I foresee its usage in a Technical Communication related course; for the purposes of my activity, this was piloted as a teaching case in a Writing for Business and Industry class.

The objective of the teaching case was to introduce undergraduate students to key surveillance terminology through exploring enactment of power in the workplace. Taylorism, first developed by Frederick Taylor whose goal was to obtain the most efficient practices in the workforce, may be defined as "the science of dividing specific tasks to allow employees to complete assignments as efficiently as possible" (Wheeler, 2019). Taylor used scientific methods to assign workers to tasks they performed best (Gilliom & Monahan, 2013 as cited in Wheeler, 2019). According to Lanz (2013), "Division of labor has been an important source of

productivity gains since the first human beings engaged in hunting and gathering" (p. 194). Through this activity, emphasis was placed (and may be placed) on the ways employers observe workers with the intended goal (at least Taylor's intended goal) to make sure employees are not wasting company time. Instructors may utilize this activity to spark conversation with students about engaging in digital activism by alerting their peers of how they may be surveilled in the workplace, and also holding employers accountable for how they enact monitoring practices. Surveillance techniques like Taylorism are used in corporations to observe workers and make sure employees are not wasting company time by "slacking in their tasks" (Wheeler, 2019). Ideally, companies believe that by measuring the efficiency levels of each employee, they can achieve the optimal success rate.

One implication of defining surveillance as the "application of power over the observed audience" may be viewed through what Andrejevic refers to as "mass culture," which, "like the mass market that produces it, has long been criticized for being top down, homogeneous, and non-participatory" (2007, p. 28). As I have written previously (Banville & Sugg, 2021), speaking broadly, the basic tenet of Panopticism is the power of control–control over norms–wherever they may be found. This provides those with power–actual and assumed–to manipulate non-conformity into the authority figures' idea of conformity, thus normalizing the function of surveillance. Employees who surveil can negatively affect trusting relationships between employers and employees. Additionally, surveillance in the work environment places emphasis on achieving success and often puts success over care (Wheeler, 2019).

It is important to note that efficiency as a theme was only one of three major thematic takeaways from this study (with issues of safety/security and compliance as the other themes). Further, the reading lists, assignments, and case examples are generalized to focus on

surveillance broadly discussed and may be revised as instructors see fit. This case example seeks to bring awareness to citizens of how society has been slowly turning into a hyper-suspicious assemblage based on the assumed necessity of safety and security, often introduced by state powers through times of trauma or fear.

For example, in my specific college undergraduate course, students are seated at tables of five groups of five students (adapt as necessary). Though this may be transferable into an online or digital setting, this activity was only piloted in-person as a teaching case. The classroom activity emulates aspects of the Stanford Prison Experiment by creating roles for students to play (employees, employers, managers, etc.) to analyze the ways power shifts and surveillance is enacted in the workplace. Each table of five students, and subsequently each person seated at the table, was assigned a specific role: employer, manager, employee, timekeeper, and observer. Based on their assigned roles, students were responsible to finish a group task on paper, and then mimic the task in an online platform. The measure of success will be time, to initiate a conversation about what efficiency means in surveillant contexts.

The Case

Since each student was assigned a role, they each had to brainstorm what that particular role may look like. What would the role consist of what would the person say, what is their responsibility, and so forth? To enact such a case within a short class period (50 minutes), the Writing for Business and Industry course engaged in a realistic case example. The prompt for the case asked each group to envision that they were their respective roles in a local company/organization. That is, any organization of their choosing, there is an employer, manager, employee, timekeeper, and observer. The organization is contracted to solve community-based problems; one problem in particular noted a breach of client information.

The five students in each group must respond to the problem in their respective roles:

> There is an internal incident where an employee was meeting with a client using Microsoft Teams. The employee did not realize that any messages sent within the chat feature would be viewed by other employees within the company who had access to the channel. It is important that the organization maintains a positive relationship with all clients. Part of this relationship is oftentimes guaranteeing a level of anonymity, as well as confidentiality for client projects and conversations. The company recognizes a need for outlining and communicating best practices for privacy for clients, as well as determining potential risks, consequences, and ethical implications. Your suggested best practices will be read and utilized as internal company policy addressing digital privacy; however, it will also have external application with current and potential clients.

Surveillance and privacy occur within the workplace in different ways - both apparent, and often invisible ways. This case is intended for students to explore best practices of communicating the impacts of surveillance and privacy within the professional workplace. This case also demonstrates how instructors and students may add another layer of how technical communicators may understand biometrics: that is, the information collected such as driver's licenses and passports (among other documents), *are* personal identifiers of the body and *can* be distributed. For example, students may consider what efficiency means to the company, what is considered best performance/practice and by whom, how privacy and surveillance is implemented in today's workforce, and how companies are defining personal information and biometrics?

This case also gives students an opportunity to engage in their own research, exploring questions in their respective roles about privacy leaks: What data is at risk? Who is most at harm? What management plan is in place, and how will clients know that you are in control of the situation? What are best practices for maximum efficiency?

Topics for Discussion

This particular classroom case example could lead to a wide range of topics about surveillance and the workplace. In an informal setting, students in an undergraduate Writing for

Business and Industry course that I taught discussed themes such as power, privacy, efficiency, and different types of surveillance.

In the assemblage process, groups which were previously exempt from routine surveillance are now increasingly being monitored (Haggerty & Ericson, 2000). Though written over two decades ago, Haggerty and Ericson's discussion of privacy remains relevant to current day: "privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation" (2000, p. 616). They compare the space of negotiating privacy to the emergence of the wage economy; in this way, there was an exigence for the fixing of monetary prices to labor, power, citizens and economists.

Due to recent shifts in surveillance technologies, scholars and instructors in technical communication must call attention to and explore technological ethics including describing how data and information are collected, who has a right to privacy and why, and communication exchanges between employer/employee and the public. Instructors may also elect to focus on a specific site of surveillance; for example, my dissertation study focused on healthcare as a site of surveillance. Students in a Scientific Writing course, for example, might consider how biometrics as a form of surveillance are implemented in their careers (or future careers). How are biometrics used, perceived, and communicated? How do they (students) view their responsibility (both personal and professional) and role(s)?

6.3 Surveillance Pedagogy: Across TPC Programs

It is important to center feminist and social justice methodologies as approaches to reorienting the lens of how surveillance pervades our lives; though surveillance is not solely understood as digital, many of the technologies that put bodies on visual display are not new and are rather associated with longstanding forms of oppression. As Agboka and Dorpenyo (2022)

note, the social justice turn in technical and professional communication (TPC) has inspired much discussion about programmatic and curricular efforts. At the core of both feminist and social justice methodologies are principles such as access, equity, rights, and participation, all of which facilitate inclusivity, collaboration, diversity, and justice.

Modern-day surveillance, as well as historical implications of surveillance, have much to do with seeing and being seen. Who is visible and who is invisible. Based in feminist methodologies, it may be determined that since white heteropatriarchal societies such as the United States have centered a male-dominated viewpoint, this shapes not only the top-down or lateral surveillance and control of "other" bodies, but also the history behind every form of data collection. Because surveillance is locally contextualized, and oftentimes sweeping generalizations are made culturally dependent, class discussions about specific sites of surveillance may make visible the invisible.

As I've argued before (Banville & Sugg, 2021), part of recognizing roles comes from understanding/unpacking actions that are interpreted as privileged. As both instructors and professionals, Rehling argues that professional communication programs prepare students for careers as "writers, editors, document designers, presentation developers, and information managers in technology industries, other businesses, government, and nonprofit organizations" (Kynell-Hunt & Savage, 2004, p. 89). Due to the wide range of careers that students and we are involved in, issues of surveillance must be explored in the classroom space to show how surveillance is not "universally and uniformly applied to all human bodies and, furthermore, monitoring occurs with different degrees of specificity and intention" (Dubrofsky & Magnet, 2015, p. 59). Technical communicators are in unique positions to analyze and inform audiences of the varying degrees that surveillance is applied to bodies, especially within the professional

workplace. It is of course important to recognize that social justice pedagogy is constantly in flux, “responding to and adjusting for the space, place, and time in which it is occurring and the bodies with whom it is engaging” (Gilson, 2021, p. 189).

The way biometric companies discuss efficiency, compliance, and security, as well as how they define biometric identification, and the respective technology is relevant as a practice of digital literacy in the technical communication classroom. For example, security firm BioCatch provides tools for companies to “learn employees’ digital behavior and identify when an unauthorized person is trying to access information” (Larson, 2018). Companies can add BioCatch software to apps and websites. It runs in the background to build a ‘behavior profile’ of a user, and “learns activities like how someone holds the phone, whether they type with one or two hands, and how they scroll or toggle between screens” (Larson, 2018). Administrators in technical communication can utilize biometric technologies as a relevant case study in understanding sites of surveillance. The focus in the curriculum might center how the biometric company positions themselves and their product, as well as furthering the role of a technical communicator in this exchange.

To summarize, this chapter helps to outline potential course objectives, assignments, and a case study to guide students in exploring how surveillance impacts their daily lives. Biometric technologies are one aspect of surveillance that impacts our (as instructors, and students) everyday lives. We should discuss with students how and why bodies are impacted by surveillance technologies, especially because technical communicators are, “uniquely poised to function as public intellectuals” (Bowdon, 2004, p. 325). The goals of such implementation are to enact change through intervening in decision-making protocols to advocate and create awareness and transparency.

6.4 Chapter Summary

It is imperative for faculty (and students) to explore the ways pervasive technologies impact our agency, privacy, communication practices, and personal/professional lives and careers. Topics of digital literacy, including privacy and surveillance, are relevant and applicable to all courses. The pedagogical and programmatic impact of this dissertation study guides technical communicators in implementing concepts, ideas, and themes (such as privacy, surveillance, efficiency, security, and compliance) into the technical communication classroom. This study has implications for exploring digital literacy and ethical implications of emerging technologies.

In this chapter, I build a case for incorporating surveillance studies into an upper-level business and/or technical and professional communication class. Surveillance technologies such as biometrics are a topic every college graduate should be aware of (as should instructors!). Universities should be implementing issues surrounding surveillance as a core learning outcome. This is contextual depending on the school; however, this course (or outcomes) could be added to First-Year Composition to introduce students to surveillance or embedded in writing courses across the disciplines. After all, surveillance manifests in our everyday life, for *everyone.* This conversation, though situated within the context of higher education courses, can surely extend into secondary education spaces, as well as through workshops for instructors and training materials for technical communicators[97] (as I define them).

[97] Those who communicate and negotiate specialized information (like neonatal nurses).

REFERENCES

Agboka, G.Y., & Dorpenyo, I.K. (2022). Curricular efforts in technical communication after the social justice turn. *Journal of Business and Technical Communication, 36*(1), 38-70.

Bawden, D. (2008). Origins and concepts of digital literacy. In C. Lankshear & M. Knobel, *Digital literacies: Concepts, policies and practices Vol. 30,* (pp. 17–32).

Beck, E., Goin, M., Ho, A., Parks, A., & Rowe, S. (2021). Critical digital literacy as method for teaching tactics of response to online surveillance and privacy erosion. *Computers and Composition, 61.* https://doi.org/10.1016/j.compcom.2021.102654

Beck, E., & Hutchinson Campos, L. (Eds). (2021). *Privacy matters: Conversations about surveillance within and beyond the classroom*. Utah State University Press.

Bennett, K.C. (2022). Prioritizing access as a social justice concern: Advocating for ableism studies and disability justice in technical and professional communication. *IEEE Transactions on Professional Communication, 65*(1), 226-240. https://doi.org/10.1109/TPC.2022.3140570

Berne, P., Morales, A.L., Langstaff, D., & Invalid, S. (2018). Ten principles of disability justice. *Women's Studies Quarterly, 46*(1), 227-230. https://doi.org/10.1353/wsq.2018.0003.

Bowdon, M. (2004). Technical communication and the role of the public intellectual: A community HIV-prevention case study. *Technical Communication Quarterly, 13*(3), 325-340

Brier, E. (2021). Pandemic pedagogy: Practical and empathetic teaching practices. *Spectra, 8*(2), 31-37. http://doi.org/10.21061/spectra.v8i2.180.

Browning, E.R., & Cagle, L.E. (2017). Teaching a 'critical accessibility case study': Developing disability studies curricula for the technical communication classroom. *Journal of Technical Writing and Communication, 47*(4), 440–463, https://doi.org/10.1177/0047281616646750

Buchanan, R. (2001). Human dignity and human rights: Thoughts on the principles of human-centered design. *Design Issues, 17*(3), 35–39.

Butler, J., Trager, B., & Behm, B. (2019). Exploration of automatic speech recognition for deaf and hard of hearing students in higher education Classes. *In Proceedings of the 21st International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '19).* Association for Computing Machinery, New York, NY, USA, 32-42. https://doi.org/10.1145/3308561.3353772

Casper, M., & Moore, L.J. (2009). *Missing bodies: The politics of visibility.* New York: New York University Press.

Colton, J.S., & Walton, R. (2015). Disability as insight into social justice pedagogy in technical communication. *Journal of Interactive Technology and Pedagogy, 8*. Retrieved from

https://jitp.commons.gc.cuny.edu/disability-as-insight-into-social-justice-pedagogy-in-technical-communication/

currie, s.m. (2023). *the mad manifesto*. Dissertation forthcoming. University of Waterloo.

Dorpenyo, I.K. (2022). Local knowledge as illiterate rhetoric: An antenarrative approach to enacting socially just technical communication. *Journal of Technical Writing and Communication, 52*(3), 291-315. https://doi.org/10.1177/00472816211030199

Dubrofsky, R.E. and Magnet, S.A. (2015). *Feminist Surveillance Studies*. Durham and London: Duke University Press.

Duin, A.H., & Tham, J. (2020). The current state of analytics: Implications for learning management system (LMS) use in writing pedagogy. *Computers and Composition, 55.* https://bit.ly/3bY5Ctk

Erevelles, N. (2011). *Disability and difference in global contexts: Enabling a transformative body politic.* New York: Palgrave.

Gilson, O.A. (2021). An intersectional feminist rhetorical pedagogy in the technical communication classroom. In R. Walton & G.Y. Agboka (Eds.), Equipping technical communicators for social justice work: Theories, methodologies, and pedagogies (pp. 178-194). University Press of Colorado. http://www.jstor.org/stable/j.ctv1mjqtfr.13

Gilster, P. (1997). *Digital Literacy*. New York, NY: John Wiley & Sons, Inc.

Gries, L. (2017). Mapping obama hope: A data visualization project for visual rhetorics. *Kairos: A Journal of Rhetoric, Technology, and Pedagogy, 21*(2). http://kairos.technorhetoric.net/21.2/topoi/gries/index.html

Hitt, A. (2018). Foregrounding accessibility through (inclusive) universal design in professional communication curricula. *Business and Professional Communication Quarterly, 81*(1), 52-65. https://doi.org/10.1177/2329490617739884.

hooks, b. (1994). *Teaching to transgress: Education as the practice of freedom*. New York: Routledge.

Jiwani, Y. (2015). Violating in/visibilities, honor killings and interlocking surveillance(s). In R.E. Dubrofsky & S.A. Magnet (Eds.), *Feminist Surveillance Studies*, (pp. 79-93). Durham and London: Duke University Press.

Jones, N.N. (2016). The technical communicator as advocate: Integrating a social justice approach in technical communication. *Journal of Technical Writing and Communication, 46*(3), 342-361. https://doi.org/10.1177/0047281616639472

Kerr, I., Lucock, C., & Steeves, V. (2009). *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. Oxford: Oxford University Press.

Kynell-Hunt, T., & Savage, G. (2004). *Power and legitimacy in technical communication: The historical and contemporary struggle for professional status*. Routledge.

Larson, S. (2018, March 18). Beyond passwords: Companies use fingerprints and digital behavior to ID employees. *CNN Business*. https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html

Munoz, J.E. (2009). C*ruising utopia: The then and there of queer futurity (sexual cultures, 13)*. NYU Press.

Neilson, S. (2021). The problem with "burnout": Neoliberalization, biomedicine, and other soul mates. *The Routledge Companion to Health Humanities*, 1st edition. Retrieved from https://www.taylorfrancis.com/chapters/edit/10.4324/9780429469060-22/problem-burnout-shane-neilson.

Office of Human Research Protections (OHRP). (2013). *Human Subject Institutional Review Board (IRB) Guidebook.* Rockville, MD: Office of Human Research Protections.

Ornatowski, C.M. (1992). Between efficiency and politics: Rhetoric and ethics in technical writing. *Technical Communication Quarterly, 1*(1), 91-103.

Piepzna-Samarasinha, L. L. (2018). *Care work: Dreaming disability justice.* Vancouver, Canada: arsenal pulp press.

Price, M. (2015). The bodymind problem and the possibilities of pain. *Hypatia, 30*(1), 268-284. https://doi.org/10.1111/hypa.12127

Pons, A.P., & Polak, P. (2008). Understanding user perspectives on biometric technology. *Commun. ACM, 51*(9), 115-118. https://doi.org/10.1145/1378727.1389971

Reilly, C. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition, 61*. https://doi.org/10.1016/j.compcom.2021.102652

Rodgers, J., Thorneycroft, R., Cook, P.S., Humphrys, E., Asquith, N.L., Yaghi, S.A., & Foulstone, A. (2022). Ableism in higher education: the negation of crip temporalities within the neoliberal academy. *Higher Education Research & Development*, 1-14. https://doi.org/10.1080/07294360.2022.2138277

Rose, E.J. (2016). Design as advocacy: Using a human-centered approach to investigate the needs of vulnerable populations. *Journal of Technical Writing and Communication, 46*(4), 427-445. https://doi.org/10.1177/0047281616653494

Seigel, M. (2013). *The rhetoric of pregnancy*. University of Chicago Press.

Selfe, C.L. (1999). *Technology and literacy in the 21st century: The importance of paying attention.* SIU Press.

Smyser-Fauble, B. (2018). The university required accommodations statement: What 'Accommodation' teaches technical communication students and educators. In A.M. Haas & M.F. Eble (Eds.), *Key theoretical frameworks: Teaching technical communication in the twenty-first century* (pp. 212-240). University of Colorado Press.

Spilka, R. (2010). *Digital literacy for technical communication: 21st century theory and practice*. New York: Routledge.

Tham, J.C.K., & Verhulsdonck, G. (2023). Smart education in smart cities: Layered implications for networked and ubiquitous learning. *In IEEE Transactions on Technology and Society*. https://doi.org/10.1109/TTS.2023.3239586.

Tsai, P. (2018, March 12). Data Snapshot: Biometrics in the workplace commonplace, but are they secure? *Spiceworks.* https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure

Walton, R., Moore, K., & Jones, N. (2019). *Technical communication after the social justice turn: Building coalitions for action.* Routledge.

Walton, R., & Agboka, G. (2021). *Equipping technical communicators for social justice work: Theories, methodologies, and pedagogies.* Utah State University Press.

Williamson, B. (2015). Educating the smart city: Schooling smart citizens through computational urbanism. *Big Data & Society, 2*(2), 1-13.

Youngblood, S.A. (2012). Balancing the rhetorical tension between right-to-know and security in risk communication: Ambiguity and avoidance. *Journal of Business and Technical Communication, 26*(1), 33-62.

Zuboff, S. (2019). *Age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

APPENDIX A: IRB APPROVAL LETTER

EAST CAROLINA UNIVERSITY
University & Medical Center Institutional Review Board
4N-64 Brody Medical Sciences Building· Mail Stop 682
600 Moye Boulevard · Greenville, NC 27834
Office **252-744-2914** · Fax **252-744-2284** ·
rede.ecu.edu/umcirb/

Notification of Exempt Certification

From: Social/Behavioral IRB
To: Morgan Banville
CC: Nicole Caswell
Date: 7/25/2022
Re: UMCIRB 22-000647
Am I who I say I am? The Illusion of Choice: Biometric Identification in Healthcare

I am pleased to inform you that your research submission has been certified as exempt on 7/25/2022. This study is eligible for Exempt Certification under category # 2b.

It is your responsibility to ensure that this research is conducted in the manner reported in your application and/or protocol, as well as being consistent with the ethical principles of the Belmont Report and your profession.

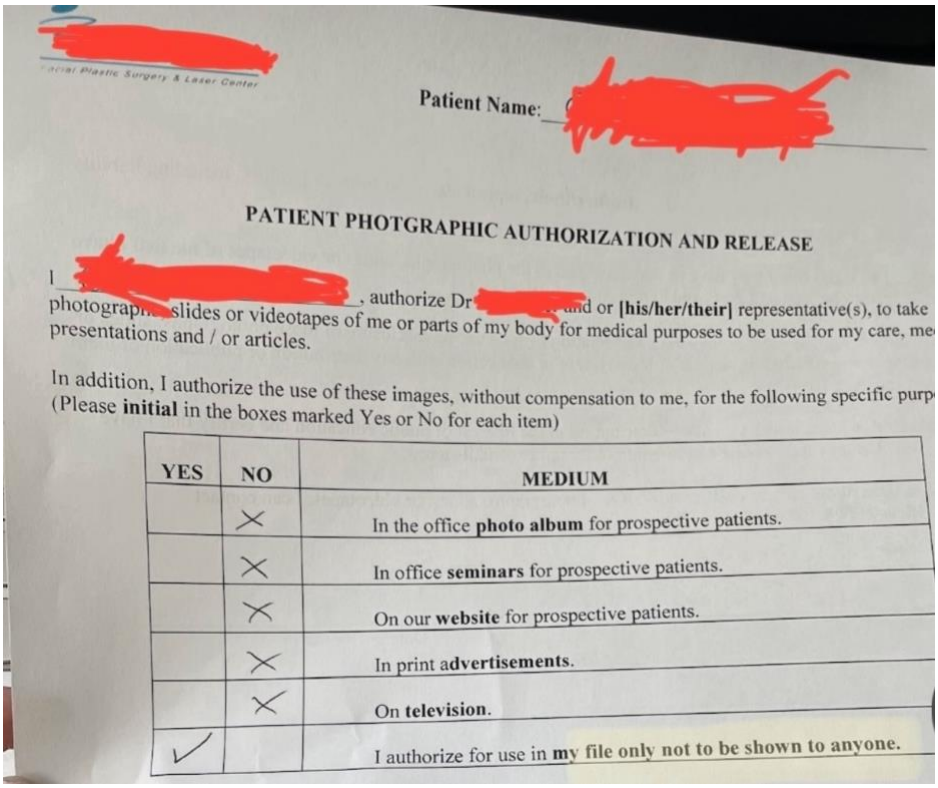
This research study does not require any additional interaction with the UMCIRB unless there are proposed changes to this study. Any change, prior to implementing that change, must be submitted to the UMCIRB for review and approval. The UMCIRB will determine if the change impacts the eligibility of the research for exempt status. If more substantive review is required, you will be notified within five business days.

Document	Description
Consent Paragraph(0.04)	Consent Forms
Proposal(0.01)	Study Protocol or Grant Application
Questions(0.01)	Interview/Focus Group Scripts/Questions
Recruitment(0.02)	Recruitment Documents/Scripts
Screening Survey and Interview(0.01)	Surveys and Questionnaires

For research studies where a waiver or alteration of HIPAA Authorization has been approved, the IRB states that each of the waiver criteria in 45 CFR 164.512(i)(1)(i)(A) and (2)(i) through (v) have been met. Additionally, the elements of PHI to be collected as described in items 1 and 2 of the Application for Waiver of Authorization have been determined to be the minimal necessary for the specified research.

The Chairperson (or designee) does not have a potential for conflict of interest on this study.

APPENDIX B: PATIENT CONSENT PHOTO (Edwards, 2022)



[redacted] Facial Plastic Surgery & Laser Center

Patient Name: [redacted]

PATIENT PHOTGRAPHIC AUTHORIZATION AND RELEASE

I [redacted], authorize Dr [redacted] and or **[his/her/their]** representative(s), to take photograph[redacted] slides or videotapes of me or parts of my body for medical purposes to be used for my care, me presentations and / or articles.

In addition, I authorize the use of these images, without compensation to me, for the following specific purp (Please **initial** in the boxes marked Yes or No for each item)

YES	NO	MEDIUM
	X	In the office **photo album** for prospective patients.
	X	In office **seminars** for prospective patients.
	X	On our **website** for prospective patients.
	X	In print a**dvertisements**.
	X	On **television**.
✓		I authorize for use in **my file only not to be shown to anyone.**

Image from Lapine, California-based AI artist (Edwards, 2022)

APPENDIX C: INTERVIEW SCRIPT

The following is the script, questions, and scenarios (two chosen depending on interviewee experience):

In this interview, we will first focus on your professional life as a neonatal nurse, then shift to some questions about your personal life. This part would be about you as a receiver of medical care.

As a nurse:

6. Tell me about your work as a neonatal nurse. Where do you work, how long have you been a nurse, what do you think about the job?
    1. What are some of your duties? How has the job changed over tim*e (extra questions)*
7. As a neonatal nurse, what has your experience been with technologies in healthcare? That is, what type of technology (not just digital) do you use in your day-to-day?
8. How do you view power structures in the healthcare institution:
    1. Between you and a supervisor
    2. Between you and the patient
9. Biometrics are personal identifiers of the body. **In your screening survey response, you mentioned…**
    1. How do biometric technologies and issues of privacy complicate the relationship between you and your supervisor and you and the patients?
10. Think of a time when you were at the (fill in the blank based on screening survey - **hospital, or other healthcare institution**). What is your experience with utilizing technologies to collect personal identifiers from patients? What does this look like/what do the technologies collect? *This is really the major question.*

As a patient:

11. For the purpose of this study, I define biometric technologies as any identifier of the body that is collected and used for personal identification. Based on this definition, have you ever had biometric information [personal information from your body] collected within a healthcare institution? What unique identifier did the institution collect?
12. Thinking back, how did you feel about the personal identification being collected from you?
13. Think of a time when you visited a healthcare office (specify). What was your experience with the biometric technology in the office (was there a facial scanner, etc.)? What were the technologies used for and what did they collect from you?

After the questions, I shifted into scenarios. I chose two out of three of the following scenarios to discuss depending on the questionnaire responses. That is, based on the definitions and chosen examples, I decided whether or not the neonatal nurse had/didn't have experience with biometrics. If they seemed to have a level of informedness about biometric technologies based on my definition, then I skipped the last scenario about wearables.

In the next part of the interview, we're going to talk through some scenarios which will be followed by a few questions. The first scenario is about newborn fingerprinting.

First scenario: (link to article)
Researchers have developed a new technology that fingerprints newborns. This technology collects temperature, pulse, breathing and oxygen, and identifies the infant through their fingerprint. Let's imagine you have been told this technology would be implemented in a month...

- How would this biometric technology influence your day-to-day role? Do/did you already use these technologies and what does this look like?
- What potential pros and cons do you see with this technology?
- How would you, as a patient, respond to your newborn being fingerprinted?
    - How do you think your patients would react?
    - What about your role as a nurse?

Next example scenario:
Northwell Health, based in New Hyde Park, New York, United States, is a healthcare network made up of 23 hospitals and over 700 physician offices and urgent-care centers. Northwell began rolling out a biometric system using iris scanning and facial recognition technology from RightPatient Inc. Northwell is one of the first major medical systems in the United States to outwardly discuss and deploy biometric technologies—and, as such, have been widely lauded by online medical, technology, and business publications as a "pioneer" in medical innovation.

- You mentioned that some of the technologies your workplace employs include (**fill in the blank:** facial recognition, fingerprinting, skeletal tracking, voice recognition, and palm/vein scanners). How do you use these technologies in your role? ***OR*** do you see some of these technologies (iris or facial) being implemented in your own hospital?
- If you don't directly use the technology, what would it look like if implemented in:
    - your own unit, day-to-day, or personally?
- What are some of your concerns with implementing this technology, if any, and why?

Here's where I check the time: I want to thank you for your time and willingness to talk with me. Do you have any further comments or questions?

Last example scenario (used in the interview if people are unfamiliar with biometrics)**:**
Most familiar to everyday people, and likely in your role as a neonatal nurse, are wearable devices (or biometric wearables). These devices, like Fitbit and Apple Watches, collect personal bodily identifiers such as pulse, heart rate, oxygen level, and blood pressure. Most recently, these wearables have been poised as a method for alerting people to if they may be positive for COVID-19 (linked article).

- Have you heard of biometrics prior to this study? In what capacity?
- Do you work with wearable technologies, and what does this look like?
- Are issues of privacy and technology use discussed with patients in your role?
- What about how the healthcare institution discusses privacy and technology use with you?

APPENDIX D: CONSENT PARAGRAPH AND QUESTIONNAIRE QUESTIONS

Consent. You are being invited to participate in a research study titled "Am I who I say I am? The Illusion of Choice: Biometric Identification in Healthcare" being conducted by Morgan Banville, a PhD Candidate at East Carolina University in the English department. The goal is to survey 100 individuals who identify as neonatal nurses in the United States. The survey will take approximately 10 minutes to complete. It is hoped that this information will assist in better understanding perceptions and use of biometric technologies. Your responses will be kept confidential, and no data will be released or used with your identification attached.

Your participation in the research is voluntary. You may choose not to answer any or all questions, and you may stop at any time. We will not be able to pay you for the time you volunteer for this portion of the study. Please call Morgan Banville at 508-817-6937 for any research related questions or the University & Medical Center Institutional Review Board (UMCIRB) at 252-744-2914 for questions about your rights as a research participant.

Q1. Describe your responsibilities as a neonatal nurse.
Q2. Describe your current workplace setting (hospital, private practice, etc.). How long have you been in this setting?
Q3. In your role as a neonatal nurse, what does privacy or personal information in healthcare mean to you?
Q4. This study is examining the use of and perceptions of biometric technologies, which are personal identifiers of the body that are collected for authentication purposes (commonly facial recognition, fingerprinting, palm scanners, and so on).
What does the term biometric technologies mean to you?
Q5. Does your current workplace employ these kinds of technologies? Select all that apply.
(The choices are: Facial Recognition, Fingerprinting, Skeletal Tracking, Pulsometer, Voice Recognition, Iris Scanning, Palm Scanner, Vein Scanner, Non-Contact Biometric Scanner (such as ION), N/A or None, Other).
Q6. As a neonatal nurse, where/how have you engaged with biometric technologies within healthcare (broadly defined)?
Q7. Are you interested and willing to participate in a short one-on-one interview session? This session will be conducted virtually, compensated if chosen to participate, and will be no longer than one hour.