Surveillance & Society

Quantifiable Bodies: The Influence of Biometric Technologies in Patient Consent

Morgan Banville et Elena Kalodner-Martin

Volume 22, numéro 3, 2024

Open Issue

URI : https://id.erudit.org/iderudit/1113686ar
DOI : https://doi.org/10.24908/ss.v22i3.16522

Aller au sommaire du numéro

Éditeur(s)

Surveillance Studies Network

ISSN

1477-7487 (numérique)

Découvrir la revue

Citer cet article

Banville, M. & Kalodner-Martin, E. (2024). Quantifiable Bodies: The Influence of Biometric Technologies in Patient Consent. *Surveillance & Society*, *22*(3), 325–337. https://doi.org/10.24908/ss.v22i3.16522

Résumé de l'article

While research has been done to identify the potential implications of biometric technology on marginalized populations' privacy and autonomy, this paper contributes to existing research by examining these technologies in healthcare settings. Drawing from insights across surveillance studies, rhetoric of health and medicine, and technical communication, we identify how one leading healthcare institution in New York City has employed rhetorics of efficiency, effectiveness, safety, and security regarding its biometric technology system. This employment of biometric technologies often contributes to patients' marginalization and dismissal. As we explore, interrogating the language used by the healthcare institution to describe biometrics opens opportunities for us—surveillance studies scholars, patients, allies, students, and more—to ensure that innovations within the healthcare system promote equity, agency, and improved outcomes for all.

Surveillance & Society

Article

Quantifiable Bodies: The Influence of Biometric Technologies in Patient Consent

Morgan Banville

Massachusetts Maritime Academy, USA
morgancbanville@gmail.com

Elena Kalodner-Martin

Massachusetts Institute of Technology, USA
kalodner@mit.edu

Abstract

While research has been done to identify the potential implications of biometric technology on marginalized populations' privacy and autonomy, this paper contributes to existing research by examining these technologies in healthcare settings. Drawing from insights across surveillance studies, rhetoric of health and medicine, and technical communication, we identify how one leading healthcare institution in New York City has employed rhetorics of efficiency, effectiveness, safety, and security regarding its biometric technology system. This employment of biometric technologies often contributes to patients' marginalization and dismissal. As we explore, interrogating the language used by the healthcare institution to describe biometrics opens opportunities for us—surveillance studies scholars, patients, allies, students, and more—to ensure that innovations within the healthcare system promote equity, agency, and improved outcomes for all.

Introduction

Grounded in surveillance studies, technical communication, and rhetoric of health and medicine, this study challenges how biometric technologies normalize surveillance practices, further suggesting impacts to privacy and "opt out" procedures. We focus specifically on unpacking language used by Northwell Health, a healthcare system that we use for our case example, to discuss the ways biometric technologies and patient consent is communicated in the context of Northwell's iris scanning and facial recognition rollout program. Language is one way surveillance scholars may intervene in communication practices, which is why we focus on not just the *ways* a major healthcare network uses surveillance technology but also the ways it *employs* and *discusses* such technology. We also further Novotny and Hutchinson Campos' (2019b: 650) claim that design of technologies, such as biometrics, can be adapted based on "consultation with privacy and surveillance scholars, and by redesigning Terms of Service/Use with options for users to decide what and how their personal, private health data is collected, stored, and used by the technology companies and their third parties."

We explore potential ways for how surveillance studies scholars may create systems of accountability to mitigate harm and challenge dominant power structures, particularly for those susceptible to silencing in institutional contexts. We refer to systems of accountability as the ways in which surveillance studies scholars may build coalitions between stakeholders in the medical system, analyze sites of surveillance, make apparent and transparent how the public are impacted, how they can advocate for themselves individually and collectively, and future steps for redressing inequity and harm. The following are our research questions:

Banville, Morgan, and Elena Kalodner-Martin. 2024. Quantifiable Bodies: The Influence of Biometric Technologies in Patient Consent. *Surveillance & Society* 22 (3): 325-337.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

- How are biometric technologies within health and medicine communicated to patients and wielded as a form of disciplinary control?

- What is the impact of surveillance technologies such as biometric technologies on patient ways of knowing?

- How do discourses surrounding biometric technologies in healthcare impact patient agency and autonomy?

Banville (2023) defines biometric technologies as any identifier of the body that is collected and used for personal identification (and authentication). The goal of collecting personal identifiers of the body is to prove or legitimize the self. As Banville (2023) notes, collection is often, if not always, used to prove you are who you say you are against the state system (or contracted third-party's repository) of personal identification. 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: 14). Digitization of the body occurs within the Northwell Health system; as such, biometric identification has often been "normalized" 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 the justifications, Lyon (2007: 25) mentions that, despite the ubiquity of surveillance technologies, it is important to study specific "sites of surveillance" to understand their nuances. The site of surveillance that this study focuses on is a hospital, though this is one of many sites within the assemblage of the larger medical-industrial complex. It is important to note that, throughout the manuscript, we refer to both "healthcare sites" and "healthcare systems or networks." Though these are related, we want to call attention to their differences: in this case, a healthcare site is a specific area of medical care, such as one hospital or clinic. A healthcare network, however, is a collection of sites that share a governing body (and thus, may also share policies and procedures). Because Northwell Health constitutes over two dozen hospitals and more than seven-hundred outpatient facilities and discussions of its biometric rollout apply to multiple locations, we refer to the Northwell healthcare network to emphasize how far-reaching the impact and implications may be for patients, providers, and other Northwell Health users and stakeholders.

Promoted under the guise of increased safety, improved identification protocols, and efficiency, biometric technologies have long been used by law enforcement and military personnel to identify "suspicious" individuals—often across racial and ethnic lines (Banville 2023). In healthcare networks, this may look like using biomarkers 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. Beyond shoring up beliefs about what kinds of knowledge are "valuable" (and profitable) to share in the name of improved patient care, biometric technologies continue to further harm those who are disabled, Black, Indigenous, people of color, LGBTQIA+, and other historically excluded groups.

In this study, we analyze a case example situated within the Northwell Health system as a site of surveillance. This specific site is a rich case example to guide our study in promoting advocacy and accountability work by better equipping technical communicators to consider how knowledge is (and could be) created, circulated, legitimized, and controlled, both within healthcare contexts and beyond. To further our understanding of the case example, we combined elements of rhetorical analysis and apparent feminism to determine how biometric technologies are being discussed in the healthcare context. For example, does the healthcare system discuss autonomy of patients, consent, privacy, and so forth? How do our findings allow for opportunities to discuss places to build collaborations between stakeholders across the medical system, careful to consider ways that do not further marginalize or undermine patient knowledge and experience? What can we learn about how these technologies are positioned, and what do we gain by

examining them? To begin to answer these questions, we first ground surveillance studies within technical communication, introduce how we take up biometrics within a biomedical framework, and discuss the methodologies that have guided our analysis.

We focus on biometric technologies specifically because of their increasing implementation into the everyday lives of people; this is a problem due to society's shift in implementing technologies that assist in security, efficiency, and convenience. Furthermore, given the likelihood that we will all interact with health and medicine at some point in our lives, considering the impact that biometric technologies can have within these settings is of deep personal, community, and professional interest. Governing bodies, such as medical institutions and their sponsors, often position biometric technologies as safe and secure; however, there is little to no discussion regarding the potential consequences of biometric data collection. Further, people, especially patients, are often expected to comply with self-surveilling their own bodily identifiers. "Good patients" are those who "comply" and therefore are also the ones who must engage in self or lateral surveilling to remain in "compliance." In addition to employing biometric technologies, the news outlets and organizations tend to discuss biometrics as helpful through showcasing how the tech centralizes care through the reduction of miscommunication; that is, biometrics are positioned as convenient for patient matching and authentication. Even so, biometric technologies and their collection of personal identifiers should be critically analyzed.

Situated at the Intersection of Technical Communication and Surveillance Studies

As we reveal about Northwell Health in the subsequent analysis, bodies are most easily controllable when quantifiable, and patients often must sacrifice privacy in the name of health; this collection and profiting off biometric data further exploits patients, especially the communities most vulnerable to abuse, silencing, and dismissal in medical contexts. Because timing is so important to emergency departments in hospitals, biometric technologies are used as a tool to help healthcare professionals keep patients secure while also completing a task with the maximum efficiency: in other words, efficiency is usually determined by the shortest possible amount of time to attend to a patient. Hartzband and Groopman (2016: 107) state, "physicians' sense that the clock is always ticking, and patients are feeling the effect." In shortened periods of time, doctors lack the ability to make decisions that listen to patients' preferences.

We view surveillance studies scholars as technical communicators: those who negotiate and communicate specialized information (Banville 2023). As surveillance studies and technical communication scholars have argued and established, technologies are not neutral nor objective, nor always accurate (Broussard 2023; Benjamin 2019; Noble 2018). As our primary concern, one such technology that is not neutral are biometric technologies, which include health-related applications and tools (see Tham 2016, 2017; Novotny and Hutchinson Campos 2019a). We as surveillance studies scholars are well-positioned to communicate specialized knowledge and explore how knowledge is communicated: how do we use our knowledge and skills to address information imbalances?

One example of the way surveillance studies scholars have addressed information imbalance is through the Algorithmic Justice League (AJL), a digital advocacy group that raises awareness about the social implications of artificial intelligence (AI). The AJL brings together art, stories, and research from a variety of stakeholders to mitigate AI bias and harm. This coalition is one of many examples of work surveillance scholars are extending outside of academia to engage in more public-facing scholarship. The AJL is an example of how surveillance studies scholars can commit to scholarship and activism both with and for vulnerable communities. To better understand the impact of biometric technology usage in healthcare systems, we believe it is helpful to use more familiar examples, most notably from the AJL.

Though resolved at the time of revisiting this example, the United States Internal Revenue Service (IRS) had partnered with ID.me for tax-related identification. ID.me is well-known for its origination in

ecommerce to validate teachers and workers for corporate discounts. Joy Buolamwini (2022), founder of the AJL, writes that ID.me (formerly known as TroopSwap) claims to provide "secure identity proofing, authentication, and group affiliation verification for government and businesses across sectors." This example is one of many where governmental agencies utilize third parties to collect personal information about its citizens (and those who are not). In fact, ID.me alone serves "27 states, multiple federal agencies, and over 500 name brand retailers" (Buolamwini 2022). One of the deep-rooted problems with a biometric system such as ID.me, is how it fails to adequately address its known harms or deeply engage with specific findings that indicate substantial racial bias (Buolamwini 2022). Technologies and algorithmic bias have not just been critiqued within higher education as perpetrating substantial racial bias (Broussard 2023; Noble 2018), but this claim has also been documented in a 2019 US Department of Commerce report (Grother, Ngan, and Hanaoka 2019). According to the US Department of Commerce's National Institute for Standards and Technology, researchers observed, "higher rates of false positives for Asian and African American faces relative to images of Caucasians. The differentials often ranged from a factor of 10 to 100 times, depending on the individual algorithm. False positives might present a security concern to the system owner, as they may allow access to impostors" (Grother, Ngan, and Hanaoka 2019).

We give this example of a federal entity, the IRS, partnering with ID.me for intended "ease of access" in submitting taxes because of the transferability to other vulnerable systems, such as healthcare. Along with the documented claims that false positives with one-to-one facial recognition are common amongst Asian and African American faces, the privacy and security risks are high and should be addressed. While ID.me certainly poses a larger issue for people of color, like many other aspects of biometric identification, other oppressed groups will be affected as well. 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 and Currah 2015). Furthermore, in popular media, there have been cited instances where insurance companies such as UnitedHealthcare have used AI models to deny care, despite a high error rate. This example addresses the complexities within the healthcare network, since UnitedHealthcare is the largest health insurer in the United States (Mole 2023). Artificial intelligences, as demonstrated with the false positives in facial recognition technologies, are not perfect. As Mole (2023) writes, the lawsuit filed against UnitedHealthcare is based on the algorithm's inaccuracies: over 90 percent of the denials are reversed, since UnitedHealthcare is using the AI algorithm to "override doctors' judgments and wrongfully deny critical health coverage to elderly patients." Mole (2023) reports that this denial has resulted in "patients being kicked out of rehabilitation programs and care facilities far too early, forcing them to drain their life savings to obtain needed care that should be covered under their government-funded Medicare Advantage Plan." The UnitedHealthcare example is one of many that are part of healthcare networks' increasing use of technologies that further harm vulnerable populations. We believe these examples help to provide some context for the concerns that surround biometric technologies, and how surveillance studies scholars may continue to intervene and contribute to decision-making protocols, especially in particularly vulnerable sites such as healthcare system(s).

The aforementioned examples may be labeled as cruel optimism (Berlant 2011). 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: 16). Neoliberal capitalism uses biopolitical control disguised as potentially "positive" deliverables such as safety and security. Queer theorists such as Ruti (2017) question and critique the ideals of success articulated by scholars such as Jack Halberstam: for example, Ruti (2017: 16) critiques the idea that 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." 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 in our society. Opting out

then, in this capacity, is the ability to defeat the cruel optimism that "exists when something you desire is actually an obstacle to your flourishing" (Berlant 2011: 1). So, as Banville (2023) argues, instead of continuing our desires and fantasies as established by the dominant norm, we must "opt out" of such; this may lead to our "seeing" the norms that we have been persuaded to conform to and defy such structures. There is an illusion of choice associated with opting out, which 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 (Banville 2023: 67). In our Northwell Health example, cruel optimism appears when patients who belong to marginalized populations become increasingly alienated from their very own wellbeing—whether it be due to algorithmic bias or issues of human bias that intervene with the datasets—due precisely to their commitment to it.

Health and Biomedicine

As we have suggested, one such space that we might intervene and resist is in healthcare networks—these systems include hospitals, practitioner offices, pharmaceutical companies, and insurance providers—all of which impact and are implicated in patient care. Biometric technologies are still quite "new" in these spaces and systems, and it is therefore important to ground our analysis of their use and effects by drawing connections between biometrics and bio*medicine.* As we have discussed, the United States has a preoccupation with quantifying, measuring, and controlling physical bodies. In the medical-industrial complex, this preoccupation marginalizes and undermines patient knowledge, minimizes agency, and infringes upon their privacy. Biometric technology expands and enables this, and as more institutions turn towards collecting and using biometric data, it is increasingly important for surveillance studies scholars to identify underlying ideological motives.

Biomedicine is the study and practice of applying biological and physiological principles to health and medical care settings (Foucault 1975) with the goal of "correct[ing] disease and restor[ing] normal functioning" (Fuller 2017: 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 system across the United States and in much of the Western world for over a century. Furthermore, in its most general sense, because biomedicine determines which conditions and what types of interventions are "approved" through institutionally determined protocols and procedures, biomedicine exhibits enormous rhetorical sway across the whole medical-industrial complex. As such, understanding how biomedicine operates is imperative to understanding how other facets of our healthcare system—such as the deployment of biometric technology—may be used, when, and most importantly, why.

Krieger (2011: 130) summarized biomedicine's core theoretical commitments in three keyways: that health phenomena must be understood in terms of physical and biochemical entities and processes; that experimental techniques are the preferred means of acquiring and assessing health-related knowledge; and that human bodies are best understood as composed of a collection of subsidiary parts and processes. These values shape every aspect of the medical-industrial complex, from institutional policies to how medications are approved, authorized, dispensed, and controlled. This is evidence of, as Derkatch (2016) puts it, how biomedicine operates as a bounded system that perpetuates itself as the sole arbiter of authority, credibility, and legitimacy. Our concern here is in untangling these implications to both highlight how biometrics may work in service to biomedical ideology and showcase how they may contribute to healthcare disparities for multiply marginalized patients (Dubriwny 2012; Hernández and Dean 2020; Parrot and Condit 1996).

Though biomedicine is well-established, the use of biometrics in healthcare settings is increasing in its popularity and traction. As such, research is needed to untangle how biomedicine and biometrics work together to restrict patient autonomy, agency, and privacy under the guise of improved healthcare processes and outcomes for providers and patients alike. To begin this work, we look at the example of Northwell

Health (also referred to as "Northwell"), a New York-based healthcare network that began using biometric technologies for patient identification, record matching, care coordination, and more. While these measures sound like positive interventions (and can be), we draw from research at the intersections of surveillance studies and technical communication to dig deeper into the unstated (or invisible) consequences, limitations, and considerations for these technologies in medical settings. This creates opportunities for how—and why—surveillance studies scholars might further intervene in biometric usage across the medical-industrial complex.

Methods: Case Example

To better understand how discourses about biometric technology circulate in medical settings, we specifically chose a case example from Northwell Health to create thematic analyses. Because the communication practices that surround a particular technology's deployment often precede its actual implementation, we argue that this case example can bridge to a larger textual corpus, such as patient consent forms, that would benefit from a rhetorical analysis. Though this is a worthy future project for surveillance studies scholars, we begin this work by examining a specific form of biometrics at one healthcare network to gain and reveal an understanding of how biometric technology is currently positioned and by whom.

Northwell Health, based in New Hyde Park, New York, US, is a healthcare network made up of twenty-three hospitals and over seven-hundred physician offices and urgent-care centers. Northwell is New York State's largest healthcare provider and private employer and primarily serves New York City, Long Island, and Westchester. According to their 2020 financial report, their net income was $775.5 million that year, up from $672.3 million in 2019 (Northwell Health 2020). That same year, Northwell began rolling out a biometric system using iris scanning and facial recognition technology from RightPatient Inc. Northwell is one of the first major healthcare networks to implement biometric technology on such a wide scale, and thus offers a unique opportunity to examine how its benefits, limitations, and risks are posed to stakeholders across the medical system.

To examine this, we collected eight articles from online publications that discuss Northwell Health's biometric technology plan. These articles were written for a wide range of readers, including patient audiences, healthcare venture capitalists, and practitioners. As such, our analysis examined how the value and implications of these technologies in healthcare settings were explained to diverse readers. Because of the particularly vulnerable position that patients are in due to imbalances of authority and power, our methodology, detailed below, focuses specifically on biometric discourse and patient populations.

We approached analyzing the texts utilizing intercoder reliability. That is, after one person read through each Northwell Health article and completed a round of initial coding, the second person conducted a separate analysis. This inductive coding round helped establish a basic understanding and shared language for talking and writing about our data's surface-level meaning (Charmaz, Thornberg, and Keane 2017: 424). From there, we completed a second round of abductive coding, which blends inductive and deductive approaches and allows for the development of new theories about the data based on existing concepts and questions (Vila-Henninger et al. 2022). For example, we both identified the "accuracy" of biometric technologies as an inductive theme in our corpus, and revisiting the texts with this knowledge provided an opportunity to group other related codes together in conversational categories for further analysis.

Methodology: Apparent Feminism and Rhetorical Analysis

We draw from a joint methodology in this project: rhetorical analysis and apparent feminism. Rhetorical analysis is a "qualitative research method that is designed for the systematic investigation and explanation of symbolic acts and artifacts for the purpose of understanding rhetorical processes" (Foss 2018: 6), such as the production and circulation of health-related content online. However, rhetorical analysis also helps to

identify "rhetorical acts as they relate to identity categories or historical moments but also engages how complex networks of relationships affect rhetorical meaning" (Dingo 2012: 14). The complex network of relationships, and the structures of power that are both explicit and implicit within them, are central to our understanding of how biometric technologies exert control over patient choice. Furthermore, because Northwell Health is a network of multiple institutions across New York state, rhetorical analysis also provides insights into how to contextualize the larger scale impact of discriminatory technology design and implementation.

As Frost (2018) reveals in an analysis of reproductive health policies, terms like efficiency may appear to be impartial, which thus rejects the need for feminist analyses of such documents while masking the material and embodied consequences they have for women's health. Central to our analysis, however, is that apparent feminism is not only about identifying the way these "objective" terms may, even if unintentionally, contribute to marginalization and harm for vulnerable populations like patients. Apparent feminism is also focused on providing solutions, especially through "coalition-building with those who might appear to be feminist in their activism or ideological perspectives, but for whatever reason do not embrace that label" (Frost 2013: 65). Put differently, apparent feminism explicitly invites those who are committed to achieving justice-oriented aims, such as elevated access to clinical information, patient agency and autonomy, and improved healthcare outcomes for all patients, to work alongside those who see these goals as being inherently about—and accomplished through—feminist ideals of equity, community, sustainability, and respect (Ollivier and Tremblay 2000).

Findings

As have discussed, Northwell is one of the first major healthcare networks in the United States to outwardly discuss and deploy biometric technologies—and, as such, has been lauded by the online medical, technology, and business publications in our textual corpus as a "pioneer" in medical innovation. Because of this, Northwell is a fitting case study to examine how rhetorics of efficiency, effectiveness, and safety are often employed to obscure the risks and limitations of this technology.

Efficiency

Because of the timely nature of many medical concerns, efficiency is often a central biomedical goal. However, considerations of efficiency also extend beyond time. Of the eight articles examined for language about biometric use in healthcare, 100% of them explicitly mention the ways that biometric technologies can save energy and labor for providers, medical staff, or patients, with 43% of them also referring to saving resources and space. While we do acknowledge that the imperative for efficiency *can* lead to improvements in patient care, such as increased care coordination, decreased wait times, and access to medical information and records, we also call attention to its shortcomings. One notable shortcoming manifests when the constant drive for efficiency comes at the expense of patient privacy and autonomy.

For example, HealthLeaders Media published a 2018 article in which Keely Aarnes, Associate Vice President of Revenue Cycle Management at Northwell Health, praised one aspect of Northwell's facial recognition software: the ability to identify patients even before they have checked in, spoken with a receptionist, or requested care. "Today, you have to stand in line, register, and write your name on a clipboard. Tomorrow, we'll know a patient has arrived before they've even spoken to somebody because we've picked up on their facial image. That's game-changing," Aarnes shared. "It really changes the way we look at healthcare; it becomes more of a concierge service. We'll welcome you before you've even told us who you are" (Aarnes qtd in. Roth 2018). In this way, efficiency refers to the time that patients may spend seeking care and navigating medical bureaucracies; by positioning facial recognition software as the solution to overburdened systems, complicated procedures, or disorganized protocols, we suggest that new concerns regarding privacy and patient agency may be introduced while allowing the reasons for systemic inefficiencies to go uninterrogated. Furthermore, though we also want to identify the value of personalized

healthcare solutions that treat each patient as a unique individual with unique needs, we want to identify how Aarnes' framing *removes* from patients the ability to introduce themselves and their concerns, and to take an active role in clinical decision-making.

In another one of our articles, Sean Kelly, MD, the Chief Medical Officer at digital identity company Imprivata, discussed how biometrics also facilitate efficiency regarding prescriptions, one of the most highly regulated aspects of many medical systems. As Kelly posits, biometrics may be used in dual-factor authentication, enabling "easy, fast, and highly-secure ways" for medication information to be shared between providers, patients, and pharmacies (qtd. in Marbury 2019). Through Kelly's use of phrases like "highly-secure" to pitch the value of iris and fingerprint scanning, and Aarnes' reference to patient convenience in describing facial recognition, we are meant to understand that *refusing* biometric technologies implicitly means longer wait times, more imprecise care, less security, and as we discuss in more depth below, lower-quality care.

Effectiveness

Medical effectiveness, which we take up as any measure that a healthcare institution or provider can take to improve care outcomes, is also referenced in 100% of our articles and is another driving reason for Northwell's biometric use. In identifying moments where rhetorics of effectiveness are used, we do not mean to suggest that healthcare providers should not be concerned about effectiveness or efficacy, nor do we believe that effectiveness is not centrally important in determining quality of care. Instead, we identify how the drive for effectiveness—and the way surveillance technologies are implicated in this drive—similarly comes at the cost of privacy and autonomy.

In another trade publication, Aarnes shared, "We intend to also pilot and test opportunities through AI [artificial intelligence] that can identify indicators from changes in appearance, pointing to clinical indicators…. With a longitudinal view of the patient's pictures, there are many opportunities to create alerts to the patient's care team" (qtd. in Joy 2019). This is an example of the ways that biometrics can shore up biomedical logics and have consequences for patient agency; by prioritizing certain forms of evidence over patients' needs and goals, concerns are raised directly with providers and not with patients. This model of "proactive" care also means that patients' concerns may not be taken seriously if a "clinical indicator" cannot be observed or measured by the AI system in use.

However, the link between biometric technologies, effectiveness, and institutional oversight is also reinforced for providers on a psychological level. For example, in an article published by Northwell Health (2023), Dr. Jennifer Laffey, the Vice President of Employee Health Services at Northwell, asserted that biometrics provide valuable insights into what medical concerns employees face and "if and what kinds of health care services, interventions, incentives and support they can offer their employees." As the article further explains, these programs—created and reinforced through aggregated biometric data—can boost employee productivity, reduce absenteeism, and lead to a positive return on investment for the Northwell system. And yet, because employees, like patients, are likely not invited to weigh in on their health concerns or participate in discussions about how to revise wellness programming, they too may be deprioritized at the expense of institutions' professional, social, and economic values. By calling attention to the way biometrics can contribute to precarity for multiple stakeholders across the healthcare system, we ultimately want to call attention to the ways that surveillance is always about control and protecting the interests of those who wield it, even if the rhetorics surrounding its deployment appear to be about consumer, client, or employee benefit.

Safety and Security

Our final emerging theme and another central reason that biometrics are positioned as valuable in healthcare settings, especially at Northwell, is safety and security. Cited examples about the role of biometric technologies within healthcare often include improved patient matching and identification systems,

increased coordination across providers, and consistent access to records for both patients and healthcare professionals. However, as we have introduced earlier, safety is often positioned within a neoliberal worldview, where governments and other regulating institutions are given power to surveil and regulate the existence and movement of marginalized populations. Taken alongside a biomedical hierarchy of knowledge-making—with powerful medical institutions and regulatory bodies at the top and patients at the bottom—the language of safety and security suggests protecting the values of those people and companies in power over those who seek their services.

This power differential is carefully reinforced in medical settings. Given negative connotations that patients had with the word "scan," Aarnes reported to *Managed Healthcare Executive Magazine* that Northwell staff would refrain from using this word when discussing how biometric information was collected and stored; instead, training resources focused on "finding the sweet spot of information and educating our patients that this is for their benefit in safety and ease of registration" (Aarnes qtd. in Marbury 2019). This example illustrates how rhetorics of safety and security, coupled with complex consent forms, can foreclose opportunities for patients to fully understand personal identification collection. Rather than engage in transparent practices, Northwell Health has elected to shift their language to ease patient fears. This masking of language displays one of the main issues with surveillance and privacy in general: it is difficult to notice all the ways our bodies are surveilled and the following consequences of such surveillance due to the largely invisible and insidious ways surveillance occurs. Because biometrics are poised as a necessity for safety and security, patients are led to believe that this is for their own good and that any negative connotations of words associated with biometric identification (such as "scan") is inaccurate. As such, they may be unable to opt out of such technologies or may consent to them without a full understanding of what information is being collected or through what methods.

While biometric technology processes may not be fully explained to patients in acquiring their initial consent, we also want to identify the ongoing infringements to patient privacy that occur in the name of safety and security. According to Laura Semlies, Vice President of Digital Patient Experience at Northwell, their systemwide biometric rollout means that, when patients enroll in one location, they will not need to update their information when at another facility nor jump through the hoops of completing paperwork again (Knowles 2019). Though feminist scholarship has long named consent to be an ongoing and negotiated practice (Im et al. 2021), Northwell's policy—in which a patient may, with some varying degree of transparency, agree to biometric data collection once—means that patients will not be able to easily revisit their consent for biometric surveillance at other healthcare sites or in different situations. Furthermore, because there is no public information at the time of this writing (November 2023) that indicates how a patient may *revoke* consent at all Northwell Health locations, we are further meant to understand that biometric use in the name of safety, efficiency, and effectiveness is a permanent fixture in patient care within this network.

Surveillant Action and Advocacy

Though we have treated each of the broad themes as discrete categories, we want to identify the ways in which efficiency, effectiveness, and safety and security often overlap. For example, iris identification and high-resolution facial imaging can be used to "warn staff of security risks" by identifying high-risk patients, such as those with a history of fraudulent or "drug-seeking" behaviors (Aarnes qtd. in Marbury 2019). Much work has been done to uncover how deficit models of addiction and substance abuse contribute to stigma and decreased care outcomes (Frank and Nagel 2017), and biometric technologies that support these ideas further perpetuate inaccessible healthcare systems for people struggling with addiction. However, this example also demonstrates the complex overlap between the three themes that we have outlined in our analysis.

In this case example, biometric technologies promote efficiency because they allow patients to be identified without the need for direct patient → provider communication, even if that risks misidentifying the reason for a patient's visit. Biometric technologies support effectiveness, because they may predict what a patient is seeking and thus supposedly connect that person with the "appropriate" intervention, though patients may not be consulted in the creation of this treatment plan. Finally, they allow for increased safety and security by identifying people whose past histories in medical settings mark them as an institutional threat or risk, even though this puts the patient's health and safety beneath that of a powerful governing body. Though these are all inherent and important risks to note, we also see many opportunities for patients, surveillance studies scholars, and allies to work together to promote true efficiency, effectiveness, and safety and security for all.

We suggest that the first step towards redressing the harmful effects of these surveillance policies requires looking beyond the protocols and documents that institutions use to create consumer compliance. While companies who create biometric technologies will argue that patients are notified about privacy and consent practices through Terms and Conditions and Privacy Policies, surveillance scholars have argued (Banville 2020; Neville 2020; Woods and Wilson 2021) that such documents are inaccessible, and further, can be modified due to the digitality. This is a particularly pressing concern in healthcare; the high-stakes and potentially emergent nature of medical care likely means that Terms and Conditions are not a primary concern to patients who are seeking medical care. These examples all demonstrate that the policies and procedures that are put in place to ensure consent and safety often do not function this way; as we discuss below, this creates both a need and an opportunity for taking more effective, holistic, and sustainable actions to ensure patients' safety and agency.

Given these concerns, the healthcare context, and the rhetorics surrounding biometrics' use and value, we contend that the tension and power dynamics between health institutions and patients must be further untangled and explored. Surveillance studies scholars are well-poised to intervene and advocate for patient rights in data collection processes by asking:

- What is the apparent need for biometric technology?
- How can patients have a say or opportunity to opt out of certain technologies?
- Are patients notified verbally and linguistically of the implications or harms of biometrics data collection and dissemination?
- "How can users call for a redesign of an application based on negative experiences such as surveillance, non-consensual data collection, or troubling interactions with other users and/or representatives working on behalf of the tech company (content moderators, designers, etc.)?" (Novotny and Hutchinson Campos 2019b).

Ideally, patients should be notified and aware of the processes involved with their own personal identifiers, or biometric data. We hope that from this article, surveillance studies scholars will:

- Mobilize the fusion of apparent feminism and rhetorical analysis as a methodology for understanding how the deployment of biometric data in the healthcare field heavily relies on masking language (or its very lack thereof) and devaluation of the affective dimension of medical conditions.
- Continue to make apparent the invisible: that is, creating public-facing documents that inform patients about the very systems they are agreeing to.

- Further contribute to engaging in systems of accountability through focusing on popular sites of surveillance, such as within healthcare networks. Such sites of surveillance within popular industries, especially those most precarious, are where surveillance studies scholars should take up their work.

- Shift conversations about surveillance away from sole discussion of "privacy, security, and efficiency" to a consideration of the "ethical problem of combating new forms of discrimination that are practiced in relation to categories of privilege, access, and risk" (Hall 2015: 148).

- Engage in coalitional work to shift language and practices surrounding privacy and surveillance from individual to collective responsibility. Build collaborations between stakeholders across the medical system, carefully considering and amplifying patient knowledge and experience(s).

As we have mentioned, bodies are most controlled when quantifiable, and patients often give up privacy in the name of health; this collection and profiting off patients' biometric data further exploits patients, especially communities most vulnerable to abuse. We, as surveillance studies scholars and patients ourselves, must intervene in issues of consent, privacy, and security to create systems of accountability. To reiterate, systems of accountability are created when surveillance studies scholars analyze sites of surveillance and make apparent and transparent the ways in which the public are impacted, the ways they can advocate for themselves and collectively, and next steps/options (site dependent). As Amidon, Moore, and Simmons (2023: 5) note, systems of accountability can be reflected in the coalitional and community work that we do as surveillance scholars: "partnering with community groups and organizations to fund or facilitate meetings or workshops, develop grant proposals, create documentation, improve the usability of organizational processes or services, and/or participate in activist campaigns to respond to injustices causing harm within communities." The Northwell Health case example is only the beginning of the future of biometric technologies and identification in healthcare, and the subsequent push for regulatory efforts. For example, a bill establishing consumer health data rights known as ESHB 1155,90 or "My Health, My Data Act," has passed 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.[1] States should take notice of the increase in efforts towards introducing ways to protect people that extend into the digital sphere.

Though biometric technologies have been positioned as necessary for security and protection, it is crucial that surveillance studies scholars "resist, subvert, and intervene" in the production of knowledge and decision-making that is not transparent for public audiences (Frost and Eble 2015). Currently, biometric technology use in the medical-industrial complex creates a manipulative relationship: patients truly cannot opt out because they need treatment (patients/people seeking treatment are in an especially vulnerable position). Those who create and implement biometric technologies further do not consider patient confidentiality and autonomy, including data protection. Interrogating the language used by the healthcare institution to describe biometrics opens opportunities for us—surveillance studies scholars, patients, allies, students, and more—to ensure that innovations within healthcare networks promote equity, agency, and improved outcomes for all.

References

Amidon, Timothy, Kristen Moore, and Michele Simmons. 2023. Community Engaged Researchers and Designers: How We Work and What We Need. *Communication Design Quarterly* 11(2): 5–9.

[1] As of when this was written in Spring 2023.

Banville, Morgan. 2020. Resisting Surveillance: Responding to Wearable Device Privacy Policies. *The Proceedings of the 38th ACM International Conference on Design of Communication (SIGDOC '20), October 03-04, Denton, Texas, US*, 1–8. New York: ACM.

———. 2023. Am I Who I Say I Am? The Illusion of Choice: Biometric Identification in Healthcare. PhD diss., East Carolina University.

Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code.* Cambridge, UK: Polity Press.

Berlant, Lauren. 2011. *Cruel Optimism.* Durham, NC: Duke University Press.

Broussard, Meredith. 2023. *More than a Glitch: Confronting Race, Gender, and Ability Bias in Tech*. Cambridge, MA: MIT Press.

Charmaz, Kathy, Robert Thornberg, and Elaine Keane. 2017. Evolving Grounded Theory and Social Justice Inquiry. In *The SAGE Handbook of Qualitative Research*, edited Norman K. Denzin and Yvonna S. Lincoln, 411–443. Thousand Oaks, CA: Sage Publications.

Derkatch, Colleen. 2016. *Bounding Biomedicine: Evidence and Rhetoric in the New Science of Alternative Medicine*. Chicago, IL: University of Chicago Press.

Dingo, Rebecca. 2012. *Networking Arguments: Rhetoric, Transnational Feminism, and Public Policy Writing*. Pittsburgh, PA: University of Pittsburgh Press.

Dubriwny, Tasha N. 2012. *The Vulnerable Empowered Woman: Feminism, Postfeminism, and Women's Health.* New Brunswick, NJ: Rutgers University Press.

Foss, Sonja. 2018. *Rhetorical Criticism: Exploration and Practice*. 5th Edition. Long Grove, IL: Waveland Press.

Foucault, Michel. 1975. *The Birth of the Clinic: An Archaeology of Medical Perception*. New York: Vintage Books.

Frank, Lily E., and Saskia K. Nagel. 2017. Addiction and Moralization: The Role of the Underlying Model of Addiction. *Neuroethics* 10 (1): 129–139.

Frost, Erin A. 2013. Theorizing an Apparent Feminism in Technical Communication. PhD diss., Illinois State University.

———. 2018. Apparent Feminism and Risk Communication: Hazard, Outrage, Environment, And Embodiment. In *Key Theoretical Frameworks: Teaching Technical Communication in the Twenty-First Century*, edited by Michelle Eble and Angela Haas, 23–45. Logan, UT: Utah State University Press.

Frost, Erin A., and Michelle Eble. 2015. Technical Rhetorics: Making Specialized Persuasion Apparent to Public Audiences. *Present Tense* 4 (2): http://www.presenttensejournal.org/wp-content/uploads/2015/04/FrostandEble.pdf.

Fuller, Jonathan. 2017. The New Medical Model: A Renewed Challenge for Biomedicine. *Canadian Medical Association Journal* 189 (17): E640–E641.

Gates, Kelly. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. 2019. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. NISTIR 8280, National Instutite of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280.

Hall, Rachel. 2015. Terror and the Female Grotesque: Introducing Full-Body Scanners to U.S. Airports. In *Feminist Surveillance Studies*, edited by Rachel E. Dubrofsky and Shoshana Amielle Magnet, 127–149. Durham, NC: Duke University Press.

Hartzband, Pamela, and Jerome Groopman. 2016. Medical Taylorism. *The New England Journal of Medicine* 374: 106–108.

Hernández, Leandra H., and Marleah Dean. 2020. "I Felt Very Discounted": Negotiation of Caucasian and Hispanic/Latina Women's Bodily Ownership and Expertise in Patient-Provider Interactions. In *Interrogating Gendered Pathologies*, edited by Erin A. Frost and Michelle F. Eble, 101–118. Boulder, CO: University Press of Colorado.

Im, Jane, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S. Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, May 8–13*, 1–18. https://doi.org/10.1145/3411764.3445778.

Knowles, Megan. 2019. How Hospitals Use Biometrics to Prevent Patient ID Errors, Speed Service. *Becker's Clinical Leadership,* February 8. https://www.beckershospitalreview.com/quality/how-hospitals-use-biometrics-to-prevent-patient-id-errors-speed-service.html [accessed August 10, 2023].

Krieger, Nancy. 2011. *Epidemiology and the People's Health: Theory and Context.* Oxford, UK: Oxford University Press.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Malden, MA: Polity Press.

Marbury, Donna. 2019. Why Biometrics are the Future of Patient Care. *Managed Healthcare Executive*, March 7. https://www.managedhealthcareexecutive.com/view/why-biometrics-are-future-patient-care [accessed August 10, 2023].

Mole, Beth. 2023. UnitedHealth Uses AI Model with 90% Error Rate to Deny Care, Lawsuit Alleges. *Ars Technica*, November 16. https://arstechnica.com/health/2023/11/ai-with-90-error-rate-forces-elderly-out-of-rehab-nursing-homes-suit-claims/ [accessed August 10, 2023].

Moore, Lisa J., and Paisley Currah. 2015. Legally Sexed, Birth Certificates and Transgender Citizens. In *Feminist Surveillance Studies*, edited by Rachel Dubrofsky and Shoshana Magnet, 58–79. Durham, NC: Duke University Press.

Neville, Stephen. 2020. Eavesmining: A Critical Audit of the Amazon Echo and Alexa Conditions of Use. *Surveillance & Society* 18 (3): 343–356.

Noble, Safiya. 2018. *Algorithms of Oppression*. New York: New York University Press.

Northwell Health. 2020. Annual Financial Information and Operating Data. https://www.northwell.edu/sites/northwell.edu/files/2021-06/Northwell-Health-Annual-Financial-Information-2020.pdf.

Novotny, Maria, and Les Hutchinson Campos. 2019a. Data Our Bodies Tell: Towards Critical Feminist Action in Fertility and Period Tracking Applications. *Technical Communication Quarterly* 28 (4): 332–360.

———. 2019b. Tracing the Future Lineage for OBOS: Reproductive Health Applications as a Text for Feminist Rhetorical Inquiry. *Peitho* 21 (3): https://cfshrc.org/article/tracing-the-future-lineage-for-obos-reproductive-health-applications-as-a-text-for-feminist-rhetorical-inquiry/#works-cited.

Ollivier, Michèle, and Manon Tremblay. 2000. *Questionnements Féministes et Méthodologie de la Recherche.* Montréal, CA: L'Harmattan.

Parrot, Roxanne Louiselle, and Celeste Condit. 1996. *Evaluating Women's Health Messages: A Resource Book*. Los Angeles, CA: SAGE Publications.

Roth, Mandy. 2018. Biometric Technology for Patient Identity: 4 Things to Know. *Health Leaders Media,* December 11. https://www.healthleadersmedia.com/innovation/biometric-technology-patient-identity-4-things-know [accessed August 10, 2023].

Ruti, Mari. 2017. *The Ethics of Opting Out: Queer Theory's Defiant Subjects.* New York: Columbia University Press.

Tham, Jason. 2016. Globally Fit: Attending to International Users and Advancing a Sociotechnological Design Agenda for Wearable Technologies. In *Proceedings of the 34th ACM International Conference the Design of Communication, Silver Spring, MD, September 23–24,* 1–9. http://dl.acm.org/citation.cfm?id=2987599.

———. 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.

Vila-Henniger, Luis, Claire Dupuy, Virginie Van Ingelgom, Mauro Caprioli, Ferdinand Teuber, Damien Pennetreau, Margherita Bussi, and Cal Le Gall. 2022. Abductive Coding: Theory Building and Qualitative (Re)Analysis. *Sociological Methods and Research* 53 (2): https://doi.org/10.1177/00491241211067508.

Woods, Charles, and Noah Wilson. 2021. The Rhetorical Implications of Data Aggregation: Becoming a "Dividual" in a Data-Driven World. *The Journal of Interactive Technology & Pedagogy* 19: https://jitp.commons.gc.cuny.edu/tag/social-media/.

Textual Corpus[2]

Alkhaldi, Nadejda. 2021. Biometrics in Healthcare: Use Cases, Benefits, and Things to Consider. *Itrex Group,* September 14. https://itrexgroup.com/blog/biometrics-in-healthcare-applications-advantages-challenges/ [accessed August 10, 2023].

Buolamwini, Joy. 2022. The IRS Should Stop Using Facial Recognition. *The Atlantic,* January 27. https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386/ [accessed August 10, 2023].

Definitive Healthcare. 2022. 3 Ways Biometric Technologies Improve Hospital Performance. *Definitive Healthcare,* May 15. https://www.definitivehc.com/blog/ways-biometric-technology-improves-healthcare [accessed August 10, 2023].

Gormley, Brian. 2019. Hospitals Turn to Biometrics to Identify Patients. *The Wall Street Journal,* February 6. https://www.wsj.com/articles/hospitals-turn-to-biometrics-to-identify-patients-11549508640 [accessed August 10, 2023].

Joy, Kevin. 2019. Biometrics in Healthcare: How it Keeps Patients and Data Safe. *Health Tech Magazine*, December 23. https://healthtechmagazine.net/article/2019/12/biometrics-healthcare-how-it-keeps-patients-and-data-safe-perfcon [accessed August 10, 2023].

Northwell Health. 2023. How On-Site Biometric Screenings Lead to a Healthier Workforce. April 11. https://northwelldirect.northwell.edu/blog/biometric-screenings [accessed August 10, 2023].

Siwicki, Bill. 2018. Biometrics Entering a New Era in Healthcare. *Healthcare IT News,* July 30. https://www.healthcareitnews.com/news/biometrics-entering-new-era-healthcare [accessed August 10, 2023].

Zucco, Erica. 2023. Bill to Strengthen Privacy of Health Data Passes State House, Senate. *King TV*, April 6. https://www.king5.com/article/news/politics/state-politics/bill-strengthenprivacy-health-data/281-527855ee-640a-4e80-b655-6f89c977fdc0 [accessed August 10, 2023].

[2] The textual corpus includes eight articles that were collected from online publications that discuss Northwell Health's biometric technology plan. These articles were written for a wide range of readers, including patient audiences, healthcare venture capitalists, and practitioners. While all of the sources contributed to the analysis, only those that were directly quoted or referenced are cited in-text.