Scientific Research Publishing

Open Journal of Social Sciences, 2026, 14(3), 15-35
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Beyond Recognition: The Complexities of Biometrics and Minority Rights

Fatma Fattoumi

Laboratory of Language and Cultural Forms, Department of English, Higher Institute of Languages of Tunis, University of Carthage, Carthage, Tunisia
Email: fattoumifattouma@gmail.com

How to cite this paper: Fattoumi, F. (2026). Beyond Recognition: The Complexities of Biometrics and Minority Rights. *Open Journal of Social Sciences, 14,* 15-35.
https://doi.org/10.4236/jss.2026.143002

Received: December 12, 2025
Accepted: March 3, 2026
Published: March 6, 2026

Copyright © 2026 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

The ubiquitous use of biometric technology in contemporary society, from unlocking smartphones to enforcing border control and law, has raised concerns regarding its impact on minority rights. In particular, the Arab Muslim minority has been identified as a vulnerable group subject to potential violations of privacy, bias, and discrimination. This paper aims to critically examine the complexities of biometric technology and its impact on the Arab Muslim minority, drawing on US-specific examples. Our analysis reveals how biometric technology can perpetuate existing biases and marginalize Arab Muslim voices, thereby exacerbating issues of inequity and inclusivity. We argue that a democratic approach to biometric technology is crucial, emphasizing the principles of transparency, accountability, and individual rights. Through a nuanced understanding of the intricacies of biometric technology and its implications for the Arab Muslim minority, we can advance towards a more just and equitable society that upholds the rights of all individuals, regardless of their ethnic or religious affiliation.

Keywords

Biometric Technology, Arab Muslim Minority, Bias and Discrimination, Privacy, Democratic Oversight

1. Introduction

Our bodies are the most immediate markers of identity, mediating both self-recognition and social perception (Postan, 2016). They carry the traces of lived experience, signal the passage of time, and disclose aspects of our existence—from vulnerability to mortality—that we may wish to conceal. Increasingly, these corporeal characteristics have been appropriated by states as mechanisms of verifica-

tion. Advances in biometric technology—systems that identify individuals through fingerprints, facial features, iris patterns, voiceprints, or behavioral markers such as gait—have transformed the body into a site of governance and surveillance (Jakubowska & Naranjo, 2020; Ziadah, 2021). From unlocking smartphones to border control and law enforcement, biometric systems are promoted for efficiency and security, yet they also encode and reproduce existing social hierarchies (Lawal, 2020; Lee et al., 2019; Jain, Ross, & Nandakumar, 2016; Grand View Research, 2023; De Hert & Bouchagiar, 2022).

For Arab Muslim minorities in the United States, these technologies operate at the intersection of visibility and vulnerability (Crenshaw, 1991; Munir, 2025; Roberts & Oosterom, 2025). Algorithmic misidentification, intensified scrutiny, and opaque security processes render these communities disproportionately exposed to risk, raising profound ethical and political concerns. Framed through Foucauldian biopolitics, Agamben's notion of bare life, and Mbembe's necropolitics, biometric governance emerges not merely as a technical system but as a mechanism through which bodies are classified, rendered legible, and subjected to differential power (Nedelcu & Soysüren, 2020). The body becomes simultaneously visible and precarious, recognized yet contingent, alive yet governed by data-driven authority. Despite this rich theoretical landscape, empirical engagement with the lived experience of Arab Muslim minorities under the specific 'digital border' regimes of the mid-2020s remains fragmented. While biopolitics and necropolitics provide the grammar for understanding state power, there is an urgent need to synthesize these frameworks with a concrete analysis of current U.S. regulatory gaps and algorithmic biases.

This study investigates the impact of biometric technology on Arab Muslim minorities in the US, asking: 1) To what extent do biometric infrastructures facilitate "digital epidermalization" and "failed mobility" for Arab Muslim minorities in the United States? 2) How does the transition toward "second-generation" behavioral biometrics institutionalize a "pre-crime" logic that disproportionately targets communities previously "stained" by post-9/11 scrutiny? 3) In the absence of federal regulation, how do "techno-authoritarian imaginaries" and "social sorting" mechanisms consolidate state power at the expense of minority democratic agency? By integrating critical theory with empirical analysis, this research seeks to illuminate the ethical, political, and social stakes of biometric governance, offering strategies to align technological innovation with democratic values.

2. Literature Review

2.1. Arab Muslim Minorities in the United States

In an academic context, the positioning of Arab Muslim minorities in the United States is defined by a unique intersection of ethno-linguistic heritage and religious affiliation. This dual identity distinguishes them both from Arab Christians, who share an ethnic bond but different ontological frameworks, and from the broader "Global Ummah," which encompasses diverse non-Arab populations

(Pew Research Center, 2017).

Sociologically, this group often exercises a sense of cultural stewardship. Because the Quran was revealed in Arabic, many Arab Muslims view themselves as the foundational custodians of Islamic tradition, creating a synthesis where language and theology are inextricably linked (Haddad, 2004). In the American diaspora, this manifests as a claim to cultural authority within religious spaces, as communities strive to preserve linguistic purity against the pressures of Western assimilation (Naber, 2012).

However, this identity has been profoundly reshaped by the post-9/11 landscape. Since the 2001 attacks, Arab Muslims have been systematically "stained" by the specter of terrorism, subjected to intensified state scrutiny and public suspicion. This hyper-surveillance has forced the community to navigate a dual existence: acting as internal guardians of cultural authenticity while simultaneously defending their right to belong in a society that frequently views their identity through a lens of inherent threat (Garvie et al., 2016; Ziadah, 2021).

2.2. Overview of Biometric Technology and Its Various Applications

Biometric technology refers to the use of unique biological characteristics to identify individuals (Hodwitz & King, 2025). It has become an increasingly prevalent tool in many aspects of modern society, from unlocking smartphones to border control and law enforcement. Biometric technologies include fingerprint scanning, facial recognition, voice recognition, and iris scanning, among others (Cuellar, To, & Mehrotra, 2025; Jain et al., 2016). Facial recognition technology, in particular, has been widely adopted in various industries, including law enforcement, financial services, and retail. For instance, the United Arab Emirates (UAE) government has implemented a facial recognition system to monitor and track the movement of its citizens and residents (Ziadah, 2021). In the United States, facial recognition technology has been used by law enforcement agencies to identify suspects and monitor public spaces (Garvie et al., 2016). While the potential benefits of biometric technology are clear, concerns have been raised about its implications for individual privacy and security (De Hert & Bouchagiar, 2022). Biometric data is often collected without individuals' informed consent, and there are no clear guidelines for how this data can be used, shared, or stored. Additionally, biometric data is not immutable and can be stolen or compromised, potentially leading to identity theft or other forms of fraud (Jain et al., 2016).

Moreover, biometric technology has the potential to perpetuate existing biases and discrimination against marginalized communities, including Arab Muslim minorities (Sutrop & Laas-Mikko, 2012). Studies have shown that facial recognition technology can be biased against people of color, leading to misidentification and false arrests (Buolamwini & Gebru, 2018). This can have serious implications for Arab Muslim minorities who may already face discrimination and racial profiling in their daily lives.

Given the increasing prevalence of biometric technology and its potential impact on Arab Muslim minorities, it is crucial to examine the various ways in which it can affect their lives and well-being. Through a nuanced understanding of the complexities of biometric technology, we can work towards a more just and equitable society that upholds the rights of all individuals, regardless of their race, ethnicity, or background.

2.2.1. Impact of Biometric Technology on Minority Communities

The scholarly discourse on biometric technologies reveals a persistent tension between the promise of "objective" security and the reality of systemic exclusion. While these systems are often marketed as neutral tools of efficiency, research consistently demonstrates that they function as engines of differential surveillance, particularly for minority communities (Sutrop & Laas-Mikko, 2012). The large-scale harvesting of biometric data—facial templates, iris scans, and fingerprints—represents more than a privacy risk; it constitutes a fundamental shift in how the state manages bodies (Bigo, 2014).

2.2.2. From Algorithmic Bias to Digital Epidermalization

At the technical level, the myth of algorithmic neutrality is debunked by the "accuracy gap." Empirical studies, most notably by Grother et al. (2019), have documented that facial recognition systems exhibit significantly higher error rates for specific racial and ethnic groups. For instance, NIST testing has shown that false-positive rates can be up to 100 times higher for West and East African and East Asian faces compared to White faces. These disparities are not merely technical glitches; they are a manifestation of what Browne (2010) identifies as "digital epidermalization." Epidermalization is a theoretical concept, most famously developed by Fanon (1952/2008), to describe how social meanings—especially race, inferiority, and power—become inscribed onto the body, as if they were part of the skin itself. In this framework, the technological "rendering" of the body re-inscribes race as a permanent risk factor, ensuring that the "stain" of post-9/11 suspicion is algorithmically immortalized for Arab Muslim minorities.

2.2.3. The Mechanisms of Social Sorting and Failed Mobility

The deployment of these technologies in law enforcement and border control—exemplified by the Traveler Verification Systems (TVS) deployed by U.S. Customs and Border Protection (CBP) as part of the Biometric Entry-Exit Program. It relies mainly on facial recognition technology to verify travelers' identities—creates an environment of "automated profiling" (Khan & Efthymiou, 2021). This infrastructure facilitates what Ziadah (2021) describes as "social sorting," a process where biometric IDs are weaponized to regulate ethno-racial hierarchies. By categorizing individuals based on data-driven "risk metrics," the state effectively justifies the "failed mobility" of those who fall outside Western secular norms (Al-Khateeb, 2021). This contributes to a broader "techno-authoritarian imaginary" where surveillance is used not just to catch criminals, but to manage "anomalous" populations (Schopmans & Tuncer Ebetürk, 2024).

2.2.4. The Pre-Crime Logic of Second-Generation Biometrics

The theoretical landscape is further complicated by the emergence of "second-generation" biometrics. As Sutrop and Laas-Mikko (2012) argue, the shift from verifying identity to predicting behavioral intent institutionalizes a dangerous "pre-crime" logic. By attempting to algorithmically "read" internal psychological states, the state subjects Arab Muslim communities—already under intense scrutiny—to a form of automated judgment that suppresses democratic agency and moral autonomy.

By situating biometric systems within this critical socio-technical framework, this study moves beyond a simple analysis of privacy. It investigates how these technologies intersect with the historical marginalization of Arab Muslim minorities, asking whether a system built on biased "Street-Level Algorithms" can ever truly align with the principles of equitable governance and civil liberties.

This study builds on these insights by examining the impact of biometric technologies on Arab Muslim minorities, emphasizing both the risks of bias and the potential for inclusive, equitable governance. By situating biometric systems within broader socio-technical and ethical frameworks, this research contributes to a nuanced understanding of how emerging technologies intersect with civil liberties, minority rights, and social equity.

3. Theoretical Framework: Biopolitics, CRT, and the Architecture of the Digital Border

The integration of biometric technologies into the modern state apparatus cannot be understood as a mere upgrade in administrative efficiency. Rather, it represents a fundamental shift in the relationship between the human body, sovereign power, and political belonging (Agamben, 1998). This study utilizes a multi-layered theoretical framework to analyze how these systems impact Arab Muslim minorities, moving from the normative protections of international law to the critical insights of biopolitical theory and Critical Race Theory (CRT).

3.1. The Normative Foundation and the Paradox of Recognition

Minority status in international law is not defined by simple arithmetic, but by the asymmetric power relations between a group and the state. As Francesco Capotorti established in his foundational 1977 (Capotorti, 1977) formulation, a minority is characterized by its "non-dominant" position and a collective "will to survive" through the preservation of distinct cultural markers (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2010). For decades, Arab Muslim communities in the United States navigated a legal "gray zone," classified as "White" for census purposes—a status that provided a surface-level promise of inclusion while facilitating a form of statistical erasure (Pew Research Center, 2017).

Alsharif (2024) notes that the 2024 implementation of the Middle Eastern or North African (MENA) census category marked a pivotal victory for visibility, allowing for targeted civil rights enforcement and equitable redistricting. How-

ever, this visibility is inherently paradoxical. As these communities become more legible to the law, they simultaneously become "hyper-legible" to a security state. This visibility does not always translate into recognition; instead, it often facilitates exposure to a "digital border"—a pervasive infrastructure of biometric surveillance and "continuous vetting" that encodes religious and ethnic identity as a permanent risk factor.

3.2. Critical Race Theory and the Algorithmic Reproduction of Inequality

To understand why biometric systems disproportionately flag certain bodies, this research draws on Critical Race Theory (CRT). CRT posits that racism is not merely an episodic occurrence of individual prejudice but is systemic and embedded within the very structures of law and technology (Delgado & Stefancic, 2017). In the context of biometrics, this means that "neutral" algorithms inherit the racial hierarchies of their training data.

As Buolamwini and Gebru (2018) demonstrated, facial recognition systems exhibit significantly higher error rates for darker skin tones and can be confounded by religious attire like the hijab. Within a CRT framework, these are not "glitches" to be fixed by better code; they are technological inscriptions of historical marginalization. For the Arab Muslim subject, a recurring "false positive" or a "black box" security flag is an algorithmic manifestation of a pre-existing field of suspicion, transforming a technical failure into a lived vulnerability.

3.3. Foucauldian Biopolitics and the Governance of "Bare Life"

In international law and critical theory, the most profound implications of biometric governance are revealed through Michel Foucault's concept of biopolitics—the technologies through which the state manages and optimizes populations by making the body a site of political intervention (Foucault, 1977: p. 170). Biometrics go beyond mere identification; they "administer" the body, rendering it measurable and comparable within vast databases. For securitized communities, this overlays a "genealogy of power" where the state does not repress through overt force, but through constant, automated observation and categorization.

This biopolitical management often pushes the minority subject into what Giorgio Agamben describes as the "state of exception" or "bare life" (Agamben, 1998: p. 83). In these zones—most visible at border crossings and in opaque "No-Fly" lists—legal recognition is suspended and rights become contingent upon the scan of a retina or a fingerprint. When an individual is flagged by a proprietary algorithm with no path for appeal, they are reduced to a biological data point, existing simultaneously inside the law's reach but outside its protection (Agamben, 1998: p. 171).

3.4. Necropolitics and the Distribution of Precarity

Achille Mbembe explains the necropower "as the capacity to control the life and

death of citizens, because sovereignty has the power to exclude a community from the vast population, leaving them in a status of social death" (Zhao, 2022). Mbembe's (2019) concept of necropolitics illuminates the ultimate stakes of this technological expansion. In authoritarian or highly securitized contexts, biometric databases become tools for administering precarity. The power to track, immobilize, or selectively exclude specific populations allows the state to decide whose movement is "liquid" and whose is "blocked." For Arab Muslim minorities, the convergence of biopolitical management and necropolitical exposure produces a precarious form of belonging, where security is a privilege and suspicion is permanently encoded into their digital double.

A critical engagement with biometric technology must move beyond questions of technical efficiency. It must confront the ethical reality of governing through the body. Without a philosophical commitment to resisting these automated hierarchies, biometric innovation threatens to normalize a political order where justice is permanently subordinated to the imperatives of algorithmic security.

4. Methodology

The present study employs a qualitative research approach, utilizing a case study design to facilitate an in-depth examination of the impact of biometric technology on Arab Muslim minorities in the United States. A case study methodology was chosen for its capacity to generate rich, contextualized insights into complex socio-technical phenomena and to illuminate the interactions between technology, social structures, and minority rights (Yin, 2018).

Data collection draws upon multiple sources to ensure methodological rigor and strengthen the credibility of the findings. These sources include a comprehensive review of scholarly literature (n = 6) and semi-structured interviews are conducted with (N = 6) experts in biometric technologies (n = 2), civil rights (n = 2), and minority rights advocacy (n = 2). Interviews are carried out either in person or via secure video conferencing platforms, depending on participant availability, and follow a structured protocol designed to elicit detailed, contextually grounded responses.

Data analysis integrates thematic analysis for literature and document review with a grounded theory approach for interview data, enabling both the identification of emergent patterns and the development of theoretically informed interpretations (Braun & Clarke, 2006; Charmaz, 2014). NVivo software is employed for systematic coding, organization, and retrieval, ensuring rigorous management of the qualitative dataset. This multi-method approach allows for a comprehensive and nuanced understanding of the complex relationship between biometric technologies and minority rights, while promoting analytical rigor and transparency.

Ethical considerations are central to the study design. All participants provided informed consent, and strict measures were taken to maintain confidentiality and protect data. Ethical approval was obtained from the relevant institutional review

boards prior to the commencement of data collection. Several limitations are acknowledged. First, data concerning biometric technologies and Arab Muslim minorities are limited, reflecting the sensitivity of the topic and potential reluctance among participants to share personal experiences. Second, the literature review is restricted to English-language publications from the past ten years, which may exclude relevant findings from non-English or older sources. Third, potential bias in the selection of data sources and analytical procedures is recognized; this is mitigated through methodological triangulation, the inclusion of diverse data sources, and adherence to systematic coding and analytic protocols.

For the literature review, searches were conducted across databases including Google Scholar, JSTOR, and ProQuest using a combination of keywords, including: "biometric technology AND Arab Muslim minorities," "biometric technology AND privacy AND Arab Muslim minorities," "biometric technology AND security AND Arab Muslim minorities," "biometric technology AND bias AND Arab Muslim minorities," "biometric technology AND discrimination AND Arab Muslim minorities," and "biometric technology AND democracy AND Arab Muslim minorities." Additional related terms were also incorporated to maximize coverage. Articles were screened for relevance based on the research objectives and inclusion criteria, and findings were synthesized to inform the analytical framework of the study. By employing a rigorous, multi-source, and ethically grounded research design, this study aims to generate reliable, contextually sensitive insights into the socio-technical and ethical dimensions of biometric technology as they relate to the Arab Muslim minority in the U.S., contributing to both scholarly knowledge and policy discourse.

Table 1. Inclusion and exclusion criteria of eligible works.

Inclusion	Exclusion
Published between 2010-2025	Published prior to 2010
Published in English	Published in a language other than English
Primary research articles pertaining to the deployment of biometric technologies	Non-primary research articles (e.g., editorials, opinion pieces)
Related Biometric Technologies and Racial Bias	Not related to Biometric Technologies and Racial Bias

As Table 1 illustrates, we limited our search to articles published in English within the last 15 years to ensure the most up-to-date research was included. After applying the relevant filters and refining our search terms, we reviewed and selected sources that were relevant to our research question and objectives. We read the abstracts or summaries of each source to determine their relevance and importance to our study.

5. Results

The mixed-method analysis indicates that biometric technologies systematically

reproduce and exacerbate social inequities, disproportionately impacting Arab Muslim minorities in the United States. Drawing on critical race theory and Foucault's notion of surveillance as a mechanism of power/knowledge, these technologies operate not merely as neutral technical tools but as instruments that embed existing socio-political hierarchies within ostensibly objective systems (Foucault, 1977; Crenshaw, 1991).

The results demonstrate that the deployment of biometric systems functions as a mechanism of differential surveillance. This scrutiny is a direct legacy of the post-9/11 security landscape, where Arab and Muslim identities became systematically "stained" by a persistent association with threat. This environment has fostered what Browne (2010) identifies as "digital epidermalization," where the historical practice of categorizing bodies based on race is modernized through data.1 By "rendering" race through biometric markers, the state effectively automates suspicion, turning the body itself into a site of constant inquiry and commodifying it as a digital "brand."

This automation is most visible in the "accuracy gap" identified throughout the literature and confirmed by expert interviews. While facial recognition technology (FRT) performs with near-perfect accuracy for white males—with error rates as low as 0.8%—the failure rate for darker-skinned individuals can exceed 34%, particularly for those with non-Western morphologies or those wearing religious attire such as the hijab (Buolamwini & Gebru, 2018). Expert interviews (n = 6) corroborated these findings, with participants across the technology and civil rights sectors noting that such technical failures translate into a lived reality of "failed mobility" (Al-Khateeb, 2021). In this context, the "rhetorical screening" marketed as efficient security actually functions as a digital wall, trapping refugees and Arab travelers in loops of secondary screenings and "high-risk" flagging. As Khan and Efthymiou (2021) observe, systems like the Traveler Verification System (TVS) rely on "Street-Level Algorithms" that suffer from significant performance drops in real-world conditions, further facilitating "social sorting" (Ziadah, 2021).

5.1. Behavioral Prediction and Techno-Authoritarianism

The data reveal an escalating danger in the transition toward "second-generation" biometrics (Sutrop & Laas-Mikko, 2012), which shifts the focus from identity verification to behavioral prediction. By attempting to "read" intent or psychological states, these systems introduce a "pre-crime" logic that is deeply susceptible to cultural misinterpretation, violating the moral autonomy of the individual. Experts in minority rights advocacy highlighted that for a community already under intense scrutiny, this reflects a broader "techno-authoritarian imaginary" (Schopmans & Tuncer Ebetürk, 2024). In this landscape, the use of evolving, non-transparent algorithms, allows for a form of democratic regression where the inaccuracy of the technology is not merely a "glitch," but a systemic feature that suppresses the political agency of minorities.

5.2. The Algorithmic Border: Biometric Governance and the Production of Racialized Suspicion

The scholarly consensus across these six works (Table 2) reveals that biometric and facial recognition technologies (FRT) are far from neutral tools of efficiency; instead, they function as sophisticated engines of social sorting and racialized exclusion. At the core of this failure is what Browne (2010) identifies as "digital epidermalization," where the historical practice of branding and categorizing bodies based on race is updated for the digital age. When algorithms are trained on Western-centric datasets, non-Western facial morphologies and darker skin tones are often "misread" or rendered invisible. Empirical data support this: while error rates for lighter-skinned males are as low as 0.8%, they can soar to over 34% for darker-skinned women (Buolamwini & Gebru, 2018), leading to a form of technical erasure that systematically denies marginalized individuals access to social goods.

Table 2. Comparative framework of biometric vulnerabilities and systemic inefficiencies across scholarly perspectives.

Reference	Surveillance Practices	Data Misuse & Risks	Privacy & Accuracy Issues	Impact on Minorities & Individuals
Browne (2010)	Digital Epidermalization: Use of biometrics to "render" race through data.	Transformation of the body into a "stamp of commodity" similar to branding.	Systems fail to "read" non-white bodies, leading to technical erasure.	Epistemic violence: Bodies that don't fit the "norm" are denied mobility and housing.
Sutrop & Laas-Mikko (2012)	Second-Gen Biometrics: Moving from identity to behavioral prediction.	Function creep: data collected for security is used for "intent" analysis.	Violation of moral autonomy; individuals lose control over their "digital self."	Predictive Policing: Minorities are disproportionately flagged as "suspicious" by intent-logic.
Al-Khateeb (2021)	Rhetorical Screening: Biometrics marketed as "efficient" but used as digital walls.	Failed promises of mobility; data becomes a tool for entrapment.	The "certainty" of the digital scan creates a false narrative of the individual.	Refugee Exclusion: Displaced persons are trapped in cycles of suspicion and "immobility."
Khan & Efthymiou (2021)	Airport Biometric Entry/Exit: Integration of TVS (Traveler Verification System).	Centralized databases create "single points of failure" for data breaches.	Low matching rates and reliance on "Street-Level Algorithms" instead of humans.	Automated Profiling: Travelers are sorted by "risk" metrics that favor Western norms.
Ziadah (2021)	Social Sorting in UAE: Using Biometric IDs to regulate ethno-racial hierarchies.	Integration of health/insurance data into state surveillance registries.	Claims of "race-neutrality" mask the hardening of ethno-racial tiers.	Labor Stratification: Migrant workers are "sorted" and monitored to maintain state control.
Schopmans & Tuncer Ebetürk (2024)	Techno-Authoritarian Imaginaries: Anticipatory use of FRT for social control.	High potential for "democratic regression" via public/private data sharing.	Use of evolving, opaque algorithms with minimal democratic oversight.	Marginalized Resistance: Civil society views these as tools for "racial and gendered purging."

This technical inaccuracy creates a "failed promise of mobility," a concept Al-Khateeb (2021) applies specifically to the refugee experience. For Arab Muslim populations, the border becomes a rhetorical trap: while the technology is sold as a means of "streamlining" travel, the reality is a cycle of false positives and algo-

rithmic suspicion that halts movement rather than facilitating it. Khan and Efthymiou (2021) further emphasize that these airport systems rely on "Street-Level Algorithms" that suffer from significant performance drops in real-world conditions, such as varied lighting or the presence of religious headwear like the hijab. This disproportionately flags travelers from the Global South as "high-risk" anomalies due to these inherent biases.

The danger escalates with the transition to "second-generation" biometrics, which Sutrop and Laas-Mikko (2012) warn is shifting from mere identity verification to behavioral prediction. By attempting to "read" intent or psychological states, these systems introduce a "pre-crime" logic that is deeply susceptible to cultural misinterpretation. For a community already "stained" by post-9/11 stigmas, this translates into intensified policing of everyday behaviors that an algorithm—designed with a Western secular "default"—marks as suspicious.

Furthermore, these technologies are frequently weaponized to maintain existing power hierarchies. Ziadah (2021) illustrates how biometric IDs are used in the UAE to enforce ethno-racial labor stratification, proving that data is rarely just data—it is a tool for "sorting" populations into tiers of citizenship and rights. This reflects the broader "techno-authoritarian imaginary" described by Schopmans and Tuncer Ebetürk (2024), where the opaque nature of facial recognition allows for a form of democratic regression. In this landscape, the inaccuracy of the technology is not merely a "glitch"; it is a systemic feature that suppresses the political agency of minorities by making public spaces a site of constant, unpredictable scrutiny.

5.3. The Architecture of Targeted Scrutiny: Biometric Governance and Racialized Suspicion

The deployment of biometric systems in public spaces and at border crossings functions as a mechanism of differential surveillance—one that weighs disproportionately on Arab and Muslim communities (Garvie et al., 2016). Framed through Lyon's (2017) analysis of the "surveillance society," these practices are far from neutral technical measures; they are manifestations of a deep-seated power asymmetry. By subjecting specific minority groups to intensified monitoring, these systems do more than just collect data—they entrench social stigmas and institutionalize what Foucault (1980) described as a form of epistemic marginalization.

Critically, this scrutiny is a direct legacy of the post-9/11 security landscape, where Arab and Muslim identities became systematically "stained" by a persistent association with threat. This environment has birthed what Browne (2010) identifies as "digital epidermalization," where the historical practice of branding and categorizing bodies based on race is modernized through data. By "rendering" race through biometric markers, the state effectively automates suspicion, turning the body itself into a site of constant inquiry and commodifying it as a digital "brand" for surveillance.

This automation is most visible in the "accuracy gap" inherent in these systems. While facial recognition technology (FRT) performs with near-perfect accuracy

for white males—with error rates as low as 0.8%—the failure rate for darker-skinned individuals can exceed 34%, particularly for those with non-Western morphologies or those wearing religious attire like the hijab (Buolamwini & Gebru, 2018). This technical failure translates into a lived reality of "failed mobility" (Al-Khateeb, 2021), where the "rhetorical screening" marketed as efficient security actually functions as a digital wall, trapping refugees and Arab travelers in loops of secondary screenings and "high-risk" flagging.

As Khan and Efthymiou (2021) note, systems like the Traveler Verification System (TVS) at airports rely on "Street-Level Algorithms" that suffer from significant performance drops in real-world conditions. This facilitates a form of "social sorting" (Ziadah, 2021) where travelers are categorized by "risk" metrics that inherently favor Western norms. In certain contexts, such as the UAE, these biometric IDs are weaponized to manage and enforce ethno-racial labor hierarchies, proving that data is frequently used to maintain tiers of citizenship and exclude those who deviate from the state-defined "norm."

The danger escalates with the transition toward "second-generation" biometrics (Sutrop & Laas-Mikko, 2012), which shifts the focus from identity verification to behavioral prediction. By attempting to "read" intent or psychological states, these systems introduce a "pre-crime" logic that is deeply susceptible to cultural misinterpretation, violating the moral autonomy of the individual. This reflects a broader "techno-authoritarian imaginary" (Schopmans & Tuncer Ebetürk, 2024), where the use of evolving, non-transparent algorithms without public consent allows for a form of democratic regression. In this landscape, the inaccuracy of the technology is not merely a "glitch"; it is a systemic feature that suppresses the political agency of minorities by making public spaces a site of constant, unpredictable scrutiny.

Given this reality, the argument from civil rights advocates is clear: the impact of biometric surveillance is too pervasive and its biases too systemic to be "fixed" through minor policy adjustments. To protect fundamental rights and halt the further marginalization of populations who have been under a microscope for decades, a total prohibition on biometric surveillance in public spaces is increasingly viewed as the only viable path forward.

5.4. Data Misuse Risks: From Security to Social Engineering

Biometric databases, when governed by opaque institutional authorities, function as high-stakes repositories for potential misuse. The results of this study, supported by the scholarly consensus of the six primary articles and the testimonies of interviewed experts, suggest that this data is rarely isolated. As Ziadah (2021) and Schopmans and Ebetürk (2024) illustrate, biometric information is frequently merged across health, insurance, and labor registries—a practice the interviewed civil rights advocates (n = 2) described as a "digital dragnet." This interoperability is used to enforce ethno-racial hierarchies, particularly against Arab Muslim populations.

In both democratic and authoritarian contexts, this "function creep" allows data collected under the guise of "national security" to be repurposed for behavioral management. Interviewed experts in biometric technologies (n = 2) noted that once a body is digitized, it becomes what Browne (2010) calls a "commodity," or a permanent, searchable "brand." This aligns with Nedelcu and Soysüren (2020), who argue that such data-leveraging constrains individual freedoms and marginalizes vulnerable populations.

The shift toward "second-generation" biometrics, as warned by Sutrop and Laas-Mikko (2012), represents the most significant misuse risk. By repurposing security data to analyze "intent," institutions transition from monitoring who a person is to predicting what they might do. Minority rights advocates (n = 2) emphasized during interviews that this "pre-crime" logic falls heaviest on Arab Muslim communities, whose cultural and religious expressions are often misinterpreted by the state as indicators of risk.

Viewed through Foucault's (1980) lens on the disciplinary functions of documentation, these systems act as mechanisms of governance that translate technical observation into total socio-political control. The "certainty" of the digital scan—critiqued by Al-Khateeb (2021)—replaces the complex reality of the individual with a static narrative of suspicion. Furthermore, as Khan and Efthymiou (2021) highlight, the centralization of these databases creates "single points of failure," where the misuse of data is not just an institutional choice but a systemic vulnerability.

Ultimately, the consensus among both the literature and the interviewed experts is that the "neutral" veneer of these databases masks their utility as tools for "racial and gendered purging" in public spaces (Schopmans & Ebetürk, 2024). This underscores a reality where the misuse of biometric data is not an anomaly, but a fundamental capability of the system's design.

5.5. Privacy Violations: The Regulatory Vacuum and the Erosion of Consent

The findings from this study reveal that privacy violations in biometric deployment are not merely accidental; they are systemic. Expert interviews (n = 6) consistently highlighted that the collection of biometric data occurs almost entirely without informed consent, facilitating a state of prolonged, involuntary tracking. This aligns with the "techno-authoritarian imaginaries" described by Schopmans and Tuncer Ebetürk (2024), where the public is subjected to evolving, non-transparent algorithms without legislative or public oversight.

The interviewed civil rights advocates (n = 2) emphasized that this lack of consent effectively strips individuals of their "contextual integrity" (Nissenbaum, 2010). When an Arab Muslim woman's facial data is captured in a public square or at a border, it is often repurposed across contexts she never authorized. This "function creep" is central to the shift toward "second-generation" biometrics identified by Sutrop and Laas-Mikko (2012). As these systems move from verifying identity to predicting behavior, they violate the moral autonomy of the indi-

vidual, as the subject loses control over their own "digital persona."

Technically, these violations are compounded by the "Street-Level Algorithms" critiqued by Khan and Efthymiou (2021). During interviews, experts in biometric technologies (n = 2) noted that these systems frequently produce "false negatives" and matching errors for non-Western morphologies. In a regulatory vacuum, these errors lead to unwarranted stops and searches. As the United States Commission on Civil Rights (2024) points out, no federal laws currently protect civil rights in the government's use of FRT. Statutes like the Privacy Act of 1974 are fundamentally ill-equipped to handle the "digital epidermalization" (Browne, 2010) that occurs when race is coded as a permanent risk factor.

Furthermore, the "rhetorical screening" used at borders, as analyzed by Al-Khateeb (2021), creates a false sense of security that justifies the suspension of privacy rights. Minority rights advocates (n = 2) noted that for Arab Muslim populations, the border is a site where privacy is completely subsumed by the "logic of the database." This echoes Ziadah's (2021) findings on "social sorting," where the claim of "technical neutrality" is used to mask the hardening of racial tiers and the systemic violation of the right to anonymity in public spaces.

6. Discussion

This study demonstrates that biometric technologies do not merely mirror pre-existing social inequalities; they actively produce, stabilize, and legitimize them through automated regimes of surveillance that disproportionately target Arab Muslim minorities in the United States. When examined through the theoretical framework developed in this research, biometric systems emerge as a *dispositif* in the Foucauldian sense—an historically situated constellation of discourses, technologies, institutions, and security rationalities that collectively render certain bodies governable, legible, and persistently suspect (Foucault, 1977, 1980). Rather than functioning as neutral instruments of identification, biometric technologies materialize post-9/11 security logics into algorithmic infrastructures that subtly but decisively reconfigure political belonging—reshaping who is presumed trustworthy, who is rendered mobile, and who remains perpetually visible under suspicion.

The findings offer strong empirical support for Browne's (2010) concept of digital epidermalization, revealing how racialized and religious difference is encoded directly into data architectures. The documented accuracy gap—most notably the 34.7% error rate affecting darker-skinned individuals—cannot be dismissed as an accidental or transitional technical limitation. Instead, it exemplifies what Benjamin (2019) identifies as discriminatory design: systems that reproduce racial hierarchies precisely through claims of neutrality, efficiency, and objectivity. In this configuration, algorithmic error does not signal system failure; it operates as a mode of governance. When Arab Muslim bodies are disproportionately misrecognized, the resulting frictions—secondary screenings, delays, repeated verification failures—function as automated sanctions that normalize suspicion within the ordinary experience of movement.

This logic resonates powerfully with Fanon's (1952/2008) notion of the epidermalization of inferiority, now recalibrated for the digital era. Where colonial regimes once inscribed racial difference onto the skin through discourse, surveillance, and coercion, contemporary biometric systems translate that inscription into data points, risk scores, and probabilistic classifications. The body is no longer merely seen; it is computed, transformed into a searchable and extractable surface where cultural and religious difference is continuously interpreted as a signal of threat. Biometric governance, then, does not simply observe racialized subjects—it actively produces them as algorithmic objects of suspicion.

The study further demonstrates that these effects are sustained through what Al-Khateeb (2021) conceptualizes as rhetorical screening. While biometric surveillance is publicly framed as a technology of facilitation—promising efficiency, safety, and seamless mobility—the empirical evidence reveals its operation as a technology of exclusion (Solove, 2006). For Arab Muslim travelers, the promise of frictionless movement is repeatedly displaced by recursive cycles of algorithmic scrutiny—what this study conceptualizes as failed mobility. The deployment of so-called "street-level algorithms" within systems such as the Traveler Verification System (TVS) intensifies these disparities. As Khan and Efthymiou (2021) demonstrate, performance degradation in real-world environments disproportionately affects bodies and practices that diverge from Western secular norms, including religious dress such as the hijab. In this configuration, the border no longer functions primarily as a legal threshold but as an algorithmic choke point, reducing the Arab Muslim subject to what Agamben (1998) terms bare life: included in the database only insofar as they remain excluded from full political and spatial belonging.

The shift toward second-generation biometrics marks a further escalation of this governing logic. As the findings indicate, systems designed to infer intent, affect, or behavioral risk signal a transition from identification to anticipation. This preemptive orientation collapses the distinction between identity and action, rendering everyday gestures, facial expressions, and religious affect legible as speculative indicators of threat. Such systems substantiate the ethical concerns raised by Sutrop and Laas-Mikko (2012), particularly regarding the erosion of moral autonomy and the normalization of predictive judgment in the absence of due process. Within an already racialized security landscape, behavioral biometrics intensify vulnerability by institutionalizing cultural misinterpretation as algorithmic fact.

These developments must be situated within what Schopmans and Tuncer Ebetürk (2024) describe as a techno-authoritarian imaginary, in which opaque algorithms, cross-sector data integration, and weak regulatory oversight converge to enable democratic regression. The convergence of biometric data with health, labor, and insurance registries exemplifies Ziadah's (2021) analysis of social sorting, illustrating how surveillance infrastructures are increasingly repurposed to regulate populations across multiple domains of life. As the findings make clear, this form of function creep is not incidental but structural: once digitized, the body becomes permanently governable. In Benjamin's (2019) terms, biometric systems thus operate as racializing assemblages that automate inequality while

concealing accountability behind technical complexity.

Crucially, this study challenges reformist assumptions that biometric bias can be resolved through incremental technical improvements or limited policy interventions. The evidence suggests that inaccuracy, opacity, and disproportionate harm are not peripheral defects but constitutive features of biometric governance as currently deployed. The absence of comprehensive federal regulation in the United States further entrenches these harms, enabling biometric surveillance to expand without meaningful accountability or informed consent (United States Commission on Civil Rights, 2024). As a result, privacy violations become normalized, contextual integrity erodes, and public space is transformed into a site of involuntary data extraction—particularly for populations already marked as suspect.

Taken together, this study advances scholarship on algorithmic governance by foregrounding the embodied, affective, and lived consequences of biometric surveillance for Arab Muslim minorities within a Western security context. By placing Foucauldian analyses of power in dialogue with Browne's theorization of racialized surveillance and Benjamin's critique of discriminatory design, the findings demonstrate that biometric technologies reproduce racialized power not only through representation, but through infrastructure itself. These systems do not merely fail marginalized populations; they succeed in governing them differentially.

Ultimately, reconciling security governance with democratic pluralism requires more than transparency initiatives or marginal gains in accuracy. It demands a fundamental rethinking of whether biometric surveillance—anchored in logics of prediction, commodification, and suspicion—can ever be compatible with substantive equality. Without such a reorientation, biometric technologies will continue to function not simply as tools of observation, but as infrastructures that actively reorganize social life along enduring lines of race, religion, and power.

6.1. The Roadmap for Democratic Oversight

Democratic oversight is the essential counter-weight to the "state of exception" created by biometric governance. It functions as the mechanism through which the "bare life" of the data point is restored to the "political life" of the citizen. Based on the findings of this study, the following three strategies are proposed to ensure equity and inclusivity (**Table 3**):

Table 3. Strategic recommendations for democratic oversight of biometric systems.

Strategy	Mechanism of Implementation	Specific Impact for Arab Muslim Minorities	Ethical Goal
Algorithmic Accountability	Third-party audits and "human-in-the-loop" review protocols.	Reduces misidentification caused by religious attire (hijab) and non-Western phenotypes.	Technical Justice: Mitigates "technological redlining."
Legislative Safeguards	Judicial warrants and "disparate impact" legal standing.	Protects places of worship from mass data harvesting; enables lawsuits for bias.	Juridical Protection: Restores Fourth Amendment rights.
Community Governance	Civilian oversight boards and "necropolitical" redlines.	Reclassifies cultural preservation as a right rather than a security "risk factor."	Political Agency: Shifts from "bare life" back to citizenship.

6.1.1. Algorithmic Accountability and the "Black Box" Challenge

Because biometric systems are frequently proprietary, they operate as a "black box" that shields discriminatory outcomes behind the veil of trade secrets, necessitating a mandate for technical transparency through democratic oversight. This transparency should be operationalized first through independent pre-deployment auditing, requiring federal regulations to mandate that any biometric system utilized by the Department of Homeland Security or law enforcement undergo third-party testing for "demographic differential." Such a protocol ensures that the systemic biases identified in the foundational findings of Buolamwini and Gebru (2018)—which demonstrated significant accuracy disparities for darker and non-Western phenotypes—are rigorously addressed before a system is deployed against the general public.

Furthermore, to prevent the dehumanizing reduction of identity to a mere biological data point, the right to human intervention must be codified. This ensures that any "flag" generated by an automated system is subjected to a mandatory, documented review by a human official. Crucially, these officials must be trained to recognize specific cultural and religious occlusions, such as the hijab, which frequently confound algorithmic models and lead to disproportionate false positives for Arab Muslim populations. By integrating these technical and human safeguards, the governance of biometric technology can move toward a model that prioritizes individual dignity over uncritical machine efficiency.

6.1.2. Legislative Safeguards: Bridging the "Regulatory Vacuum"

The current "regulatory void" identified by the United States Commission on Civil Rights (2024) must be filled by a comprehensive federal statute that specifically addresses the unique challenges posed by biometric identifiers. Central to this legislative effort is the restoration of the Fourth Amendment in the digital age, which requires that "real-time" facial recognition in public spaces be prohibited except under a judicial warrant based on probable cause. Such a mandate is essential to prevent the "indiscriminate data harvesting" that currently targets Arab Muslim community centers and places of worship, effectively turning communal spaces into sites of perpetual surveillance.

Furthermore, the 2024 Middle Eastern or North African (MENA) census category shift should be leveraged as a robust legal tool to protect these communities. By officially recognizing Arab Muslims as a distinct minority, the law can facilitate "disparate impact" lawsuits against agencies whose biometric tools consistently produce false positives for this demographic. Codifying this right to redress transforms the MENA category from a mere administrative label into a powerful instrument for accountability, allowing individuals to challenge the systemic biases that have historically rendered their belonging conditional.

6.1.3. Community-Led Governance and "Counter-Surveillance"

Aligning with the Foucauldian principle that "where there is power, there is resistance," democratic oversight must integrate the voices of those most impacted

by surveillance into the very structure of governance (Matulionyte & Zalnieriute, 2024). This shift is operationalized through the creation of civilian oversight boards, which ensure that communities historically subjected to intense securitization—particularly Arab and Muslim Americans—have a seated role in the procurement and policy-setting stages of biometric technology. By institutionalizing this participation, the state acknowledges that the "will to survive" and the desire for cultural preservation are not biological risk factors to be managed by an algorithm, but are fundamental democratic rights.

To further protect these rights, democratic frameworks must establish "redlines" that designate certain applications of biometrics as fundamentally incompatible with a democratic order. These redlines identify practices such as religious profiling or the tracking of legal political protests as "necropolitical" boundary crossings that must be banned entirely rather than merely regulated. By defining these limits, community-led governance moves the focus from making surveillance more accurate to ensuring that technology is not used as an infrastructure of domination, thereby upholding the principles of justice and inclusivity within the digital landscape.

7. Conclusion

This research has explored the profound and often invisible friction at the intersection of biometric innovation and the lived reality of Arab Muslim minorities in the United States. While these technologies are presented as neutral instruments of security, the findings of this study suggest they act as a "digital border" that internalizes and automates historical patterns of suspicion. For a community whose identity is often caught between a desire for cultural preservation and the pressures of securitization, the digitizing of the body represents a new frontier of biopolitical management—one where a retinal scan or a facial template can become a mechanism of "bare life," suspending legal protections in the name of algorithmic efficiency.

The study demonstrates that the "technical glitches" often cited in biometric failures—specifically the high error rates for Middle Eastern phenotypes and the "occlusion" issues related to religious attire like the hijab—are not merely engineering hurdles. Rather, they are manifestations of "technological redlining," where systemic biases are baked into training datasets and institutional deployment strategies. By integrating the critical frameworks of Foucault, Agamben, and Mbembe, this research reveals how these systems do more than identify; they categorize, sort, and eventually govern populations (Caputo, 2014). The current regulatory vacuum at the federal level exacerbates this, leaving Arab Muslim communities hyper-visible to the state yet statistically erased from protective legislation.

Ultimately, the future of biometric governance must be a democratic project, not just a technical one (Matulionyte & Zalnieriute, 2024). To prevent the entrenchment of a permanent digital hierarchy, policymakers must move beyond

procedural "fixes" toward a model of robust democratic oversight that prioritizes transparency, accountability, and the right to human intervention. This requires a fundamental shift: moving from a political order where bodies are sorted before they are heard, to one where the dignity of the human subject precedes the data point. If the United States is to remain a true pluralistic democracy, its technological systems must learn to recognize the citizen before they scan the suspect.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the research, authorship, and/or publication of this work.

References

Agamben, G. (1998). *Homo Sacer: Sovereign Power and Bare Life* (D. Heller-Roazen, Trans.). Stanford University Press.

Al-Khateeb, M. T. (2021). Toward a Rhetorical Account of Refugee Encounters: Biometric Screening Technologies and Failed Promises of Mobility. *Rhetoric Society Quarterly, 51,* 15-26. https://doi.org/10.1080/02773945.2020.1841276

Alsharif, M. (2024). *"We Exist": New Middle Eastern or North African Census Category Helps Community Members Feel Seen*. NBC News. https://www.resource.dnsafrica.org/2024/04/03/we-exist-new-middle-eastern-or-north-african-census-category-helps-community-members-feel-seen-nbc-news/

Benjamin, R. (2019). *Race after Technology: Abolitionist Tools for the New Jim Code*. Polity Press.

Bigo, D. (2014). The (In)securitization Practices of the Three Universes of EU Border Control: Military/Navy—Border Guards/Police—Database Analysts. *Security Dialogue, 45,* 209-225. https://doi.org/10.1177/0967010614530459

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology, 3,* 77-101. https://doi.org/10.1191/1478088706qp063oa

Browne, S. (2010). Digital Epidermalization: Race, Identity and Biometrics. *Critical Sociology, 36,* 131-150. https://doi.org/10.1177/0896920509347144

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81,* 77-91.

Capotorti, F. (1977). *Study on the Rights of Persons Belonging to Ethnic, Religious and Linguistic Minorities (UN Doc. E/CN.4/Sub.2/384/Rev.1)*. United Nations.

Caputo, A. C. (2014). Physical Security Integration. In A. C. Caputo (Ed.), *Digital Video Surveillance and Security* (2nd ed., pp. 363-393). Elsevier. https://doi.org/10.1016/b978-0-12-420042-5.00011-3

Charmaz, K. (2014). *Constructing Grounded Theory* (2nd ed.). Sage Publications.

Crenshaw, K. (1991). Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review, 43,* 1241-1299. https://doi.org/10.2307/1229039

Cuellar, M., To, H. K., & Mehrotra, A. (2025). *Accuracy and Fairness of Facial Recognition Technology in Low Quality Police Images: An Experiment with Synthetic Faces (CoRR abs/2505.14320)*. https://arxiv.org/abs/2505.14320

De Hert, P., & Bouchagiar, G. (2022). Visual and Biometric Surveillance in the EU. Saying

"No" to Mass Surveillance Practices? *Information Polity, 27,* 193-217. https://doi.org/10.3233/ip-211525

Delgado, R., & Stefancic, J. (2017). *Critical Race Theory: An Introduction* (3rd ed.). New York University Press.

Fanon, F. (1952/2008). *Black Skin, White Masks* (R. Philcox, Trans.). Grove Press. (Original Work Published 1952)

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Pantheon Books.

Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*. Pantheon Books.

Garvie, C., Bedoya, A., & Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Center on Privacy & Technology, Georgetown Law. https://www.perpetuallineup.org/

Grand View Research (2023). *Biometric Technology Market Size, Share & Trends Analysis Report by Component, by Offering, by Authentication Type, by Application, by End-Use, by Region, and Segment Forecasts (2023-2030) (Report No. 978-1-68038-299-0).* https://www.grandviewresearch.com/industry-analysis/biometrics-industry

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (NIST Interagency/Internal Report 8280)*. National Institute of Standards and Technology.

Haddad, Y. Y. (2004). *The Muslims of America*. Oxford University Press.

Hodwitz, O., & King, S. (2025). Biometrics. In J. R. Vacca (Ed.), *Computer and Information Security Handbook* (4th ed., pp. 1161-1176). Elsevier. https://doi.org/10.1016/b978-0-443-13223-0.00072-2

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letters, 79,* 80-105. https://doi.org/10.1016/j.patrec.2015.12.013

Jakubowska, E., & Naranjo, D. (2020). *Ban Biometric Mass Surveillance: A Set of Fundamental Rights Demands for the European Commission and EU Member States*. European Digital Rights (EDRi). https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Khan, N., & Efthymiou, M. (2021). The Use of Biometric Technology at Airports: The Case of Customs and Border Protection (CBP). *International Journal of Information Management Data Insights, 1,* Article ID: 100049. https://doi.org/10.1016/j.jjimei.2021.100049

Lawal, G. S. (2020). *Ethical and Legal Implications of Biometric Data Collection in Digital Health Services (Preprint)*.

Lee, N., Resnick, P., & Barton, G. (2019). *Algorithmic Bias Detection and Mitigation: Reducing Consumer Harms*. Brookings Institution. https://coilink.org/20.500.12592/k29pdg

Lyon, D. (2017). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.

Matulionyte, R., & Zalnieriute, M. (2024). Facial Recognition Technology in Context: Technical and Legal Challenges. In *The Cambridge Handbook of Facial Recognition in the Modern State* (pp. 9-124). Cambridge University Press.

Mbembe, A. (2019). *Necropolitics* (S. Corcoran, Trans.). Duke University Press. https://doi.org/10.2307/j.ctv1131298

Munir, B. (2025). Islamophobic Artificial Intelligence in the USA: A Critical Analysis of Religious Bias in Datasets. *Law Library Journal.* https://doi.org/10.2139/ssrn.5265355

Naber, N. (2012). *Arab America: Gender, Cultural Politics, and Activism*. New York University Press.

Nedelcu, M., & Soysüren, I. (2020). Precarious Migrants, Migration Regimes and Digital Technologies: The Empowerment-Control Nexus. *Journal of Ethnic and Migration Studies, 48,* 1821-1837. https://doi.org/10.1080/1369183x.2020.1796263

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Office of the United Nations High Commissioner for Human Rights (2010). *Minority Rights: International Standards and Guidance for Implementation.* United Nations. https://www.ohchr.org/sites/default/files/Documents/Publications/MinorityRights_en.pdf

Pew Research Center (2017). *Demographic Portrait of Muslim Americans*. Pew Research Center's Religion & Public Life Project. https://www.pewresearch.org/religion/2017/07/26/demographic-portrait-of-muslim-americans/

Postan, E. (2016). Defining Ourselves: Personal Bioinformation as a Tool of Narrative Self-Conception. *Journal of Bioethical Inquiry, 13,* 133-151. https://doi.org/10.1007/s11673-015-9690-0

Roberts, T., & Oosterom, M. (2025). Digital Authoritarianism: A Systematic Literature Review. *Information Technology for Development, 31,* 860-884. https://doi.org/10.1080/02681102.2024.2425352

Schopmans, H., & Tuncer Ebetürk, İ. (2024). Techno-Authoritarian Imaginaries and the Politics of Resistance against Facial Recognition Technology in the US and European Union. *Democratization, 31,* 943-962. https://doi.org/10.1080/13510347.2023.2258803

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154,* 477-564. https://doi.org/10.2307/40041279

Sutrop, M., & Laas-Mikko, K. (2012). From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics. *Review of Policy Research, 29,* 21-36. https://doi.org/10.1111/j.1541-1338.2011.00536.x

United States Commission on Civil Rights (2024). *The Civil Rights Implications of the Federal Use of Facial Recognition Technology: 2024 Statutory Enforcement Report.* https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage Publications.

Zhao, S. Y. (2022). Achille Mbembe, Necropolitics [Book Review]. *International Journal of Communication, 16,* 2961-2963.

Ziadah, R. (2021). Surveillance, Race, and Social Sorting in the United Arab Emirates. *Politics, 44,* 605-620. https://doi.org/10.1177/02633957211009719