UNIVERSITY OF PENNSYLVANIA

SCHOOL OF SOCIAL POLICY AND PRACTICE

MASTER OF SCIENCE IN SOCIAL POLICY AND DATA ANALYTICS

CRITIQUE & REWORK A TECHNOLOGY
FINAL PROJECT

FACIAL RECOGNITION TECHNOLOGIES IN LAW ENFORCEMENT: A CRITICAL ANALYSIS OF THEIR USE, IMPACT AND PATHS FOR IMPROVEMENT

Author: Rose Barragan

Professor: Dr. Desmond Patton

Course: SPP 6000: Advocacy in
Digital Media, Tech and Society

Fall 2024
December 4th, 2024

ABSTRACT

This report addresses the challenges associated with facial recognition technologies, exploring relevant cases where governments and security agencies have implemented them. It analyzes their current uses, which are marked by inequity, lack of transparency, and the absence of adequate oversight mechanisms. In addition, it delves into the systemic barriers that hinder these technologies' ethical and responsible development.

The paper also proposes a redesign of police body cameras operated by Axon, a product that, while not currently employing FRT, is encountering growing demand from governments and law enforcement agencies to integrate this technology. This paper presents a unique opportunity to proactively design ethical technology from the ground up. The redesign proposal seeks to develop body cameras that incorporate FRT from an ethical, inclusive, and human-centered perspective, establishing a model that prioritizes fairness, transparency, and the protection of the fundamental rights of individuals and communities.

1. UNVEILING THE CHALLENGES OF FACIAL RECOGNITION TECHNOLOGIES

Have you ever considered how facial recognition technology determines who can cross borders or board a plane? Now, imagine your face being flagged in a high-profile police investigation simply because a software system identified you as a match. Could your own face, an intrinsic part of your identity, become a source of unwarranted scrutiny or complication in your life?

"One false match can lead to missed flights, lengthy interrogations, tense police encounters, false arrests, or worse. However, the technology's flaws are only one concern. FRT can enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale" (Fox, A., 2019).

This is precisely what is happening in the digital age. Accelerated advances in the field of technology have resulted in an unprecedented expansion in the development and use of applications with Facial Recognition Technology (FRT)[1], which is capable of identifying and tracking individuals' facial information.

Remarkably, the global FRT market is projected to grow from $5.01 billion in 2021 to $12.67 billion by 2028, driven by increasing demand from governments and law enforcement agencies using it for criminal investigations, surveillance, and other security-related activities (Cision PR Newswire, 2022).

This is highlighted by a recent study conducted in 2021 by the U.S. Government Accountability Office (GAO), entitled "Facial Recognition Technology: Current and Planned Uses by Federal Agencies," which has focused on examining its use by federal law enforcement at points of entry and in commercial environments, as well as in digital access and cybersecurity, domestic law enforcement, and physical security.

However, there exist unsettling scenarios of how **U.S. law enforcement agencies**, such as FBI & DMV, CBP & TSA, and NJPD, **have indiscriminately and without oversight employed these technologies, in which human beings' fundamental rights and liberties are severely undermined** and even violated due to:

- The inadequate safeguards in place
- Lack of awareness
- Unauthorized consent for facial data collection
- Indiscriminate application
- Insufficient democratic oversight
- Issues of fairness and reliability (including significant racial bias)
- Lack of accountability and transparency measures
- Erosion of anonymity and privacy rights (which are crucial for safety and security)
- Legal loopholes within regulations.

[1] Facial Recognition is a type of technology application that leverages Artificial Intelligence algorithms; more precisely, it uses a type of deep learning algorithm called Convolutional Neural Network (CNN), which is well suited for image classification tasks, as CNNs learn from more complex facial features, filter image features and use them to classify images into different categories.

On top of that**,** as facial recognition applications are not mature technologies, they tend to suffer from **racial bias and inaccuracies**, leading to numerous damaging lawsuits and regulatory issues **affecting personal data and privacy**. Under these unprecedented circumstances, individuals need to know when and where FRT is recording their facial information, as this unregulated, state-of-the-art technology threatens to violate human beings' liberties and undermine their civil rights. Hence, law enforcement agencies, as well as, individuals in society, urgently need oversight of its development, deployment, and use.

Furthermore, this hurdle scales up when FRT evolves into Live Facial Recognition (LFR). LFR is a process that involves automated real-time processing of digital images containing information related to an identified or identifiable individual. The process starts extracting images of faces from CCTV; then, LFR software will process them, measuring facial features to produce a biometric template for each image. This template is then used to uniquely identify individuals (Witley, S., & Vittorio, A., 2023). For example, this technology can analyze and process real-time biometric information for population surveillance and **law enforcement purposes**.

In other words, a part of **what makes face recognition so perilous is that law enforcement agencies and private organizations continually use the technology in secret and without any democratic oversight, where there is a lack of accountability and transparency. The disproportionate use of LFR, unwarranted intrusion into individuals' lives, and legal loopholes within the regulations lead to scenarios in which rights and freedoms are severely under attack.**

2. PROBLEMATIC USE CASES OF FACIAL RECOGNITION TECHNOLOGIES IN LAW ENFORCEMENT

Although the widespread use of FRT by law enforcement agencies has increased nationwide, it has also been majorly criticized by privacy and digital rights advocates due to privacy concerns and other dangers related to fundamental rights and equity, as observed in the following real-life examples:

2.1. 2011 – 2019: FBI, U.S. DEPARTMENT OF MOTOR VEHICLES (DMV), AND U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)

FRT has become a standard screening tool for federal investigators, in particular the FBI, which has performed more than 390,000 facial recognition searches since 2011 using Department of Motor Vehicles (DMV) databases at the national, local, and state levels (Harwell, D., 2019).

However, this widespread use has raised concerns about privacy and consent since Americans' photos are scanned without their knowledge. The use of DMV databases has **created a vast surveillance network without formal approval** from Congress or state legislatures, leading to a legal gray area.

Furthermore, individuals renewing their driver's licenses do not explicitly allow their photos for federal facial recognition searches, causing questions about privacy and transparency. The lack of transparency, limited information on search frequency, targets, accuracy, and testing under normal conditions, particularly when searches yield few potential matches, remain a significant challenge.

Civil rights advocates and organizations have raised concerns about potential **misidentification and wrongful arrests, especially for individuals with darker skin tones** (L. Goodwin, 2017). This situation highlights the broader issue of public control over Government-held data and reinforces the need for regulatory frameworks that balance security with individual rights and privacy concerns.

2.2. 2019 - 2020: U.S. FEDERAL ORGANIZATIONS (DHS, CBP & TSA)

Relevant federal organizations such as U.S. Customs And Border Protection (A.K.A CBP) and the U.S. Transportation Security Administration (A.K.A TSA) have increasingly employed FRT at airports and other entry points. Just the first one alone has scanned more than 20 million travelers' faces by mid-2019 in collaboration with international airlines like Delta, JetBlue, and United Airlines collaborating to set up surveillance infrastructure (U.S. Department of Homeland Security, 2019).

However, there are concerns about the extensive and persistent government surveillance that FRT enables, especially given CBP's and TSA's past records of tracking **journalists, subjecting travelers to invasive searches, and targeting individuals based on factors like their national origin, religious beliefs, or political views**.

To shed more light on CBP's and TSA's facial recognition programs, a lawsuit has been filed by UCLA (New York Civil Liberties Union Foundation, 2020) to disclose government contracts with airlines, airports, and other entities related to facial recognition use, policies for biometric information acquisition, processing, and retention, and evaluations of the technology's effectiveness.

This will help enhance public and policymaker understanding of the federal agencies' facial surveillance systems, assess privacy safeguards, and evaluate potential discrimination based on race or other characteristics in CBP's and TSA's use of this technology (ACLU, 2020).

2.3. NEW JERSEY POLICE DEPARTMENT

The New Jersey Police Department pulled out facial recognition to identify Mr. Francisco Arteaga as a potential criminal suspect in an armed robbery in the city of New Jersey. However, Arteaga's defense was not given any information regarding the algorithm or software used in the process, which **raised concerns about the transparency and fairness** of the identification.

The court in State of New Jersey v. Francisco Arteaga (New Jersey v. Francisco Arteaga, 2023) held that the defendant's due process rights would be violated unless he was given access to the raw materials used by police to identify him, as well as information about how the facial recognition software worked, its source code, and its error rate. Such access was necessary to challenge witness identifications, examine the state's investigation, and establish reasonable doubt.

The court's decision highlighted the flaws inherent in facial recognition technology and recognized that it is often unreliable, mainly when **dealing with people of color, transgender and nonbinary individuals, and Black women** (Gullo, K., 2025). The court also emphasized that law enforcement **should not be allowed to use "black box" technology in criminal cases without transparency and scrutiny.** Despite these inaccuracies, law enforcement has widely adopted this technology for identifying suspects in criminal cases.

This ruling sets an important precedent for cases involving facial recognition technology and emphasizes the need for defendants to **examine and question the reliability of this technology** in order to protect their constitutional rights.

3. INSTITUTIONAL AND SYSTEMIC BARRIERS TO ETHICAL FRT DEPLOYMENT

The continued misuse of facial recognition technologies (FRT) stems from deeply ingrained institutional and systemic barriers. Despite growing awareness of the ethical and privacy issues associated with FRT, its deployment often bypasses safeguards meant to protect principles of privacy, equity, and fairness. Key challenges include the lack of individual consent, regulatory loopholes, insufficient industry accountability, grassroots resistance, and a fragmented approach to oversight. Understanding these barriers is crucial for crafting a more ethical and equitable framework for FRT use.

I. **Lack of permission during the Data acquisition and retention process:** facial recognition data has been collected from public spaces and social platforms without individuals' consent, posing a significant problem. The issue of consent raises concerns about the ethical, privacy, and transparency implications of collecting individuals' biometric information without their knowledge or approval.

II. **Regulatory loopholes and lack of national standards**: Another contributing factor is the absence of comprehensive regulations and guidelines at the federal level for facial recognition algorithms used by governmental organizations. While there is indeed the Biometric Information Privacy Act (BIPA, 2020) - a law set forth on August 3, 2020[2], to regulate **private** entities' collection, retention, disclosure, and destruction of biometric information - the Act **does not include** any Federal, State, or local government agency or academic institution (BIPA Section 2, paragraph 3)

III. **Grassroots opposition**: The widespread grassroots opposition to facial surveillance has led to legal challenges and calls for stricter regulations. This opposition highlights the need for comprehensive regulatory frameworks prioritizing individual rights and privacy.

2 This bill was introduced in the 116th Congress, which met from Jan 3, 2019 to Jan 3, 2021. Legislation not passed by the end of a Congress is cleared from the books. In other words the Bill was introduced in a previous session of Congress, but it did not receive a vote.

IV. **Oversight challenges:** Technology is moving much faster than legislative bodies and courts can respond. Deploying FRT in critical spaces such as airports and ports of entry by the government raises significant concerns about the potential for pervasive surveillance without adequate safeguards. Furthermore, FRT's technical limitations and inherent biases remain poorly understood, even by policymakers and companies marketing these systems. This lack of understanding exacerbates the difficulty of ensuring proper oversight and accountability in real-world applications.

Therefore, given that multiple U.S. law enforcement agencies are widely adopting FRT, it is essential to take prompt action to redesign this technology to ensure it is inclusive, protects fundamental rights, and enhances people's lives, addressing barriers and pitfalls associated with risks in privacy, bias, oversight, and transparency.

4. REDESIGNING FACIAL RECOGNITION TECHNOLOGY: TOWARDS INCLUSIVITY, ACCESSIBILITY, AND PURPOSE-DRIVEN INNOVATION

To redesign this technology, I propose starting with the baseline products offered by Axon (Axon, 2018), the leading manufacturer of police body cameras. In 2019, the Axon Independent AI and Policing Technology Ethics Board released a comprehensive report stating that Axon would not commercialize face-matching capabilities in body cameras (Smith, 2019) (Warzel, 2019). The decision was based on concerns about the lack of maturity of FRT for law enforcement, citing privacy risks and racial equity issues (Ingber, 2019).

So, how does Axon body camera technology work? Axon's work on face recognition focuses on detecting, tracking, and re-identifying faces in videos. For that, Axon's body cameras integrate the "Automated People Detection (APD) feature," which streamlines identifying individuals in body camera footage, enabling quick review of key moments. However, as Axon states – "*While fully functional, some aspects of APD may be refined over time*" (Axon, 2024). This acknowledgment raises an important question for many communities: *How will these refinements be implemented, and what implications might they carry?*

Furthermore, It is worth highlighting that the Ethics Board report was published in 2019, prior to the COVID-19 pandemic. However, as covered in the first section of this paper, the use of FRT by governments and law enforcement agencies has significantly expanded since the pandemic. This prompts a forward-looking question: *Could Axon reconsider integrating FRT into their body cameras in response to increasing demand from these sectors?*

Recognizing that the **integration of FRT may be a logical next step for Axon, the priority should be to design a system that incorporates this technology responsibly**. For that reason, I propose starting with Axon's existing body cameras, which currently utilize only face detection, as the foundation for this redesign, and gradually building upon this framework to integrate FRT thoughtfully and ethically.

This redesign must **center on hope**—hope for a future where technology serves as a tool for equity, trust, and progress. It should especially prioritize those communities that have historically faced misidentification, experienced police misconduct, or suffered wrongful arrests that may trigger traumatic experiences, aiming to rebuild trust and promote justice through thoughtful and ethical innovation.

Furthermore, the redesign would place **human and ethical principles at the center of the design**, where we can aspire to develop innovations that uplift communities, protect civil liberties, and repair historical inequities. With careful guidance and commitment, we have an opportunity to build tools that not only enhance safety but also build trust in the communities they serve.

Redesigning from an ethical perspective law enforcement body cameras that embed FRT requires proposing improvements that address the entire lifecycle of these technologies, from 1) the pre-development and 2) the development phase to 3) deployment, including 4) the importance of placing the human in the loop and 5) designing use cases where this technology becomes a lever for life improvement, joy, and social change. This will ensure that the technology includes principles of inclusion, accessibility, and ethical integrity from the start.

I. PRE-DEVELOPMENT PHASE

As highlighted in *section 2 - problematic Use Cases* - vulnerable and marginalized groups, as well as racial and ethnic minorities, are often the most affected by these technologies. That is why when planning the use case where this technology is to be implemented, it is necessary to consult these groups to integrate their views and realities into the approach to this technology. This ensures that the technology reflects a diverse understanding of the world.

II. DEVELOPMENT PHASE

Another major problem reflected in this paper is the lack of consent of individuals when giving their biometric data. That is why, when creating a biometric data dataset, the data that incorporates it must have the **explicit and informed consent of the individuals**. Likewise, it clearly must communicate how **individuals can opt out** of having their data included on the training datasets.

Additionally, the **dataset should ensure that it reflects a diversity of demographics, including ethnicity, gender, age, and cultural backgrounds**. For example, include variations in skin tones, facial features, and cultural attributes (makeup, facial tattoos, headscarves, religious elements such as bindi and tilaka, etc.). This new dataset will help minimize bias and encourage inclusiveness.

Once the dataset is complete and diverse, it is also necessary to have **programmers whose training and background are also diverse**. This will help prevent homogeneity in decision-making and ensure that design ideologies reflect various perspectives and experiences.

Finally, once the recognition model is developed and before it is deployed in the market, a **proof of concept (POC) in a controlled environment is necessary**. These POCs will help identify and mitigate potential bugs in the programming and use before their full-scale deployment. However, it is also necessary that a **diverse cross-section of communities evaluate the effectiveness, fairness, and transparency of the new product during its POC evaluation**. Their feedback is essential to create a new product that truly serves the community and is accepted by society.

III. IMPLEMENTATION PHASE

One of the missing aspects in the use of these technologies by people who do not belong to law enforcement bodies, is the possibility to a**ccess open source versions for non-commercial use.** In this way, individuals and communities are able to understand and manipulate this technology in a secure and transparent environment where transparency and explainability are at the forefront.

Using **open-source deployments facilitates the participation of affected communities**, allowing them to evaluate, provide feedback, and establish checks and balances on what works and what doesn't with this technology.

On the other hand, it is imperative to improve the clarity with which facial recognition results are presented by **developing a more user-friendly interface** that is more connected to the legal and judicial system. This will enable law enforcement officers to understand and use the information effectively, ensuring that it is clear, accurate, useful, and complete.

In addition to the results appearing on the **interface being connected to the legal/juridical system, they should also be connected to the social workforce platforms** for additional evidence and support, before decisions are made, **reducing the risks of reliance on FRT as the sole decision tool.** By addressing each phase of the value chain, FRT can become an equitable, reliable tool designed with the communities it serves in mind.

IV. HUMAN IN THE LOOP

Furthermore, looking at the big picture of the technology we seek to redesign, **it is also necessary to take into account the human component**. Throughout the suggestions for improvement in the redesign, we have talked about requesting the express consent of the people, creating datasets that reflect the diversity of realities, involving them in the process of evaluating the POCs, and so on.

However, it is necessary to go a step further and **create an independent committee** with experts in artificial intelligence, privacy advocates, police chiefs, local communities (such as Community-Oriented Policing Services - COPS) and affected individuals such as Francisco Arteaga. This independent committee will seek to audit practices where body cameras powered by FRT are employed to ensure ethical applications, prevent misidentification, and suggest best practices, such as training programs at all levels.

To foster a comprehensive understanding of emerging technologies, it is crucial to **introduce technology literacy workshops and training programs.** This implies implementing one-day educational workshops for students and community members at schools and local centers focused on artificial intelligence, facial recognition technologies (FRT), and other digital innovations. Simultaneously, it is necessary to develop specific training programs for technology professionals, including both the mastery of applied ethical principles and the ability to work with more diverse and inclusive datasets. These initiatives will not only ensure greater equity and accountability in the design and use of these tools, but will also enhance the development of critical skills and technological understanding that permeates all levels of society.

V. NEW APPROACHES FOR THE TECHNOLOGY

Finally, in addressing the question of how this technology can **improve lives and bring joy,** I have tried to take an innovative and positive perspective on its application. In a global context marked by war conflicts, natural disasters, forced displacement, and migration in precarious conditions due to corrupt governments, facial recognition and the extensive databases available in governments and security agencies can become powerful tools to make a significant difference in people's lives.

For example, FRT could be used to **identify missing persons**, making it easier to locate them more quickly and efficiently. Likewise, this technology could be used in **humanitarian efforts** to reunite families separated in the aftermath of natural disasters or armed conflicts.

Furthermore, in receiving countries such as the United States, FRT could be instrumental in supporting individuals who become lost within complex migration systems. These applications reflect an ethical and empathetic use of technology and offer a clear example of how FRT can transcend its current limitations to become a tool that promotes human welfare.

5. PERSONAL REFLECTION

We cannot stop technology from coming.

Technology's advancement is inevitable, and the global demand for AI-powered biometric solutions continues to rise. These technologies are increasingly used to verify and identify individuals, manage access to online accounts, authorize payments, and monitor attendance. Beyond consumer applications, biometric tools have become essential in national security and border protection, serving as standard screening mechanisms for federal agencies like the FBI, Customs and Border Protection, and the TSA.

The problems come when facial technologies' extensive and often secretive deployment operates without adequate democratic oversight, resulting in limited accountability and transparency. These technologies frequently perpetuate discrimination, disproportionately targeting marginalized groups, failing to accurately identify people of color, and excluding vulnerable communities from fair treatment.

Despite the potential for innovation, many current biometric solutions remain incomplete and unethical, reflecting corporate priorities that favor profit over societal well-being.

A particularly striking insight from my research comes from Shoshana Amielle Magnet's publication, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Magnet, 2011). Magnet highlights the troubling reduction of human beings into binary data—mere "zeros" and "ones"— representing a troubling objectification, breaking the human body into replicable parts, from retinas to fingerprints, and undermining individuality.

So, while these unique traits define our identity, society seems increasingly willing to trade them away in the name of technological advancement.

6. CONCLUSION AND TAKEAWAYS

We cannot stop technology from coming - especially when governments and law enforcement agencies are the ones sponsoring them. For that reason, this paper presents an opportunity for individuals and communities historically excluded from decision-making processes. It is a chance to co-create a tool that integrates facial recognition technology (FRT) ethically.

This new approach embeds fundamental ethical principles, including **transparency, explainability, equity, and robustness.** Additionally, it establishes mechanisms for checks and balances, ensuring that diverse stakeholders have a seat on the table, whose backgrounds and perspectives are essential for fostering balanced decision-making and safeguarding the rights of individuals historically subjected to systemic abuse. By seizing this moment, we can ensure that technological advancements align with societal values, improve the quality of life and individual well-being, and protect human rights while addressing the growing demand for innovative solutions.

7. NEXT STEPS

I have shared this document with Regina Holloway, a lawyer by profession, the Community Impact team leader, and the vice president of Strategic Partnerships and Policy at Axon. My goal is to meet with her in the coming days to discuss the redesign proposal, gain her insightful feedback on the paper, and ensure that the proposed redesign aligns with future market demands, addresses community needs, and upholds ethical standards. I hope to ask questions like:

- *Have I included all the necessary stakeholders who should have a seat at the table?*
- *What should be the first step when redesigning this product, considering all the phases presented above?*
- *What challenges do large companies (Axon) typically face when advocating for more equitable products that could potentially embed FRTs? Could it be Community buy-in?*
- *When building the new "FRT-powered body camera" team, What should be the right balance between technical and social experts in that team?*

8. REFERENCES

[1] ACLU (2020). ACLU v. DHS: FOIA Lawsuit Seeking Information on Implementation of Face Surveillance at Airports. *ACLU*. https://www.aclu.org/cases/aclu-v-dhs-foia-lawsuit-seeking-information-implementation-face-surveillance-airports#:~:text=In%20March%202020%2C%20the%20ACLU,this%20technology%20in%20the%20future

[2] ACLU. (2019, June 27). *ACLU comment on Axon's decision to ban facial recognition on body cameras: ACLU of Northern Ca*. ACLU of Northern California. https://www.aclunc.org/news/aclu-comment-axon-s-decision-ban-facial-recognition-body-cameras

[3] Axon. (2018, December 7). *A quick guide to face recognition with ai*. Axon News & Resources. https://www.axon.com/news/face-recognition-with-ai

[4] Axon. (2024, September 19). *Automated People Detection Overview and Permissions*. My Axon. https://my.axon.com/s/article/Automated-People-Detection-Overview-and-Permissions?language=en_US

[5] BIPA, 2020 - S.4400 - National Biometric Information Privacy Act of 2020. bill. https://www.congress.gov/bill/116th-congress/senate-bill/4400/text

[6] Foye, U., Regan, C., Wilson, K., Ali, R., Chadwick, M., Thomas, E., Allen-Lynn, J., Allen-Lynn, J., Dodhia, S., Brennan, G., & Simpson, A. (2024b). Implementation of body worn camera: Practical and ethical considerations. Issues in Mental Health Nursing, 45(4), 379–390. https://doi.org/10.1080/01612840.2024.2308605

[7] Fox, A. (2019). How can facial recognition be racially biased? *The Hill*. https://thehill.com/changing-america/respect/equality/475533-racial-bias-of-facial-recognition-systems-confirmed-in/

[8] GAO. (2021, August 24). *Facial recognition technology: Current and planned uses by federal agencies*. Facial Recognition Technology: Current and Planned Uses by Federal Agencies | U.S. GAO. https://www.gao.gov/products/gao-21-526

[9] GovTrack.us. (2024). S. 4400 — 116th Congress: National Biometric Information Privacy Act of 2020. Retrieved from https://www.govtrack.us/congress/bills/116/s4400

[10] Gullo, K. (2025). Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition.

[11] Harwell, D. (2019, July 7). FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches. *The Washington Post*. https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/

[12] June 27). *Major police body camera manufacturer rejects facial recognition software*. NPR. https://www.npr.org/2019/06/27/736644485/major-police-body-camera-manufacturer-rejects-facial-recognition-software

[13] L. Goodwin, G. (2017). *FACE RECOGNITION TECHNOLOGY* [Testimony before the Committee on Oversight and Reform, House of Representatives, United States Government Accountability Office]. https://www.gao.gov/assets/gao-19-579t.pdf

[14] Magnet, S. A. (2011). When biometrics fail: When Biometrics Fail: Gender, Race, and the Technology of Identity. *Duke University Press*. https://doi.org/10.1215/9780822394822

[15] New Jersey v. Francisco Arteaga (June 7, 2023). A-3078-21. Superior Court Of New Jersey Appellate Division. https://www.njcourts.gov/system/files/court-opinions/2023/a3078-21.pdf

[16] New York Civil Liberties Union Foundation (2020). *ACLU V. DHS — Face Recognition Surveillance Complain. United States District Court Southern District Of New York* [Complaint For Injuctive Relief]. Aclu V. Dhs — Face Recognition Surveillance Complaint.

[17] *Reports of the Axon Ethics Board*. The Policing Project. (n.d.). https://www.policingproject.org/axon

[18] Smith, R. (2019, June 27). *The future of face matching at Axon and AI Ethics Board Report*. Axon News & Resources. https://www.axon.com/news/ai-ethics-board-report

[19] U.S. Department of Homeland Security (2019). *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies* [Report to Congress]. https://www.tsa.gov/sites/default/files/biometricsreport.pdf#page=11

[20] Warzel, C. (2019, June 27). *A major police body cam company just banned facial recognition*. The New York Times. https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html

[21] Witley, S., & Vittorio, A. (2023). Facial Recognition Software Is Everywhere, With Few Legal Limits. *Bloomberg Law*. https://news.bloomberglaw.com/privacy-and-data-security/facial-recognition-software-is-everywhere-with-few-legal-limits