NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

REGULATING FEDERAL LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

by

Sapan Patel

December 2023

Co-Advisors: Nadav Morag (contractor)
Rodrigo Nieto-Gomez

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE REGULATING FEDERAL LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Sapan Patel	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This research examines optimal regulation allowing federal law enforcement to use facial recognition technology (FRT) while protecting civil liberties. Through a literature review, a comparative analysis of the European Union's Law Enforcement Directive (LED), and a policy analysis for U.S. regulation it evaluates frameworks balancing effectiveness and proportionality. Findings show that comprehensive legislation upholding fairness, accountability, and purpose limitations, complemented by independent auditing and oversight, can enable public safety benefits while constraining unfettered use. However, flexibility is imperative; legal, ethical, and technical dimensions remain uncertain. The research concludes that nuanced, principled governance provides the most prudent path. The next steps involve ongoing stakeholder engagement, implementation planning, and impact evaluation to refine balanced oversight as case law, technology, and societal norms evolve. This analysis fills a gap by evaluating policy tradeoffs—equipping stakeholders with evidence to inform sound FRT governance. With adaptable oversight, facial recognition can be steered toward just ends.

14. SUBJECT TERMS facial recognition, artificial intelligence, legislative framework, law enforcement, comparative method, policy analysis, technology	**15. NUMBER OF PAGES** 95
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

REGULATING FEDERAL LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

Sapan Patel
Special Agent/National Program Manager, Department of Homeland Security
BA, Emory University, 2007
MS, Georgetown University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: Nadav Morag
Co-Advisor

Rodrigo Nieto-Gomez
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research examines optimal regulation allowing federal law enforcement to use facial recognition technology (FRT) while protecting civil liberties. Through a literature review, a comparative analysis of the European Union's Law Enforcement Directive (LED), and a policy analysis for U.S. regulation it evaluates frameworks balancing effectiveness and proportionality. Findings show that comprehensive legislation upholding fairness, accountability, and purpose limitations, complemented by independent auditing and oversight, can enable public safety benefits while constraining unfettered use. However, flexibility is imperative; legal, ethical, and technical dimensions remain uncertain. The research concludes that nuanced, principled governance provides the most prudent path. The next steps involve ongoing stakeholder engagement, implementation planning, and impact evaluation to refine balanced oversight as case law, technology, and societal norms evolve. This analysis fills a gap by evaluating policy tradeoffs—equipping stakeholders with evidence to inform sound FRT governance. With adaptable oversight, facial recognition can be steered toward just ends.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
CIA	Central Intelligence Agency
CNN	convolutional neural network
CRS	Congressional Research Service
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DPO	data protection officer
EO	executive order
FIPP	Fair Information Privacy Principle
FISWG	Facial Identification Scientific Working Group
FRT	facial recognition technology
GAO	Government Accountability Office
GDPR	General Data Protection Regulation
ICE	Immigration and Customs Enforcement
ICO	Information Commissioner's Office
ISO	International Organization for Standardization
LED	Law Enforcement Directive
MIT	Massachusetts Institute of Technology
ML	machine learning
NCMEC	National Center for Missing and Exploited Children
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
PIA	privacy impact assessment

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Facial recognition technology (FRT) has gained prominence as a potent tool in the toolkit of law enforcement agencies, offering a range of capabilities from advanced surveillance to efficient suspect identification. While the technology presents opportunities for enhanced public safety measures, its widespread application in policing introduces a plethora of ethical and societal concerns. These include worries about privacy intrusion, informed consent, racial and gender bias, and the potential erosion of civil liberties.[1] This research seeks to formulate an optimal policy strategy that enables federal law enforcement agencies to exploit FRT's benefits without compromising individual rights and freedoms.

The methodology employed in this study involves a comprehensive literature review, focusing on the developmental trajectory of FRT and the ethical considerations associated with its integration into law enforcement practices. Algorithmic advancements have contributed to substantial improvements in the accuracy and fairness of FRT.[2] However, significant issues around transparency and accountability still exist.[3] Additionally, this thesis conducts a comparative analysis with the European Union's Law Enforcement Directive (LED) to distill principles such as lawfulness, purpose limitations, and regulatory oversight, which could be invaluable in shaping U.S. policy. It must be noted, however, that transplanting European regulatory frameworks to the American context requires nuanced adaptation to reflect the specific operational realities and legal constraints faced by U.S. law enforcement agencies.

A rigorous policy analysis is the cornerstone of this thesis, systematically examining a spectrum of regulatory alternatives. These range from an outright ban on law

[1] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," Georgetown Law, Center on Privacy and Technology, October 18, 2016, https://www.perpetuallineup.org/.

[2] P. Jonathon Phillips et al., "Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms," *Proceedings of the National Academy of Sciences* 115, no. 24 (June 12, 2018): 6171–76, https://doi.org/10.1073/pnas.1721355115.

[3] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020, sec. Technology, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

enforcement's use of FRT to nuanced, comprehensive legislation. These alternatives are evaluated against various criteria, including proportionality, economic cost, public trust, and operational efficiency. The findings indicate the need for comprehensive, principle-based regulation as the most balanced approach. Such regulation would entail mandatory auditing procedures, enhanced transparency measures, and incorporate relevant principles from the LED. This could effectively restrict law enforcement's unchecked utilization of FRT while retaining its benefits in the context of public safety and law enforcement efficacy.

This research ultimately concludes that a nuanced approach to governance, rooted in core principles like fairness, accountability, and purpose limitation, can facilitate the ethical and responsible use of this powerful technology. The study acknowledges that given the legal, ethical, and technological uncertainties surrounding FRT, any governance framework must be flexible and adaptable. Oversight structures must be revisited and refined continuously to keep pace with changes in societal norms, legal landscapes, and technological advancements.

Key recommendations emanating from the research include the collaborative development of comprehensive federal legislation designed to govern law enforcement's use of FRT based on established principles of lawfulness, fairness, and purpose limitation. Robust independent auditing mechanisms should be incorporated, although it is crucial to ensure these do not become cumbersome to the point of inhibiting operational effectiveness. Additionally, agencies should provide transparent justifications for the deployment of FRT based on the principle of proportionality.

For the governance framework to be dynamic and responsive, ongoing stakeholder engagement is indispensable. Law enforcement agencies should carefully design implementation plans, and regulators should periodically conduct impact evaluations to adapt regulations as necessary. By adopting such a principled yet adaptable governance framework, agencies can guide their use of FRT towards just and ethical ends. This research thereby equips policymakers with evidence-based insights, helping them manage the complex trade-offs involved in regulating FRT, ultimately aiding in the formation of sound, balanced governance structures.

ACKNOWLEDGMENTS

First and foremost, I would like to express my profound gratitude to my colleagues. Their unwavering support during my "vacations to Monterey" was invaluable. Their willingness to step in and cover for me provided me with the peace of mind necessary to concentrate on this significant undertaking. Their generosity not only facilitated my academic pursuits, but also underscored the strength of our professional and personal bonds.

Equally, I owe a deep debt of gratitude to my friends and family. Their consistent encouragement, faith in my abilities, and genuine enthusiasm for my academic journey have been my driving force. They recognized and respected my thirst for knowledge, continually inspiring me to explore new horizons and relentlessly push my own boundaries.

I must also extend heartfelt thanks to my CHDS cohort. Sharing this academic journey with you has been an enriching experience. Our collaborative spirit, lively debates, mutual encouragement, and shared moments of both challenges and successes have immensely contributed to my growth and the fruition of this thesis.

To all of you, your belief in me and your unyielding support have made all the difference. I am endlessly thankful for your role in this milestone of my academic journey.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Congress has appointed the National Center for Missing and Exploited Children (NCMEC) to serve as a central repository and nationwide support center for issues related to missing and exploited children.[1] NCMEC uses artificial intelligence (AI) and machine learning (ML) in the form of facial recognition technology (FRT) to help fulfill its mission; one such tool—Spotlight—helps identify victims of online sexual exploitation, locate them, and prioritize efforts by determining whether a victim faces imminent danger. In one case, NCMEC used Spotlight to search for images of a missing fourteen-year-old child and discovered 87 escort advertisements offering her for commercial sex; these advertisements ran for at least eight months.[2] Law enforcement previously had no indication or evidence that the child was a victim of sex trafficking. Two days after using Spotlight, law enforcement located and rescued the child. After recovery, she reported the kidnappers forced her to participate in commercial sex acts in exchange for shelter.[3] As the NCMEC use-case of Spotlight highlights, FRT has the potential to be a valuable tool with significant benefits for society; however, certain limitations constrain its widespread application.

Critics have raised concerns about the due process and policy shortcomings when law enforcement agencies identify suspects with the assistance of facial recognition technology.[4] Law enforcement operates within strict parameters set by legislation and legal precedence; however, the jurisprudence of using FRT in law enforcement is unclear.[5] When law enforcement uses FRT irresponsibly, these concerns will continue to grow and

---

[1] Office of Juvenile Justice and Delinquency Prevention, "National Center for Missing & Exploited Children."

[2] Ann Park, *Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses* (Washington, DC: Office of Science and Technology Policy, 2022), https://www.ai.gov/rfi/2022/86-FR-56300/NCMEC-Biometric-RFI-2022.pdf.

[3] Park.

[4] Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short."

[5] T. J. Benedict, "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest," *Washington and Lee Law Review* 79, no. 2 (Spring 2022): 858–59, https://www.proquest.com/docview/2681520570/abstract/36373B0F5BA44746PQ/1.

potentially derail its future usage. For example, if law enforcement agencies are not cognizant of FRT's potential for error and violate due process by solely relying on the technology without using corroborating evidence, then the resulting case law could potentially strike down any future use of FRT.

On December 3, 2020, the president signed Executive Order (EO) 13960, Promoting the Use of Trustworthy AI in the Federal Government, into effect. EO 13960 expanded upon EO 13859, Maintaining American Leadership in AI—signed February 11, 2019—by calling on Executive Department agencies to increase the implementation of AI to enhance their operations but also dictates sound policy should guide the implementation of AI.[6] Furthermore, the AI in Government Act of 2020 created the GSA AI Center of Excellence to assist government decision-makers in developing AI capabilities.[7] Although the AI Center provides good guidance on the enterprise-level implementation of AI from a business-process standpoint, it does not address the legal and ethical concerns affecting policy development for AI usage, particularly FRT usage, by law enforcement agencies.

Today, FRT is a global phenomenon used by public and private entities worldwide.[8] U.S. federal law enforcement agencies need a framework for policy development that addresses their unique legal and ethical issues. In law enforcement, frameworks must come from legal or legislative regulation to be truly effective. This thesis aims to determine how regulation could aid U.S. law enforcement agencies in the continued, ethical use of FRT.

---

[6] Exec. Order No. 13960, 85 FR § (2020), https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

[7] GSA, *Introduction to the AI Guide for Government* (Washington, DC, 2022), https://coe.gsa.gov/coe/ai-guide-for-government/introduction/index.html.

[8] Isabelle Hupont et al., "The Landscape of Facial Processing Applications in the Context of the European AI Act and the Development of Trustworthy Systems," *Scientific Reports (Nature Publisher Group)* 12, no. 1 (2022), https://doi.org/10.1038/s41598-022-14981-6.

B. RESEARCH QUESTION

What is the best approach to regulate federal law enforcement agencies' use of facial recognition technology to maintain its operational effectiveness while addressing civil liberty concerns?

C. LITERATURE REVIEW

This literature review discusses the prevailing academic debates surrounding law enforcement agencies' ethical usage of FRT. The literature delves into the technology's accuracy, privacy, and civil liberties concerns and the need for regulation to govern FRT use.

Although FRT is not new, its usage by law enforcement agencies is still somewhat novel. Executive Orders 13859 and 13960 and the AI in Government Act of 2020 have paved the way for promoting AI implementation into government processes. With the adoption of FRT by law enforcement agencies ramping up due partly to these executive and congressional actions, stakeholders have only recently begun to research and examine the ethics of this technology adoption. As such, the literature surrounding this topic has not matured to the point of having a robust body of peer-reviewed research. This review will examine the literature addressing the evolution of the relative accuracy of FRT, privacy and civil liberties issues with FRT, and the need to regulate FRT usage.

1. Evolution of Relative Accuracy

Scientific researchers in computer vision have researched the relative accuracy of facial recognition algorithms against that of human examiners. This body of research chronicles the evolution of the advancement of FRT algorithms to meet the performance of trained human examiners. Two authors—Alice J. O'Toole and P. Jonathon Phillips—consistently appear in the literature; others often cite their work. In 2007, O'Toole et al. concluded that FRT algorithms were more accurate than untrained human examiners.[9] In 2012, Anthony

[9] Alice J. O'Toole et al., "Face Recognition Algorithms Surpass Humans Matching Faces Over Changes in Illumination," *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, no. 9 (September 2007): 1642–46, https://doi.org/10.1109/TPAMI.2007.1107.

et al. refuted the validity of such comparisons and concluded that "the perceptual function of face detection in humans cannot easily be directly compared to the function performed by computer algorithms, even when a test is devised that presents an identical challenge to both humans and computers."[10] In 2014, O'Toole and Phillips expanded the scope of their research to include more advanced comparison methodologies. O'Toole and Phillips conclude that "for matching frontal faces in still images, algorithms are consistently superior to humans. For video and difficult still face pairs, humans are superior."[11] Also, in 2014, Chaochao Lu and Xiaoou Tang published complementary claims that machine-learning FRT algorithms can surpass human accuracy in still image comparisons.[12] Finally, in 2018, O'Toole, Phillips, and others authored the penultimate paper on the relative accuracy of FRT algorithms. O'Toole et al. compare FRT algorithms developed between 2015 and 2017 against trained forensic facial examiners and conclude that "the best machine performed in the range of the best humans: professional facial examiners."[13] The National Institute of Standards and Technology (NIST) references this paper as the seminal work on relative FRT accuracy. The current consensus in the literature is that modern FRT algorithms—specifically those that employ deep convolutional neural network machine learning—are at least as accurate as trained human examiners.

2. Privacy and Civil Liberties

In examining the privacy and civil liberties concerns with law enforcement employing FRT, the literature revolves around the debate between security and privacy. Much of the literature includes legal reviews, government reports, and academic theses. One group posits that law enforcement should continue ethically using FRT by balancing

[10] Samuel E. Anthony, Maryam Vaziri Pashkam, and Ken Nakayama, "Comparing Computer and Human Performance on Identical Face Detection Tasks," *Journal of Vision* 12, no. 9 (August 13, 2012): 499, https://doi.org/10.1167/12.9.499.

[11] P. Jonathon Phillips and Alice J. O'Toole, "Comparison of Human and Computer Performance across Face Recognition Experiments," *Image and Vision Computing* 32, no. 1 (January 1, 2014): 74, https://doi.org/10.1016/j.imavis.2013.12.002.

[12] Chaochao Lu and Xiaoou Tang, "Surpassing Human-Level Face Verification Performance on LFW with GaussianFace" (arXiv, December 19, 2014), https://doi.org/10.48550/arXiv.1404.3840.

[13] Phillips et al., "Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms," 6171.

privacy and security. In contrast, the other argues law enforcement should cease using FRT in favor of privacy over security.

In 2017, the House of Representatives, Committee on Oversight and Government Reform held a hearing on law enforcement's use of FRT. The committee chairman advised, "just because we can doesn't mean we necessarily should."[14] Many proponents of law enforcement advocate continuing to use FRT but doing so ethically. The Facial Identification Scientific Working Group (FISWG) continually evaluates and develops best practices for law enforcement's usage of FRT. Finklea et al. of the Congressional Research Service (CRS) suggest using FISWG recommendations as a roadmap for law enforcement agencies to enhance future usage of FRT.

Similarly, Yeung et al. of the RAND Corporation recommend finding a balance between security and privacy for the continued use of FRT.[15] Carter agrees in his NPS thesis that the benefits of FRT can outweigh potential privacy concerns.[16] The CRS and RAND reports identify the need for unified legislation to govern law enforcement's usage of FRT and provide some broad recommendations for policy considerations. However, as FRT continues evolving and becoming interwoven in law enforcement processes, legislators need to provide greater specificity on this complex issue.

The counterargument calls for a moratorium on FRT's use by law enforcement. The literature taking this position comes mainly from legal reviews and proposed bills. San Francisco banned law enforcement's use of FRT in 2019, becoming the first major municipality to impose a blanket ban on the technology. The banning legislation cited

[14] *Law Enforcement's Use of Facial Recognition Technology: Hearing before the Committee on Oversight and Government Reform, House of Representatives*, House of Representatives, 115th Cong. 1 (2017), 1, https://www.govinfo.gov/content/pkg/CHRG-115hhrg28689/pdf/CHRG-115hhrg28689.pdf.

[15] Douglas Yeung et al., *Face Recognition Technologies: Designing Systems That Protect Privacy and Prevent Bias* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/research_reports/RR4226.html.

[16] Anthony M. Carter, "Facing Reality: The Benefits and Challenges of Facial Recognition for the NYPD" (Master's thesis, Monterey, CA; Naval Postgraduate School, 2018), https://calhoun.nps.edu/handle/10945/60374.

dangers to privacy and civil liberties that outweigh potential benefits to security.[17] In her law review article, Lovallo formulated a similar conclusion calling for a ban on FRT usage in Texas.[18] In her Harvard thesis, Lord postulates, "The best recommendation for law enforcement is to opt out of using facial recognition technology."[19] Lovallo, Lord, and others who advocate for a moratorium on FRT emphasize the likelihood of misuse by practitioners, and this presumption of abuse is the driving force behind their conclusions. Although they can provide specific limited examples of misuse, they assume the actions of a small subset of practitioners reflects the tendencies of the whole group, leading to group attribution error.

3. Need for Regulation

In his examination of U.S. v Jones, Supreme Court Justice Samuel Alito wrote, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[20] The body of literature examining the regulation of FRT usage by law enforcement consists mainly of legal reviews and analyses. The literature suggests two primary approaches to regulation—defining use parameters and establishing independent oversight.

The group that suggests defining parameters for law enforcement usage of FRT is more prevalent than that suggesting independent oversight. Sabrina Lochner concludes in her legal analysis that legislation should address how and when law enforcement agencies can collect facial scans and when the scans can use FRT.[21] Notably, Lochner's analysis appeared in 2013, and although much of her analysis relies on an outdated iteration of FRT,

---

[17] Administrative Code – Acquisition of Surveillance Technology, 190110, S.F. Board of Supervisors (2019).

[18] Caroline Lovallo, "Big Brother's Fall Brings Liberty to All: Addressing the Urgency for Strict Regulation Governing Law Enforcement Use of Facial Recognition Technology in Texas," *Thurgood Marshall Law Review* 46, no. 1 (2021).

[19] Paige Lord, "The Cost of Possibility: U.S. Law Enforcement Use of Facial Recognition Technology and Violations of Civil Liberties" (Master's thesis, Harvard University, 2022), 79, https://dash.harvard.edu/handle/1/37371406.

[20] United States v. Jones, 565 U.S. 400, 10 (2012).

[21] Sabrina Lochner, "Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans," *Arizona Law Review* 55 (Spring 2013): 201–33, Nexis Uni.

the principles used still apply. For example, Peter Schuetz's conclusion in his 2021 analysis shares many of the same principles as Lochner's; however, Schuetz also suggests addressing specific technical challenges with FRT, such as algorithmic bias.[22] Others suggest novel approaches to regulation. Shackelford and Dockery conclude the need for polycentric governance in which the AI leaders of the world—the United States, the European Union, and China—work together to define parameters.[23] The complexity of such a solution would likely make it impractical, but the literature reflects the field, exploring many avenues of regulation.

The proponents of mandating independent oversight all share a central tenet—the urgent need for checks and balances with FRT usage. In her analysis, Katelyn Ringrose highlights the impact of integrating FRT with body-worn cameras on public safety and suggests establishing independent oversight mechanisms to mitigate misuse and ensure accountability.[24] Spencer Davies proposes a different method of oversight in which independent forensic reviewers would assess facial scans before law enforcement uses them.[25] David Gray suggests external accountability, even offering external review for disciplinary action against users.[26] Although oversight and accountability should play a key role in FRT regulation, much of the literature fails to address how excessive administration can disrupt effectiveness.

---

[22] Peter N.K. Schuetz, "Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework," *Law and Inequality* 39 (Winter 2021): 221–54, Nexis Uni.

[23] Scott J. Shackelford and Rachel Dockery, "Governing AI," *Cornell Journal of Law and Public Policy* 30 (Winter 2020): 279–333, Nexis Uni.

[24] Katelyn Ringrose, "Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns," *Virginia Law Review Online* 105 (2019): 57–66.

[25] A. Spencer Davies, "A Californian Algorithm: Amending Assembly Bill 2261 to Regulate Law Enforcement's Use of Facial Recognition Technology in Post Hoc Criminal Investigations," *Berkeley Jounal of Criminal Law* 26, no. 2 (2021): 27–70, https://doi.org/10.15779/Z38SB3X03N.

[26] David Gray, "Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies," *SMU Science and Technology Law Review* 24 (Summer 2021): 3–63, Nexis Uni.

4. Conclusion

Scholars and researchers, while acknowledging the remaining error margins, agree that the accuracy of FRT has drastically improved and is less problematic than in the past. Nonetheless, this technological progress doesn't fully address the ethical and societal issues associated with FRT. One of the most hotly contested areas in this context is privacy. The debate around privacy in the realm of FRT pivots on the delicate balance between maintaining individual rights and ensuring public safety. It often becomes a matter of contention as to which should take precedence—privacy rights or security needs. The crux of this argument often centers on determining the precise point where privacy concerns should yield to security interests and vice versa.

A growing consensus among researchers posits that regulatory frameworks can provide the balance that will alleviate these concerns. An expanding body of literature has started to explore various regulatory models that could potentially govern the use of FRT. These models look at principles like consent, transparency, accountability, and proportionality, aiming to mitigate the potential negative impacts of FRT while enabling its positive contributions to law enforcement and public safety.

Despite the increasing attention on regulatory frameworks, a notable gap in the literature is the lack of studies on how these regulations could impact the adoption of FRT by federal law enforcement agencies. A critical question is whether regulation would act as a barrier, hindering the diffusion of FRT into these agencies due to added constraints and requirements. Conversely, a perspective worth considering is whether regulation might boost FRT's adoption and diffusion. This could happen if the existence of a well-defined regulatory framework reassures both the public and law enforcement agencies about the ethical and responsible use of FRT. Answering these questions calls for further research that evaluate the impact of regulation on the use of FRT in law enforcement. Such studies can provide valuable insights to inform policy decisions, ultimately contributing to the development of a regulatory framework that balances privacy rights with security needs while ensuring the effective and responsible use of FRT.

D. RESEARCH DESIGN

The first section of this thesis will examine the underlying technology of FRT, specifically its advancements in accuracy and bias mitigation, and the current ethical landscape of law enforcement's use of FRT. This section will also review the history of law enforcement's early adoption of FRT.

The second section will employ the comparative method to analyze the EU's Law Enforcement Directive (LED). This research will focus on a systematic comparison of the two distinct regulatory environments of the EU and the U.S. to draw lessons from the EU's successes, failures, and unique approaches.

To conceptualize this comparative approach, this study will first perform a detailed document analysis of the LED, focusing on the scope, intent, and implementation of regulations relevant to FRT. It will extract the key principles, standards, and mechanisms that the LED employs to regulate FRT's use in law enforcement. The research will then map these findings against the potential regulatory framework in the U.S., identifying the commonalities and differences. This will involve an in-depth analysis of the principles of the LED, identify potential barriers to adoption in U.S. regulation, and provide recommendations as to which principles could provide the most benefit to FRT regulation for U.S. federal law enforcement agencies.

Throughout this section, the research will be guided by key research questions: How do the regulations reflect differing views on privacy, security, and civil liberties in the EU and US? What are the respective strengths and weaknesses of each approach? How do these frameworks address the issues of accuracy, bias, transparency, accountability, and proportionality? The objective is not just to understand these regulatory environments in isolation, but to glean insights that could potentially inform a more nuanced and effective regulatory approach to FRT in law enforcement. By understanding the specifics of each jurisdiction's approach—their successes and failures—we can derive important lessons to contribute to the ongoing policy debates and decision-making processes related to FRT in the US.

The third section will utilize Eugene Bardach's eightfold path for policy analysis.[27] The goal of this section is to synthesize the research of the first two sections to provide appropriate policy options and, ultimately, recommend a path forward that answers the main research question: What is the best approach to regulate federal law enforcement agencies' use of facial recognition technology to maintain its operational effectiveness while addressing civil liberty concerns?

I will follow the seven substantive steps in the following manner:

1. **Problem definition**: Literature review on capabilities and risks of facial recognition technology to define the core policy problem and need.
2. **Evidence**: Academic research on algorithmic biases and demographic disparities. Case study of Nijeer Parks to illustrate real-world impacts. Government reports and news articles on existing use and regulation.
3. **Alternatives**: Draw on literature to construct a range of policy options.
4. **Criteria**: Based on concerns highlighted in the literature, identify appropriate criteria to evaluate policy options.
5. **Outcome projection**: Using the Nijeer Parks case to envision the potential outcomes of each alternative.
6. **Trade-offs**: Highlight strengths and weaknesses of each policy option.
7. **Decision**: Recommend the ideal path forward

[27] Eugene Bardach and Eric Patashnik, *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving.*, 6th ed. (Thousand Oaks, CA: CQ Press, 2020).

II. TECHNOLOGY OVERVIEW

A. INTRODUCTION

This chapter provides critical background on FRT, tracing its historical origins, evolution, capabilities, applications, and current ethical considerations. The chapter begins by charting the early research efforts in the 1960s that laid the initial groundwork for FRT, then continues with the breakthrough eigenface method in the 1990s that enabled more sophisticated facial image analysis. It then explains the transformative impact of artificial intelligence, specifically convolutional neural networks, in enhancing FRT accuracy and flexibility.

The chapter also delves into FRT's practical applications, differentiating between one-to-one verification and one-to-many identification for law enforcement purposes. It highlights specific use cases, from unlocking smartphones to identifying suspects. Notably, the chapter examines the proliferation of FRT among law enforcement agencies and explores seminal government-funded development initiatives that accelerated its adoption.

Lastly, the chapter reviews the primary ethical concerns surrounding law enforcement's use of FRT. It raises pressing issues like privacy, transparency, racial bias, and false positives that can undermine public trust and civil liberties. The chapter highlights the wrongful arrest of Robert Williams as a crucial case revealing FRT's potential for misuse and disproportionate impact on marginalized communities.

In summary, this overview chapter traces FRT from its beginnings to its current capabilities and applications, while also highlighting the complex ethical landscape that accompanies its adoption. The chapter provides critical perspective and background analysis, laying the groundwork for further evaluating policy approaches and regulatory frameworks for law enforcement's use of FRT.

B. HISTORY OF FRT

In 1963, Woodrow Wilson Bledsoe, Helen Chan, and Charles Bisson initiated the first documented research project on facial biometric recognition at the Panoramic

Research Institute in Palo Alto, California.[28] There is little documentation detailing this project due in large part to it being funded by an "unnamed intelligence agency."[29] The Central Intelligence Agency (CIA) later revealed in 2004 that this project was their undertaking. In Bledsoe's proposal to the CIA—or rather a CIA front company—he stated the objective was to create, establish, and demonstrate the viability of using pattern recognition techniques and tools for facial recognition operations.[30] Bledsoe's computer vision process involved using horizontal and vertical grids to map the coordinates of facial landmarks. The challenge with this process is that it had difficulty with variations in age, expression, photo angle, and lighting.[31]

The next pivotal stride towards the modern incarnation of FRT, namely the eigenface method, ingeniously leveraged the variations in facial expressions and the conditions of the photographs. It implemented a series of intricate algorithmic processes in a concerted attempt to emulate the human cognitive process for the purposes of facial recognition.[32] This groundbreaking eigenface method, spearheaded by pioneers Matthew Turk and Alex Pentland, marked a significant departure from the erstwhile method that was primarily focused on individual facial landmarks, and instead opted to represent faces in a more comprehensive, holistic manner.[33]

In their innovative approach, Turk and Pentland focused on extracting the eigenvectors from facial images. Eigenvectors are a set of features that, when compiled, collectively characterize the distinctive variations between faces.[34] This mathematical

---

[28] Nikki Stevens and Os Keyes, "Seeing Infrastructure: Race, Facial Recognition and the Politics of Data," *Cultural Studies* 35, no. 4/5 (July 2021): 833–53, https://doi.org/10.1080/09502386.2021.1895252.

[29] M. Ballantyne, R.S. Boyer, and L. Hines, "Woody Bledsoe: His Life and Legacy," *AI Magazine*, 1996, 10.

[30] Stevens and Keyes, "Seeing Infrastructure," 836.

[31] Lila Lee-Morrison, *Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face* (Bielefeld University Press, 2019), https://doi.org/10.14361/9783839448465.

[32] Lee-Morrison, 65.

[33] M.A. Turk and A.P. Pentland, "Face Recognition Using Eigenfaces," in *1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Proceedings*, 1991, 586–91, https://doi.org/10.1109/CVPR.1991.139758.

[34] Turk and Pentland, 587.

representation enabled a more sophisticated approach to discerning individual facial attributes by capturing the multidimensional patterns of face structures. The process involved capturing the fundamental variations between a series of face images and transforming these into principal components, or eigenvectors. These eigenvectors were then used to form a basis set, or a "face space."[35] Every face in the training set was thereby represented as a point in this multidimensional space. When a new, unknown face needed to be identified, it was projected onto the same face space and the closest point—measured through a mathematical calculation—was considered the recognized face.

The creation of these eigenvectors gave rise to what Turk and Penland coined as "eigenfaces."[36] These eigenfaces serve as a smaller, more manageable set of basis features that capture the main variation between facial images. Rather than matching individual facial features, the eigenface method could then compare the weighted sum of these eigenfaces to derive a facial image. In this new framework, the task of identification evolved into one of pattern recognition, predicated on a comparative analysis of these eigenfaces. This represented a revolutionary shift from the previous reliance on explicit features, enabling the technology to effectively capture and compare more subtle variations between faces.

The evolution of FRT took a significant leap with the advent of AI. In recent years, there has been an unprecedented acceleration in the development of AI, reflecting an ambitious endeavor to bridge the divide between human cognition and machine processing. A crucial aspect of this endeavor has been the remarkable strides made in the field of computer vision, a sub-discipline of AI that aims to equip machines with the capability to perceive and interpret visual stimuli in the same manner as a human.

Specifically, the advancement of Convolutional Neural Networks (CNN), a type of deep learning model, has significantly enhanced the capabilities of computer vision, especially in detecting and differentiating facial images. Contemporary FRT takes advantage of these CNN algorithms to augment the original eigenface methodology,

[35] Turk and Pentland, 587.

[36] Turk and Pentland, 587.

presenting a more robust and nuanced approach to facial recognition. In employing CNN via deep learning processes, the algorithm is able to analyze a facial image, subsequently producing numerical representations of facial features based on the weighted characteristics identified within the image.[37] CNNs essentially transform an image into a data matrix by processing it through a series of layered filters. Each filter targets specific features by identifying differences in pixel characteristics, thereby creating a comprehensive, holistic representation of the facial image.[38]

Deep learning processes continuously train these algorithms, running varying filtering methodologies against pre-determined triplet image sets. These sets contain three closely related facial images: a baseline image, a different comparable image of the same individual depicted in the baseline image, and an image of a different individual.[39] The deep learning process is structured to reduce the gap between the baseline image and the comparable image, while increasing the separation between the baseline image and the image of the different person.

This methodology ensures that the baseline and comparable images, despite any variations, are mapped closely together in the high-dimensional space, while the image of the different individual is located further away. By creating a numerical matrix for each image and applying distance metrics, the CNN model effectively calculates the level of similarity between the images.[40] Once the deep learning process has been completed, the trained algorithm can then be applied to compare new images with the known ones. Given a new, unknown image, it generates a similar numerical matrix, which it then compares with those of the known images. The underlying principle is that the image of an individual

[37] Peng Lu, Baoye Song, and Lin Xu, "Human Face Recognition Based on Convolutional Neural Network and Augmented Dataset," *Systems Science & Control Engineering* 9, no. sup2 (May 3, 2021): 29–37, https://doi.org/10.1080/21642583.2020.1836526.

[38] William Crumpler and James Lewis, "How Does Facial Recognition Work? A Primer" (Center for Strategic and International Studies (CSIS), 2021), 4, https://www.csis.org/analysis/how-does-facial-recognition-work.

[39] Jianhong Lin et al., "A Lightweight Face Verification Based on Adaptive Cascade Network and Triplet Loss Function," ed. Liqin Shi, *Wireless Communications & Mobile Computing (Online)* 2022 (2022): 7–8, https://doi.org/10.1155/2022/3017149.

[40] Crumpler and Lewis, "How Does Facial Recognition Work? A Primer," 4.

will have a closer numerical representation to their own images than to those of different individuals.

In essence, the advent of AI and its ongoing development, particularly the breakthroughs in the field of computer vision and deep learning, have considerably enriched FRT's capabilities. Through the use of CNNs, modern FRT can now process and interpret facial images with a degree of sophistication that closely mirrors human facial recognition abilities. The integration of these advanced algorithms with traditional FRT methodologies has not only improved the accuracy of facial recognition but also widened its scope of applicability.

The learning aspect, which is fundamental to the application of CNN, plays an indispensable role in the successful deployment of FRT. As CNN algorithms operate on the principles of deep learning, they require extensive training with vast and varied datasets of images to successfully identify and differentiate between characteristic features, and to accurately capture the intricate variations and complexities within these images. Evidence to this effect has emerged from several empirical studies underscoring the significance of training CNNs on large, diverse datasets. One such prominent study was conducted as part of the ImageNet Large Scale Visual Recognition Challenge, an extensive project that focused on image classification. The findings of this study revealed that CNNs, when trained on larger datasets, invariably outperformed those that had been trained on smaller datasets.[41] The measure of performance was gauged in terms of accuracy, and the results demonstrated consistently higher accuracy rates for both training and testing sets when larger datasets were employed.

Reinforcing this observation, Peng Lu et al. conducted a study that focused specifically on evaluating the influence of dataset sizes and the number of training cycles, also known as epochs, on the accuracy of a CNN algorithm. The researchers designed an experiment where the researchers trained a CNN algorithm on varying dataset sizes for different numbers of epochs. The researchers concluded that larger datasets enabled the

[41] Jia Deng et al., "ImageNet: A Large-Scale Hierarchical Image Database," in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009, 248–55, https://doi.org/10.1109/CVPR.2009.5206848.

CNN algorithm to achieve higher accuracy rates in a single epoch, or training cycle. Furthermore, the study also noted that larger datasets could optimize the training process, thereby requiring fewer epochs; alternatively, utilizing more epochs can maximize accuracy if training with smaller datasets.[42]

These studies provide strong empirical support for the critical role that large and diverse training datasets play in maximizing the performance of CNNs in terms of accuracy. By training on diverse datasets, the algorithms learn to identify a wider range of characteristic features and patterns, thereby enhancing their ability to differentiate between facial images effectively. This, in turn, contributes to the enhancement of FRT's efficacy and precision.

C. APPLICATION OF FRT FOR LAW ENFORCEMENT

The utilization of FRT for law enforcement purposes traces its origins to the early 1990s, marking a significant milestone in technology's intersection with legal and security frameworks. The Defense Advanced Research Projects Agency (DARPA), a pioneering force behind this concept, launched its Face Recognition Technology (FERET) program with the objective of researching the potential of FRT applications. The primary purpose behind this initiative was to support security, intelligence, and law enforcement personnel in carrying out their duties more effectively and efficiently.[43]

Parallel to this, the National Institute of Justice (NIJ), a key research branch of the U.S. Department of Justice, began funding advancements in FRT during the late 1990s. The initial focus was on leveraging FRT software development to combat child exploitation and pornography, emphasizing the technology's potential to transform crime detection and enforcement. This marked the inception of a dedicated effort to integrate

[42] Lu, Song, and Xu, "Human Face Recognition Based on Convolutional Neural Network and Augmented Dataset," 35.

[43] P.J. Phillips, Patrick J. Rauss, and Sandor Z. Der, *FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results*, Report Number ARL-TR-995 (Arlington, VA: DARPA, 1996), 7, https://apps.dtic.mil/sti/citations/ADA315841.

advanced technological tools into law enforcement strategies.[44] The NIJ's efforts did not stop there; they continued to fund projects related to FRT well into the mid-2010s. In 2007, they facilitated the development of a mobile phone-based tool to aid law enforcement officers in the field. This innovative tool was designed to assist with identification tasks, making it possible to utilize FRT in real-time scenarios and remote locations. In 2013, another groundbreaking tool was developed with the NIJ's backing—a technology aimed at generating investigative leads for law enforcement, thereby revolutionizing the crime-solving process.[45]

The mid-2010s witnessed a significant leap in the evolution of FRT, with the advent of CNN algorithms. These advanced algorithms have contributed significantly to enhancing the accuracy and accessibility of FRT, thus playing a crucial role in propelling the technology's widespread adoption.[46] By 2016, FRT had permeated into numerous non-federal law enforcement agencies. As per an estimate by researchers at the Georgetown Law Center on Privacy and Technology, nearly a quarter of these agencies were employing FRT.[47] The Government Accountability Office conducted an audit in 2021 to shed further light on the prevalence of FRT. The audit, which examined 42 federal law enforcement agencies, revealed that 20 of these agencies were utilizing FRT in their operations.[48]

FRT serves as a powerful tool in modern society, with its applications spanning various sectors. Its practical application primarily falls within two categories— one to one

---

[44] National Institute of Justice, *History of NIJ Support for Face Recognition Technology* (Washington, DC: U.S. Department of Justice, 2020), https://nij.ojp.gov/topics/articles/history-nij-support-face-recognition-technology.

[45] National Institute of Justice.

[46] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NISTIR 8280 (Washington, DC: U.S. Department of Commerce, 2019), 16.

[47] Garvie, Bedoya, and Frankle, "The Perpetual Line-Up."

[48] Gretta L. Goodwin, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington, DC: Government Accountability Office, 2021).

verification (1:1) and one against many identification (1:n).[49] Each approach possesses distinctive characteristics and utilities, each serving critical roles in different contexts.

One to one verification, also known as 1:1 verification, is a straightforward yet effective application of FRT. In this process, an image is compared against a known image to ascertain if they depict the same person. The algorithm of the FRT calculates the similarity between two facial images and provides a match score indicating the likelihood of the images belonging to the same individual. The technology then concludes whether or not these two images are of the same person based on this match score and a predefined threshold.[50]

The 1:1 verification method is extensively used in security and access control situations, such as unlocking mobile phones, accessing secured facilities, or authenticating transactions in the banking sector. For example, modern smartphones often use FRT to verify the user's identity and unlock the device. Similarly, many businesses and organizations utilize FRT for physical access control to their premises. The technology checks an individual's face against the stored image to grant or deny access, providing a secure and contactless solution for access control.

On the other hand, one against many identification, or 1:n identification, involves comparing an image of an unknown person against an extensive image database of known individuals to establish the identity of the unknown person. In this case, the technology generates a shortlist of potential matches based on similarity scores, which can then be manually reviewed for confirmation.[51] This identification process is more complex and computationally intensive than 1:1 verification because it requires comparison with potentially thousands or even millions of facial images.

The 1:n identification method is a powerful tool for law enforcement and intelligence agencies, often used in criminal investigations and surveillance activities.

[49] John D. Woodward et al., "Biometrics: A Look at Facial Recognition" (RAND Corporation, January 1, 2003), 2, https://www.rand.org/pubs/documented_briefings/DB396.html.

[50] Crumpler and Lewis, "How Does Facial Recognition Work? A Primer," 3.

[51] Crumpler and Lewis, 3.

When an unidentified suspect's image is captured, for example, from CCTV footage or a photograph, it can be compared against a database of known criminals. The technology can provide potential matches, significantly aiding the process of identifying suspects and solving crimes. Similarly, at border control points, the faces of travelers can be compared against databases of known criminals or persons of interest, enhancing security measures. Moreover, FRT's 1:n identification method is also used in finding missing persons or identifying victims of crimes. An image of the missing person or victim can be compared against vast databases, such as surveillance camera footage or online photos, potentially providing leads to their location.

Whether it is for simple tasks like unlocking a smartphone or complex operations like identifying suspects from millions of images, FRT's practical applications are making a significant impact in various areas of society. However, while it brings enormous benefits, it's crucial to use this powerful tool responsibly, ensuring the privacy and rights of individuals are respected. As FRT continues to evolve, it promises to be a significant contributor to technological advancements, security, and societal well-being.

D. CURRENT ETHICAL LANDSCAPE

Law enforcement's use of FRT raises a multitude of ethical issues that intersect with concerns about privacy, accuracy, transparency, and fairness. Critics argue that the fundamental ethical concerns with FRT are privacy, fairness, transparency, and accountability.[52] FRT can be used on public spaces and databases, which can involve images of individuals who are not suspects in any criminal activity. The prospect of continuous, indiscriminate surveillance can erode privacy rights, creating a chilling effect on free speech and assembly. The right to anonymity in public spaces, perhaps a cornerstone of a democratic society, may be threatened.

There are significant ethical issues related to the accuracy of FRT, especially when it comes to false positives and racial bias. The wrongful arrest of Robert Williams in Detroit in 2020 was a significant case that highlighted the fallibility and profound implications of

[52] Garvie, Bedoya, and Frankle, "The Perpetual Line-Up."

misused facial recognition technology.[53] Williams, wrongly identified by FRT as the perpetrator of a larceny, spent approximately thirty hours in custody before being released, with his case getting dropped less than two weeks later due to lack of evidence.[54] This case underscored the importance of appropriate use, human oversight, and technical refinement of FRT. The Williams case became an exemplar of the flaws in FRT, specifically its racial bias. Studies have shown that FRT algorithms used at the time of Williams' arrest disproportionately misidentified people of color, leading to potential bias in law enforcement.[55] Williams, a black man, became a victim of this bias. His arrest served as a stark reminder of the need for technology to ensure fairness and equal treatment, reiterating that advancements in FRT should not reinforce systemic bias or create new forms of discrimination. Since Williams' arrest, the performance of FRT algorithms has improved dramatically, minimizing demographic algorithmic bias.[56] Nonetheless, law enforcement agencies need to remain cognizant of the potential for disparate impact without appropriate human oversight over FRT.

Furthermore, the case amplified the debate on privacy and civil rights concerns surrounding FRT. The incident raised questions about the extent of surveillance, the potential for unwarranted intrusion, and the possible infringement on individuals' right to privacy. The implications of the Williams case extend to policymaking, urging the need for legislation that adequately addresses the ethical, social, and legal ramifications of law enforcement's use of FRT. It emphasized the importance of checks and balances, transparency, accountability, and stringent policies in deploying FRT, highlighting the need for these tools to be used responsibly, with rigorous human oversight.

Another crucial ethical aspect is the transparency of FRT use by law enforcement agencies. Without clear guidelines, policies, and public knowledge about when, how, and

---

[53] Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, sec. Technology, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[54] Hill.

[55] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018): 1–15.

[56] Grother, Ngan, and Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, 41.

why FRT is used, there is a risk of public trust erosion. Public scrutiny is essential for any technology that has such far-reaching implications for civil liberties. Notably, transparency is not just about disclosing the use of technology, but also about explaining how it works, its limitations, and the steps taken to ensure the prevention of misuse.

In addition to these concerns, there are potential threats to the presumption of innocence. If law enforcement heavily relies on FRT in identifying suspects, the technology's determinations could unduly influence the investigations, potentially biasing the process against the identified individuals from the outset. This could lead to a form of presumed guilt before any formal investigative proceedings have been initiated, undermining the fundamental legal principle that individuals are innocent until proven guilty.

The last but equally important ethical issue is the need for public acceptance at large. While law enforcement agencies may argue that FRT is a necessary tool for maintaining public safety, it is crucial that these technologies' adoption does not occur without public knowledge and acceptance. As FRT is an intrusive technology that can fundamentally alter public spaces' nature and society at large, a comprehensive public debate about its benefits and risks, as well as its legal and ethical implications, is of paramount importance. In a democratic society, informed lawmakers—serving as the voice of the people—should regulate law enforcement's use of FRT in a manner that is publicly acceptable.

The ethical landscape of law enforcement's use of FRT is a complex web of competing interests and values. Balancing the potential benefits of FRT in fighting crime and maintaining public safety with the protection of civil liberties is a challenging ethical task that requires careful deliberation and robust regulatory frameworks. Additionally, policy makers and stakeholders should continually monitor and reassess the ethical landscape due to potential secondary effects as FRT adoption increases. For example, strategic deployment of FRT could, instead of reducing crime, displace crime from one community to another, potentially leading to inequitable policing. Given the rapidly evolving nature of the technology and its growing prevalence, addressing these ethical challenges is both urgent and necessary.

E. CONCLUSION

In closing, this chapter has provided a comprehensive overview tracing the origins, evolution, capabilities, applications, and ethical considerations pertaining to FRT. Beginning with the early 20th century research into using algorithms and biometrics for facial analysis, the chapter charted the key breakthroughs that enabled FRT to become a viable technology. The eigenface method and the integration of CNNs via deep learning were pivotal developments that enhanced FRT's sophistication and accuracy.

On the application front, FRT is now widely used for both security access control via one-to-one facial verification as well as investigative leads and surveillance through one-to-many identification. Law enforcement agencies' adoption of FRT is increasing, with agencies utilizing it for crime investigation and border security purposes. However, FRT's law enforcement applications have also raised pressing ethical concerns regarding privacy, transparency, racial bias, and erosion of civil liberties. The wrongful arrest of Robert Williams spotlighted the potential for misuse and disproportionate impact on marginalized groups.

In summary, while FRT brings numerous benefits for security and efficiency, it also poses significant risks if deployed irresponsibly and without oversight. Achieving the right balance will require robust policy frameworks that maximize FRT's advantages while also instituting necessary checks against misuse. As this overview elucidates, FRT is a powerful technology that warrants careful governance to ensure its ethical and socially responsible development. With prudent regulation and continual reassessment, FRT can fulfill its immense potential as a transformative innovation that enhances safety and efficiency while also upholding civil rights.

III. COMPARING EU'S LAW ENFORCEMENT DIRECTIVE

A. INTRODUCTION

The previous chapter discussed how the proliferation of FRT has raised significant concerns around privacy, civil liberties, and the potential for bias or misuse. This underscores the need for thoughtful policy frameworks to regulate the use of FRT, balancing public interests with individual rights. As FRT increasingly enters the domain of law enforcement, it is essential that proper oversight governs its deployment and usage. This chapter analyzes principles from the European Union's (EU) Law Enforcement Directive (LED) as a comparative model for constructing a privacy-focused policy framework to regulate U.S. federal law enforcement's use of FRT. The LED provides a set of baseline principles designed to uphold data protection standards for EU policing and criminal justice authorities.

This chapter covers the purpose and scope of the LED, highlighting its applicability to regulating biometric data processing like FRT. It summarizes the LED's core principles of lawfulness, fairness, and transparency; purpose limitations; data minimization; accuracy; storage limitations; integrity and confidentiality; and accountability.[57] The chapter compares these principles to existing U.S. regulations and frameworks, analyzing their potential benefits and implementation challenges within the specific context of U.S. federal law enforcement. It pays particular attention to principles around lawfulness, purpose limitations, and accountability given the current uncertainties around FRT's legal foundations and oversight needs.

Finally, the conclusion of this chapter weighs the merits of adapting certain LED principles into a U.S. framework legislators can optimize for governing facial recognition use, while accounting for operational realities and legal evolution. It argues that components of the LED provide a starting point to develop policies upholding privacy and civil liberties.

[57] Directive (EU) 2016/680 Law Enforcement Directive, OJ L 119 § (2016), chap. II, http://data.europa.eu/eli/dir/2016/680/oj/eng.

B. ANALYZING THE LED

A critical element of FRT use is the protection of the data rights of subjects. FRT relies on capturing and consuming vast amounts of personal data—data subject to privacy protection. The International Organization for Standardization (ISO) defines biometric characteristics as a "characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition."[58] ISO specifically states that face topography is an example of a biometric characteristic.[59] DHS, like other federal agencies and organizations, is required to safeguard personally identifiable information data, like biometric characteristics.[60] Accordingly, FRT regulation should take into consideration the novel challenges of safeguarding data rights in the face of big data collection and consumption.

In 2016, the EU passed the General Data Protection Regulation (GDPR) to provide a comprehensive and harmonized framework for data rights protection across the EU.[61] The GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[62] As part of its ongoing efforts to regulate applications of artificial intelligence, the EU relies on the GDPR to ensure that non-law enforcement entities use FRT with appropriate safeguards to protect the data rights of EU citizens. However, the EU saw fit to enact a separate, but related, piece of legislation, the LED, to guide member states with a unified framework to achieve a balance between the

58 International Organization for Standardization, *ISO/IEC 2382–37 Information Technology – Vocabulary – Part 37: Biometrics* (Geneva: International Organization for Standardization, 2022), 2.

59 International Organization for Standardization, 2.

60 Department of Homeland Security, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, DHS Directive 262–16 (Washington, DC: Department of Homeland Security, 2022).

61 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119 § (2016).

62 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 34.

legitimate objectives of law enforcement-related data processing and the data rights of its citizens.[63] When using FRT for law enforcement purposes, EU member states must comply with the principles of the LED.[64]

The LED aims to protect the privacy of EU citizens by providing strict rules on how personal data is collected, processed, and stored by law enforcement agencies.[65] The LED sets regulations that govern the way competent law enforcement authorities handle personal data for the purposes of "preventing, investigating, detecting or prosecuting criminal offenses," as well as executing criminal penalties.[66] The primary goal of this directive is to create a standard framework for processing personal data in criminal investigations and to harmonize data protection laws throughout the European Union. This framework encompasses a wide variety of personal data, including sensitive information such as names, addresses, criminal records, genetic and biometric data.[67]

To protect the rights of individuals, the LED delineates various specific entitlements, including the right to access, correct, delete, and object to the processing of personal data under certain conditions.[68] Additionally, the directive mandates that supervisory authorities be established to ensure compliance with the regulations, provide guidance to law enforcement entities and data subjects, and investigate and resolve complaints from data subjects.[69]

The LED also directs member states to impose "effective, proportionate and dissuasive" penalties for violating the provisions of the directive.[70] For example, in the UK the Information Commissioner's Office has the authority to provide guidance and

[63] European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018).

[64] Tambiama Madiega and Hendrik Mildebrath, *Regulating Facial Recognition in the EU*, EPRS Report PE 698.021 (Brussels: European Parliamentary Research Service, 2021).

[65] Directive (EU) 2016/680 Law Enforcement Directive.

[66] Directive (EU) 2016/680 Law Enforcement Directive, para. 35.

[67] Directive (EU) 2016/680 Law Enforcement Directive.

[68] Directive (EU) 2016/680 Law Enforcement Directive, para. 40.

[69] Directive (EU) 2016/680 Law Enforcement Directive, para. 48.

[70] Directive (EU) 2016/680 Law Enforcement Directive, para. 57.

oversight for law enforcement data processing as outlined in the LED. The Information Commissioner can impose a fine on law enforcement entities that fail to comply with the LED, a fine of up to £17.5 million.[71] However, the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs' *Assessment of the Implementation of the Law Enforcement Directive* concluded that the allocation of powers to oversight authorities under the LED is weaker than that of the GDPR.[72] Unlike the GDPR, the LED significantly curbs the corrective powers of oversight authorities, excludes the power to enforce compliance with data subject requests, and command the suspension of data flows to third countries. The LED's limitations also extend to the investigative powers of the oversight authorities.[73]

The LED is built upon a set of guiding principles that aim to protect the privacy and rights of EU citizens. These main principles outlined in the LED are:

1. Lawfulness, fairness, and transparency
2. Purpose limitations
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability[74]

This section will analyze these principles of the LED, identify potential barriers to adoption in U.S. regulation, and provide recommendations as to which principles could provide the most benefit to FRT regulation for U.S. federal law enforcement agencies.

1. Lawfulness, Fairness, and Transparency

Under this principle, personal data must be processed lawfully, meaning that the processing must be based on a legal basis set out in the LED or other applicable EU or

[71] "Guide to Law Enforcement Processing," Information Commissioners Office, accessed April 12, 2023, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/.

[72] Thomas Marquenie and Plixavra Vogiatzoglou, *Assessment of the Implementation of the Law Enforcement Directive* (Luxembourg: Publications Office of the European Union, 2022), 93, https://data.europa.eu/doi/10.2861/691965.

[73] Marquenie and Vogiatzoglou, 95.

[74] Directive (EU) 2016/680 Law Enforcement Directive.

member state law.[75] For example, processing may be "necessary for the performance of a task carried out in the public interest".[76] Personal data must also be processed fairly, which means that the processing must not be discriminatory, and must not result in unfair or unjustified effects on the data subject. The principle of fairness requires that data subjects are treated in a manner that is consistent with their legitimate interests and rights.[77] The principle of transparency requires that personal data must be processed clearly and understandable to the data subject. This means that the competent authority must provide the data subject with clear and concise information about the purposes and legal basis for the processing of their personal data, as well as information about their rights as data subjects.[78]

The principles behind lawfulness, fairness, and transparency can be beneficial for U.S. regulation to uphold values of privacy and civil liberty; however, a potential barrier to the U.S. fully adopting the principle of lawfulness is in establishing the appropriate legal basis. The U.S. legal system has yet to fully address the legal implications of using advanced technology like FRT on publicly acquired images.[79] In 2019, the U.S. Court of Appeals, 9th Circuit addressed Facebook's use of facial recognition on its database of images.[80] While this was a civil case focusing on a private company's use of FRT, it acknowledged Fourth Amendment issues arising from technological advances, specifically the uncertain calculus of a reasonable intrusion of privacy when utilizing advanced technologies.[81] In 2018, the Supreme Court examined the Fourth Amendment in the context of advanced technology in Carpenter v. US.[82] While the court acknowledged the third party doctrine—whereby the expectation of privacy is diminished when information

[75] Directive (EU) 2016/680 Law Enforcement Directive, para. 33.

[76] Directive (EU) 2016/680 Law Enforcement Directive, para. 16.

[77] Directive (EU) 2016/680 Law Enforcement Directive, para. 26.

[78] Directive (EU) 2016/680 Law Enforcement Directive, para. 26.

[79] Lord, "The Cost of Possibility," 44.

[80] Patel v. Facebook, Inc., 932 F. 3d 1264 (Court of Appeals, 9th Circuit 2019).

[81] Patel v. Facebook, Inc., 932 F. 3d at 1273.

[82] Carpenter v. U.S., 138 S. Ct. 2206 (Supreme Court 2018).

is voluntarily offered to a third party—it questioned whether the third party doctrine's no expectation of privacy should remain when government uses a technology that enables it to obtain information that is "detailed, encyclopedic, and effortlessly compiled."[83] It may take some time for the U.S. judiciary to evaluate the Fourth Amendment considerations for law enforcement agencies using FRT on publicly acquired images.

2. Purpose Limitations

The goal of purpose limitation is to make certain that organizations gather and use personal data only for distinct and lawful reasons. Under the principle of purpose limitation, data controllers must specify the purpose for which they are collecting personal data and must only use the data for that purpose. The principle of purpose limitation is a fundamental aspect of data protection and is designed to ensure that individuals have control over their personal data and that it is not used in a way that could be harmful or discriminatory.[84] By limiting the purposes for which data can be used, the LED seeks to protect individuals' privacy and ensure that data is not used in ways that are unexpected or harmful.

The U.S. Privacy Act of 1974, which established the Fair Information Practice Principles (FIPPs), similarly includes a purpose limitation principle.[85] While not requirements, FIPPs serve as a guideline for how federal agencies should evaluate privacy-impacting programs to ensure that information is handled in a manner that respects individual privacy and security.[86] Accordingly, the U.S. could ensure certain privacy safeguards by codifying certain elements of purpose limitations in regulation specific to the context of law enforcement's use of FRT.

---

[83] Carpenter v. U.S., 138 S. Ct. at 2209.

[84] Directive (EU) 2016/680 Law Enforcement Directive, para. 51.

[85] "Office of Privacy and Civil Liberties | Privacy Act of 1974," June 16, 2014, https://www.justice.gov/opcl/privacy-act-1974.

[86] "Fair Information Practice Principles (FIPPs)," Federal Privacy Council, accessed July 29, 2023, https://www.fpc.gov/resources/fipps/.

3. Data Minimization

Data minimization requires data controllers to carefully consider what data they need to collect and how they will use it. They are obligated to make sure that the personal data they gather and handle is sufficient, pertinent, and restricted to what is essential for the specified objective.[87] This means that they must avoid collecting any data that is not strictly necessary for their purposes, and they must not collect more data than is needed. Under the LED, data controllers must also regularly review their data processing activities to ensure that they are still necessary for the intended purpose. If the data is no longer needed or relevant, it must be deleted or anonymized.

The principle of data minimization is important because it helps to protect individuals' privacy and reduce the risk of data breaches and other data-related harms. By collecting and processing only the minimum amount of data necessary, data controllers can reduce the risk of data breaches and limit the potential damage caused by such breaches. Additionally, by minimizing the amount of data that is collected and processed, individuals' privacy is better protected, as there is less data available that can be used to identify them or infer sensitive information about them.

This principle may be difficult to implement in U.S. regulation. While this principle takes great effort to protect individual data security, it could hinder big data and predictive analytics efforts, which have proven to be effective law enforcement tools.[88] Data analytics requires the analysis of large amounts of seemingly unrelated data, which is ostensibly contrary to the principle of data minimization. In its guidelines on law enforcement's use of facial recognition, the European Data Protection Board suggests layers of "pseudonymization"—applying a random unique identifier to personal data and using that identifier during analysis instead of the actual personal or biometric data—before and

[87] Directive (EU) 2016/680 Law Enforcement Directive, chap. IV.

[88] Johan L. Perols et al., "Finding Needles in a Haystack: Using Data Analytics to Improve Fraud Prediction," *The Accounting Review* 92, no. 2 (2017): 221–45, http://www.jstor.org/stable/26550651.

during the processing of personal data to satisfy the principle of data minimization.[89] U.S. regulators and policy makers may need to examine the concept of pseudonymization to determine its feasibility as a means for upholding data minimization.

4. Accuracy

According to the accuracy principle, data controllers are required to take sensible measures to make sure that personal data is correct, comprehensive, and current. They must also ensure that any inaccurate or incomplete data is rectified or erased without delay.[90] This principle is important because inaccurate or outdated data can cause harm to individuals, for example, if it leads to incorrect decisions being made about them. The principle of accuracy applies to all personal data, including sensitive data such as health information, and to all forms of processing, including automated processing. Data controllers must also ensure that any third parties to whom they disclose personal data are informed of any inaccuracies and are required to rectify them.

The LED also requires data controllers to implement appropriate measures to ensure the accuracy of personal data, such as data validation checks, data entry controls, and regular data audits. They must also ensure that individuals are informed of their right to have their personal data rectified or erased if it is inaccurate or incomplete.[91]

No great barriers to implementation for this principle. Similar efforts are already in place in certain institutions. For example, the Code of Federal Regulations already requires accuracy and completeness provisions in Criminal Justice Information Systems.[92]

---

89 European Data Protection Board, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement* (Brussels: EDPD, 2023), 4, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

90 Directive (EU) 2016/680 Law Enforcement Directive, chap. II.

91 Directive (EU) 2016/680 Law Enforcement Directive, chap. II.

92 "Judicial Administration," 28 C.F.R. 20 § (1999), https://www.ecfr.gov/current/title-28/chapter-I/part-20.

5. Storage Limitations

In line with the storage limitation principle, data controllers are obligated to keep personal data only for the duration needed to fulfill the objectives for which it was originally gathered. This means that data controllers must regularly review the personal data they hold and ensure that any data that is no longer necessary is deleted or anonymized.[93] This is important because retaining personal data for longer than necessary increases the risk of unauthorized access, accidental loss or damage, and other security breaches. Some exemptions exist for the storage limitation principle; for instance, controllers can retain personal data for extended periods for reasons such as public interest archiving, scientific or historical studies, or for initiating, pursuing, or defending legal actions.[94]

While this principle ultimately relies on how regulators define public interest, there may be a pathway to implementation in the U.S. via anonymization. Research has shown that the effects of aging have significant consequences on the performance of facial recognition algorithms.[95] Consequently, maintaining old images in a database for the purposes of identification may prove ineffective. However, the algorithmic training process can still benefit from using old images, but anonymizing these images should not adversely affect this process.

6. Integrity and Confidentiality

In accordance with the integrity and confidentiality principle, data controllers are required to put in place suitable technical and organizational safeguards to secure the privacy of personal data.[96] This includes measures to protect against unauthorized access, accidental loss or destruction, and other security breaches. They must also ensure that

[93] Directive (EU) 2016/680 Law Enforcement Directive, chap. II.

[94] Directive (EU) 2016/680 Law Enforcement Directive, chap. II.

[95] Manisha M. Sawant and Kishor M. Bhurchandi, "Age Invariant Face Recognition: A Survey on Facial Aging Databases, Techniques and Effect of Aging," *The Artificial Intelligence Review* 52, no. 2 (August 2019): 981–1008, https://doi.org/10.1007/s10462-018-9661-z.

[96] Directive (EU) 2016/680 Law Enforcement Directive, chap. II.

personal data is processed in a way that maintains its confidentiality, meaning that it is only accessed and disclosed to authorized individuals or entities.[97]

To comply with the principle of integrity and confidentiality, data controllers must implement a range of technical and organizational measures, including encryption, access controls, data backups, and staff training. They must also conduct regular risk assessments to identify and mitigate any security risks that may arise. In addition, data controllers must ensure that any third-party service providers that they use to process personal data also implement appropriate security measures.[98]

This principle could be particularly useful when U.S. agencies utilize third-party service contracts for FRT. Mandating robust contractual agreements that require third-party providers to have certain organizational measures in place could ensure that agencies process personal data in a way that is consistent with the principle of integrity and confidentiality. For example, if a third-party provider had staff that could access agency submitted probe photos and the subsequent results of the FRT analysis of that probe photo, then the aim should be to require that those staff members are subject to measures that ensure personal data is secure and confidential.

7. Accountability

Under the principle of accountability, data controllers must document their data processing activities and keep records of the measures they have taken to comply with the LED. Data controllers must also appoint a data protection officer (DPO). The DPO is responsible for monitoring the organization's compliance with the LED and for advising on data protection matters. Data controllers are also obligated to inform both the appropriate regulatory body and the individuals impacted in the event of any data breaches.[99] To comply with the principle of accountability, data controllers must also ensure that their staff are trained and aware of the LED's requirements.[100]

---

[97] Directive (EU) 2016/680 Law Enforcement Directive, para. 28.

[98] Directive (EU) 2016/680 Law Enforcement Directive, chap. IV.

[99] Directive (EU) 2016/680 Law Enforcement Directive, para. 61.

[100] Directive (EU) 2016/680 Law Enforcement Directive, para. 63.

Given that government agencies are subject to routine auditing and are thus required to maintain a robust auditing apparatus, legislating the likes of a DPO for FRT could be a logical addition to existing auditing measures. Lawmakers will, however, need to be cognizant of the resource and organization requirements for such an accountability system to be effective. Specifically, accountability and oversight authority may need to be strictly defined to prevent the aforementioned downside of the LED in its failure to adequately define such oversight authority.

C. RECOMMENDATIONS FROM THE LED

An assessment of the LED revealed that its biggest weakness lies in harmonization efforts across EU member states. Specifically, several member states employed varying interpretations of the underlying principles of the LED such that implementation began to diverge.[101] However, the principles of the LED can still be useful if narrowly focused to a specific sector, for instance, U.S. federal law enforcement's use of FRT. U.S. federal law enforcement agencies are employing FRT without formal policy and without a regulatory framework to create sound policy. The FISWG offers law enforcement agencies some good frameworks for operational and technical FRT standards; however, it does not adequately address underlying biometric standards and principles or privacy related issues.[102] Additionally, the FISWG has no formal authority in guiding agencies to develop sound policy that gives privacy and civil liberties due consideration. Adopting certain principles of the LED can help to fill this gap and contribute to a robust legislative framework for law enforcement's use of FRT. Specifically, the principles of lawfulness, fairness, and transparency; purpose limitations; and accountability.

101 Marquenie and Vogiatzoglou, *Assessment of the Implementation of the Law Enforcement Directive*, 7.

102 "FISWG," https://www.fiswg.org/index.html.

1. Lawfulness, Fairness, and Transparency

The legal underpinnings for biometric collection, specifically pertaining to FRT, remain in a state of considerable uncertainty and continuous evolution.[103] Owing to the novelty of this technology, and the myriad legal questions it raises, the courts are likely to take a considerable amount of time to clearly delineate its legal parameters. Hence, it is paramount that any policy framework addressing this issue must be designed to withstand and adapt to this uncertainty, thereby ensuring that it remains relevant as the legal landscape around the technology continues to take shape.[104]

A well-structured policy framework should incorporate key principles such as transparency and fairness at its core, and these two pillars should guide the use of FRT, particularly within the domain of law enforcement. Transparency, in this context, refers to clearly communicating the usage, scope, and the mechanisms behind FRT, fostering an understanding of the technology among the public and the various stakeholders involved. It means openly disclosing the conditions under which FRT is deployed, the data it collects, and the methods for processing and storing that data.

On the other hand, the principle of fairness calls for an equitable application of FRT. This implies that the use of the technology must not disproportionately or unfairly impact certain communities or individuals. Given the increasing concerns over the potential for FRT to perpetuate biases or lead to discrimination, policies need to address these risks proactively.[105] This could involve rigorous testing of FRT algorithms for bias, regular audits of their use in the field, and establishing mechanisms for accountability when unfair impacts are detected. Moreover, the principle of fairness should extend to giving individuals an opportunity to contest decisions made by FRT, particularly in a law enforcement context. Any adverse decision should be subjected to a review where human intervention can mitigate potential errors or biases.

---

[103] Lovallo, "Big Brother's Fall Brings Liberty to All: Addressing the Urgency for Strict Regulation Governing Law Enforcement Use of Facial Recognition Technology in Texas."

[104] Gray, "Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies."

[105] Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short."

While the legal foundations for the use of FRT remain unstable, developing a robust policy framework based on the principles of transparency and fairness can help navigate this fluid situation. Such a framework could alleviate some legal concerns, minimize the risk of disparate impact, and foster greater public trust in the use of this technology. The Violent Crime Control and Law Enforcement Act of 1994 mandates transparency in law enforcement's excessive force reporting via a publicly published report on such instances.[106] Rights advocacy groups, like the ACLU, use these published reports to educate the public and take action against government agencies showing a pattern of abuse.[107] The transparency of the data is a critical element in establishing public trust. Mandating similar transparency in FRT abuse—or, more generally, data rights abuse—may help to establish public trust in law enforcement's use of FRT.

2. Purpose Limitations

A key area of debate within the context of FRT revolves around the use of publicly accessible photographs. The use of such images, coupled with FRT, poses significant challenges to established notions of privacy. Consequently, the traditional litmus test for determining a reasonable expectation of privacy will need to be thoroughly reassessed, particularly considering the growing prominence of the online realm.[108]

In this context, delineating precise limitations on the usage of FRT based on how a particular image was obtained will become an essential aspect of privacy considerations. It would be necessary to evaluate whether an image, despite being publicly accessible, can be used without explicit consent and to determine what exceptions, if any, could apply. The policy would need to balance the interests of public safety, law enforcement needs, and the preservation of individual privacy rights.

---

[106] Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103–322, § 210402 (1994).

[107] Jenn Rolnick Borchetta and Brandon Chapman, "State and Local Governments Must Take Responsibility for Police Violence," ACLU, June 22, 2023, https://www.aclu.org/news/criminal-law-reform/state-and-local-governments-must-take-responsibility-for-police-violence.

[108] Mariko Hirose, "Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology," *Connecticut Law Review* 49 (2017 2016): 1591, https://heinonline.org/HOL/Page?handle=hein.journals/conlr49&id=1635&div=&collection=.

Furthermore, another crucial aspect of the policy framework would involve defining restrictions on how FRT results can be used to establish probable cause.[109] This is important for jurisprudence as it could influence the standards for law enforcement investigations and the admissibility of evidence in court. For instance, should a facial recognition match alone constitute probable cause for an arrest, or should it be corroborated with other evidence?

The implications of such policy decisions on privacy rights, civil liberties, and racial and ethnic disparities cannot be overlooked. A thoughtful, robust policy framework would need to address these concerns, fostering public trust while ensuring the technology serves to enhance rather than infringe upon individual rights. Pursuant to the E-Government Act of 2002, DHS conducts and publicly publishes privacy impact assessments (PIA) for each technology system it utilizes.[110] PIAs analyze privacy risks and how the system mitigates those risks. For example, DHS assessed Immigration and Customs Enforcement's (ICE) use of facial recognition services and concluded that ICE upholds purpose limitation by requiring users to acknowledge and provide evidence that each use is pursuant to an ongoing investigation.[111] While PIAs can serve as a mechanism to inform the public that principles like purpose limitation are upheld, the GAO reported that some agencies failed to publish PIAs prior to the implementation of the system.[112] Expanding regulations to mandate timely PIAs could help ensure privacy risks are appropriately assessed prior to deployment.

3. Accountability

In crafting policy frameworks, accountability always stands out as a fundamental aspect. The LED advocates for a unique accountability infrastructure when it comes to

---

109 Benedict, "The Computer Got It Wrong," 866–70.

110 E-Government Act of 2002, Pub. L. No. 107–347, § 208 (2002).

111 Department of Homeland Security, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services* (Washington, DC: DHS, 2020), 22, https://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services.

112 Diana Maurer, *Face Recognition Technology: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy*, GAO-17-489T (Washington, DC: Government Accountability Office, 2017).

biometric privacy, a principle that, despite potentially presenting significant administrative challenges, could greatly benefit FRT programs. Notably, the implementation of FRT initiatives may require dedicated and adequately trained personnel who can thoroughly comprehend the intricate dynamics between privacy considerations and the efficacy of FRT. The presence of knowledgeable personnel would contribute to ensuring that FRT is utilized responsibly, with proper adherence to privacy rights and ethical norms. This accountability structure should also encompass clear protocols for reviewing decisions and addressing any potential misuse of the technology.

Furthermore, the roles of various actors in this accountability infrastructure must be explicitly defined, which extends to the oversight authority as well. The LED, despite its merits, falls short in adequately delineating oversight authority, a deficiency that can potentially lead to ambiguities and issues in enforcing accountability. It is, therefore, imperative that any policy framework for FRT clearly sets out the oversight authority's responsibilities and powers. The parameters of oversight need to be strictly defined to avoid any misinterpretation or potential abuse of authority. This includes defining who is responsible for oversight, what aspects they oversee, and the range of their decision-making powers.

In addition, there must be mechanisms in place for regular audits, transparency reports, and independent evaluations to monitor adherence to privacy standards and the overall performance of FRT programs. Such measures would enhance the accountability infrastructure, ensuring that FRT is employed in a manner that respects individual privacy and civil liberties, while simultaneously meeting law enforcement objectives. Pursuant to the LED, the UK established the Information Commissioner's Office (ICO) to provide oversight over law enforcement agencies' data processing.[113] However, there are concerns that entities like the ICO lack sufficient authority to be truly effective.[114] Establishing an independent oversight entity could be beneficial in the US; however, to avoid the pitfalls

[113] Information Commissioner's Office, "Guide to Law Enforcement Processing."

[114] Marquenie and Vogiatzoglou, *Assessment of the Implementation of the Law Enforcement Directive*, 92–93.

seen in the EU, U.S. regulators should ensure that oversight entities have appropriate authority.

D. CONCLUSION

This analysis posits that certain crucial tenets of the European Union's LED can provide an invaluable structure for regulating the use of FRT by U.S. federal law enforcement agencies. The LED's principles are designed to strike a delicate balance between upholding privacy rights and furthering legitimate law enforcement objectives in the processing of biometric data.

In particular, the principles of lawfulness, fairness, transparency, purpose limitations, and accountability stand out as particularly relevant for effective FRT oversight. By ensuring that the use of FRT is lawful, fair, and transparent through the development and implementation of lucid policies and explicit disclosures, the current uncertainties around legal foundations and public perceptions can be effectively addressed. Strictly limiting the purposes for which FRT can be used and establishing robust accountability mechanisms, such as the appointment of dedicated oversight personnel and regular audits, can significantly enhance privacy protections.

However, some principles espoused by the LED may require adaptation for effective application within the context of FRT. Data minimization could potentially come into conflict with the need to build comprehensive image databases, which are essential for the successful functioning of facial recognition systems. Storage limitations pose a similar constraint for retaining images over time, a practice that can be instrumental in improving the accuracy of the technology. The oversight provisions within the LED also suffer from a lack of specificity, which risks creating ambiguity in enforcement.

Despite these potential hurdles, the LED provides a strong model for key elements of a privacy-focused FRT regulatory framework, which the U.S. currently lacks. Certain principles require thoughtful consideration to balance privacy aims with operational needs. Further legal evolution will be necessary to keep pace with the societal impacts of rapidly evolving facial recognition capabilities. Regulations regarding FRT must be adaptable to both enhance protections and support beneficial uses as technology, laws, ethics, and public

opinion continue to shift. A comprehensive framework built on core principles of lawfulness, fairness, accountability, and purpose limitations can provide an ethical foundation for navigating these complex issues.

In conclusion, the principles contained within the LED highlight important areas of focus that can guide U.S. policymakers in their pursuit of developing a robust regulatory framework for governing law enforcement applications of FRT through periods of significant social and technological change. By doing so, it is possible to harness the public safety benefits of FRT while simultaneously mitigating risks of overreach, bias, and erosion of privacy. Navigating the course of FRT governance in the U.S. is a task of paramount importance, as the decisions made today will set the course for how this increasingly ubiquitous technology impacts communities for decades to come. With careful planning and policy adaptations, the U.S. can use the LED principles as a starting point for creating a balanced, efficient, and ethical FRT use that respects citizens' rights, keeps pace with technological advancements, and caters to law enforcement needs.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. POLICY ANALYSIS

A. INTRODUCTION

This chapter synthesizes the information in the previous chapters in a policy analysis for law enforcement's use of FRT. As FRT becomes increasingly embedded in policing practices, critical questions arise regarding proper governance, oversight, and regulation of this powerful technology. The purpose of this policy analysis is to systematically assess the complex issues surrounding law enforcement's use of FRT in order to identify the most prudent policy solutions.

The chapter begins by clearly defining the core problem—the lack of clear regulations governing law enforcement's use of FRT, which raises significant concerns about privacy, consent, transparency, and algorithmic bias. It highlights how the unbridled use of FRT in policing can lead to infringements of civil liberties as well as wrongful arrests stemming from algorithmic errors and lack of oversight.

Next, the analysis assembles robust evidence from academic research, investigative journalism, and real-world case studies that demonstrate the risks and implications of the status quo. The evidence covers key issues like algorithmic bias, lack of transparency and informed guidelines, and the potential for FRT to enable invasive surveillance and erosion of public trust.

With the problem and evidence established, the chapter puts forward five policy alternatives: comprehensive regulation, an outright ban, a moratorium, requiring a warrant, or maintaining the status quo. It analyzes the projected outcomes of the alternatives against selected criteria of effectiveness, proportionality, cost, and impact on public trust.

Based on this thorough analysis, the chapter recommends comprehensive regulation as the optimal policy solution. It argues that this approach can constrain unfettered use of FRT while preserving public safety benefits if coupled with appropriate oversight mechanisms, flexibility, and continuous stakeholder engagement.

B. SEVEN-STEP ANALYSIS

1. Define the Problem

FRT has emerged as a critical tool in law enforcement, opening up new dimensions in criminal investigations, public security, and law enforcement procedures. However, as this powerful technology gets further embedded into the fabric of policing, it brings with it a raft of ethical, legal, and social implications that require careful consideration. The central problem is the largely unregulated use of FRT by law enforcement, leading to serious concerns about privacy, consent, transparency, and potential bias.[115] The capacity of FRT to scan, analyze, and identify individuals from digital images or video feeds, essentially in real-time, has profound implications for personal privacy. With widespread surveillance cameras and growing databases of digital images, people can be tracked and identified without their knowledge or consent. This not only has the potential to erode the public's reasonable expectation of privacy but may also facilitate the misuse of FRT for nefarious purposes.

Adding to this is the issue of consent. Currently, individuals may not have a say in whether their biometric data is captured and used by FRT systems. The absence of a comprehensive legal framework means there are few checks and balances to prevent abuse. This is particularly relevant given the increasing commercialization of FRT systems, with companies offering law enforcement agencies access to their private databases of digital images. Transparency is another key concern. There is currently little clarity about where, when, and how FRT is being used by law enforcement. Without adequate disclosure about the application of FRT, the public is left in the dark about the extent of its use, making it difficult to hold law enforcement agencies accountable for their actions.

Perhaps one of the most prolific issues surrounding the use of FRT is the potential for algorithmic bias, which can lead to wrongful identification and disproportionately impact certain demographic groups. Research has shown that FRT systems can perform

[115] Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short."

less accurately for people of color, women, and the elderly, raising the specter of discrimination and heightening the risk of wrongful arrests or surveillance.[116]

The problem at hand, therefore, is multifaceted. It involves the need to balance the undeniable benefits of FRT in aiding law enforcement with the fundamental rights to privacy, consent, and freedom from discrimination. It also underscores the urgent need for a robust regulatory framework that ensures transparency and accountability in the use of FRT by law enforcement. The current lack of regulation and oversight of law enforcement's use of FRT has created an environment where the technology has the potential to be misused and abused. While the benefits of FRT for public safety and security are clear, without proper regulations and guidelines, these benefits are offset by serious concerns about civil liberties, privacy, and potential misuse. The need to establish a sound policy framework for the use of FRT by law enforcement is therefore not just important, but critical.

2. Assemble Some Evidence

Understanding the profound implications of FRT in law enforcement requires an in-depth examination of available evidence. Key areas of focus include academic research and case studies that highlight the current landscape of law enforcement's use of FRT. Algorithmic bias has been a consistent subject of concern within the academic community investigating FRT. Several research initiatives have demonstrated a troubling pattern of gender and racial disparities in FRT's performance. In a seminal study, Joy Buolamwini, a researcher at the MIT Media Lab, discovered that the facial recognition technology employed by IBM demonstrated a stark contrast in accuracy depending on the demographics of the subject. It was found that while the technology was 99.7% accurate for light-skinned men, its accuracy dropped to 65.3% for dark-skinned women.[117] Studies and repots like Buolamwini's, highlight the potential for unjust identification, with far-reaching implications particularly for minority groups.

[116] Buolamwini and Gebru, "Gender Shades."

[117] Buolamwini and Gebru, 9.

However, the examination of demographic impacts in the realm of FRT is often inadequately addressed in scholarly publications and media narratives. More specifically, discussions frequently pivot around accuracy without adequately detailing important metrics such as false negatives, false positives, or the rate of failure to enroll. As a majority of FRT systems are structured with a pre-determined threshold, it is paramount that both false positive and false negative rates for each demographic cohort are duly reported and assessed at that threshold. Therefore, there is an evident need for more comprehensive reporting methodologies that pay ample attention to the potential demographic variances and implications. Such a systematic approach would help in identifying and addressing potential biases, and in turn, contribute to developing more reliable, equitable, and transparent FRT systems.

NIST persistently evaluates commercially obtainable and prototype facial recognition algorithms to gauge their precision across various demographic sectors. Previously, NIST testing uncovered substantial discrepancies in false match rates for women, the elderly, and racial minorities compared to white men. However, more recent findings from NIST reveal a considerable reduction in algorithmic bias related to gender and age.[118] These enhancements are primarily due to improved training datasets and techniques. Specifically, the incorporation of deep convolutional neural networks has resulted in substantial advancements in biometric accuracy and a reduction in bias.[119] NIST's research indicates recent FRT algorithms show negligible or no statistically significant differences across different age and gender groups, with only minor gaps favoring white men.[120] The ongoing development of more sophisticated algorithms and continuous testing with representative datasets are vital to further diminish demographic bias as facial recognition technology progresses.

[118] Grother, Ngan, and Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*.

[119] Lu, Song, and Xu, "Human Face Recognition Based on Convolutional Neural Network and Augmented Dataset."

[120] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 2: Identification*, NISTIR 8271 (Washington, DC: U.S. Department of Commerce, 2023).

While these newer algorithms have taken great strides in approaching demographic parity, law enforcement agencies have been using FRT before this progress—specifically, technology that utilizes older algorithms that have shown demographic bias—raising concerns of disparate impact. Substantiating the abstract outcomes of research with real-life cases can lend a human face to these technical concerns. Robert Williams' wrongful arrest in Detroit serves as a poignant example.[121] Similarly, Nijeer Parks, a black male, was wrongfully arrested in February 2019 due to a false FRT match.[122]

a. The Case of Nijeer Parks

Parks spent 10 days in jail, and in November 2019, prosecutors dismissed their case against Parks due to a lack of evidence.[123] Following the dismissal of his case, Parks sued the city of Woodbridge for false arrest, false imprisonment, and the violation of his civil rights.[124] Based on his lawsuit, police in Woodbridge, New Jersey, wrongfully identified him as an assault suspect using facial recognition technology, leading to his immediate arrest. His resulting lawsuit paints a portrait of the misuse of facial recognition technology leading to an unjust breach of his civil rights. This incident casts light on the urgent and essential lessons surrounding the responsible governance and control of facial recognition technology in law enforcement.

At the outset, Parks' case exposes the potential flaws and errors inherent in facial recognition systems, driving home the pivotal necessity for human oversight and intervention. Police officers relied exclusively on the technological match produced by the system, ignoring Parks' persistent assertions of innocence and overlooking clear physical evidence that could have vindicated him. As alleged in his lawsuit, Parks maintained that he had never visited Woodbridge or even driven a car. In this scenario, had there been

121 Hill, "Wrongfully Accused by an Algorithm."

122 Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times*, December 29, 2020, sec. Technology, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

123 Hill.

124 Nijeer Parks v. John McCormack, L-003672-20 (Passaic, NJ. 2020).

stringent protocols necessitating corroborative evidence, Parks' wrongful arrest and subsequent incarceration could have been avoided entirely.

Second, Parks' unfortunate encounter spotlights the escalating trend of law enforcement leaning excessively on technology, often at the expense of conventional investigative techniques. Following the facial recognition match, the police officers failed to conduct any additional investigation into Parks' steadfast denial of ever being in Woodbridge or driving a car. According to the lawsuit, they intimidated Parks, using scare tactics to discourage him from challenging the identification made by the facial recognition system. This case clearly underscores the urgent need for mandatory training for law enforcement officers on understanding the limitations and potential errors of facial recognition systems to prevent overreliance and misuse.

Finally, the lawsuit filed by Parks raised serious allegations of racial bias at various stages of the process. From his arrest, through the use of excessive force, to his prosecution, the lawsuit pointed towards an anti-Black bias that played a significant role in the actions taken against Parks. These serious allegations amplify concerns about the higher error rates in older FRT algorithms when identifying minorities. To counteract these systemic issues, law enforcement agencies should implement stringent anti-bias standards, thoroughly evaluate underlying FRT algorithms for demographic bias, conduct regular audits to identify potential issues, and establish oversight and accountability procedures to ensure unbiased use of the technology.

The case of Nijeer Parks offers a stark demonstration of the potential for abuse and harm when law enforcement agencies use facial recognition technology without adequate safeguards and regulations. This case serves as a potent reminder for policymakers to learn from such incidents and to craft regulations that set guidelines for unbiased, accurate, and legally sufficient outcomes. Crucially, regulations should also require human oversight of automated decisions. As societies increasingly integrate advanced technologies like facial recognition into everyday life, it is imperative to strike the right balance. We must protect individual rights and freedoms while also achieving public safety objectives, ensuring the responsible and ethical use of such powerful technology.

b. Transparency, Privacy, and Regulation

The examination of FRT by law enforcement also calls into question ethical concerns about transparency, privacy, and the need for regulation. According to research from the Center on Privacy & Technology at Georgetown Law, around half of all adults in the United States, approximately 117 million people, have their images stored in a law enforcement facial recognition database. Alarmingly, the majority of these individuals are not aware of their presence in these databases.[125] This encroachment on individual privacy, often without the explicit consent or even knowledge of the concerned parties, raises serious questions about the ethics and legality of such data collection and storage.

Issues surrounding the transparency of FRT usage are also central to the discussion. In Clare Garvie's study, *The Perpetual Line-Up*, the spotlight was turned on the opaque nature of law enforcement's use of FRT. The study revealed that audits to assess misuse of these systems are infrequent among law enforcement agencies, that regulatory guidelines for the use of FRT are largely lacking, and that these agencies do not consistently take sufficient steps to verify the accuracy of the software.[126] In her follow-up study, *Garbage In, Garbage Out*, Garvie examined the concept of using FRT matches as investigative leads only, thus necessitating independent probable cause before arresting a suspect. However, Garvie found that most of the examined jurisdictions do not provide clear guidance or have specific policies that detail the appropriate level of corroboration or investigation independent of the FRT match necessary before arrest.[127]

The assembled body of evidence illustrates the pressing need for comprehensive regulations around law enforcement's use of FRT. As it stands, the potential for misuse and abuse of the technology is significant. The inherent bias in many facial recognition algorithms can disproportionately subject certain demographic groups to the risk of wrongful identification. Moreover, the pervasive lack of transparency and informed

[125] Garvie, Bedoya, and Frankle, "The Perpetual Line-Up."

[126] Garvie, Bedoya, and Frankle.

[127] Clare Garvie, "Garbage In, Garbage Out," Georgetown Law, Center on Privacy and Technology, May 16, 2019, https://www.flawedfacedata.com/.

guidelines regarding law enforcement's use of FRT can lead to a serious infringement of privacy rights. On examining this body of evidence, it becomes clear that the current status quo is untenable. While facial recognition technology offers significant benefits to law enforcement, ranging from enhanced efficiency to improved capabilities in identifying and tracking down criminals, it is of paramount importance that these advantages are balanced against the need to protect civil liberties, ensure privacy, and uphold principles of fairness. Policymaking in this domain must address the need for transparency, set guidelines for the collection and storage of data, mandate regular audits to check misuse, and instigate measures to correct and minimize algorithmic bias. Failing to do so could have serious consequences, further eroding public trust in law enforcement agencies and contributing to systemic biases within the criminal justice system.

3. Construct the Alternatives

Based on the problem space, available evidence and the literature review, five potential policy solutions should be examined—Comprehensive regulation, an outright ban, a moratorium, a warrant requirement, and maintaining the status quo.

a. Comprehensive Regulation

The first alternative aims to construct a comprehensive legal framework to regulate the law enforcement's use of FRT based on the principles of lawfulness, fairness, accountability, and purpose limitation. Lawfulness would ensure the adoption and use of FRT is consistent with existing laws and civil liberties. This would necessitate the creation of specific legislation that explicitly defines the legal and ethical use of FRT, providing clear boundaries for law enforcement to prevent misuse. This legislation should address not only when and how FRT can be used, but also the manner in which data is collected, stored, and shared, ensuring it aligns with established privacy laws and standards

The fairness principle would impose a requirement for the use of FRT to be nondiscriminatory and equitable. Given the issues of racial and gender bias associated with FRT, the law would need to mandate the use of FRT systems that have been rigorously tested for accuracy and bias across diverse demographic groups. Furthermore, procedures would be implemented to ensure fairness in the application of FRT, including prohibitions

on the use of FRT for discriminatory surveillance or targeting of specific demographic groups.

Accountability refers to ensuring law enforcement agencies are held responsible for the use of FRT. This could be achieved through mandatory transparency reports detailing the use of FRT and regular audits of law enforcement agencies' FRT use. Complaint mechanisms should also be put in place, allowing individuals to challenge the use of FRT in their cases and seek redress for any violations. Moreover, there should be severe penalties for any misuse or violation of the laws and regulations surrounding FRT.

Purpose limitation would ensure that FRT is used only for specific, defined purposes. This principle would help to prevent the misuse of FRT by setting explicit boundaries for its use. For example, FRT might be limited to investigating serious crimes or identifying missing persons, with prohibitions on using the technology for general surveillance or for the tracking of individuals without clear and justified cause.

Implementing this comprehensive regulatory framework would involve collaboration between lawmakers, law enforcement agencies, civil rights organizations, and technology experts to ensure all pertinent issues are addressed. The aim would be to create a robust, effective, and equitable system that allows for the benefits of FRT to be harnessed in a way that respects and protects individual rights and freedoms.

b. Outright Ban

The second alternative, an outright ban on law enforcement using FRT, is rooted in the idea that the risks of misuse and the potential for harm, particularly to marginalized and vulnerable populations, outweigh any potential benefits. This alternative proposes prohibiting all uses of FRT by law enforcement agencies, whether for identification, verification, surveillance, or any other purpose. An outright ban would eliminate the risk of misuse, discriminatory targeting, false positives, and other privacy infringements associated with FRT. The ban approach had gained traction in various jurisdictions

throughout the country; however, some jurisdictions are revisiting the approach and lifting bans.[128]

While an outright ban seems to be the most direct way to prevent privacy violations and discriminatory practices, it would also eliminate the potential benefits of FRT, such as its use in locating missing persons, identifying suspects in serious crimes, or enhancing security measures. Moreover, banning FRT does not necessarily mean that it will not be used in less regulated contexts, such as private security, raising concerns about underground use and the lack of control and accountability in these scenarios. There are also concerns about how an outright ban would affect the development and advancement of FRT and similar technologies in the future.

Therefore, this alternative would require careful consideration and a thorough weighing of potential benefits and risks. It would also demand comprehensive legislation and enforcement mechanisms to ensure that the ban is adhered to by all relevant parties and that there are strict penalties for violations.

c. Moratorium

The third alternative, a moratorium on law enforcement's use of FRT, proposes a temporary halt on the technology's use until a comprehensive set of rules and regulations can be put in place. The premise of this option is to buy time for lawmakers, regulators, technology experts, and stakeholders to understand the full implications of FRT and collaboratively create guidelines for its responsible use. A moratorium would halt the further entrenchment of FRT within law enforcement practices, thereby minimizing the potential harm caused by misidentifications and privacy violations. Meanwhile, it would also allow for continued development and further reduction of algorithmic bias across diverse populations.

By instating a moratorium, regulators would have the opportunity to catch up with the rapid development of FRT. It would give time to develop comprehensive legislation

[128] Paresh Dave, "Focus: U.S. Cities Are Backing off Banning Facial Recognition as Crime Rises," *Reuters*, May 12, 2022, https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/.

that addresses the ethical and legal concerns around FRT, including privacy, consent, data security, and potential bias. However, the duration of a moratorium is critical. If it is too short, it may not allow enough time to address the complex issues at hand. If it is too long, it might unnecessarily delay the benefits of FRT, such as aiding in missing person cases and criminal investigations. Another concern is the enforcement of the moratorium. Given that many law enforcement agencies are already using FRT, enforcing a moratorium could prove challenging, requiring robust mechanisms to monitor adherence and apply penalties in case of violations.

d. Requiring a Warrant

The fourth alternative advocates for the requirement of a warrant before law enforcement can use FRT. This approach would incorporate FRT into the existing legal framework that governs law enforcement's search and seizure practices, thereby providing a balance between public safety interests and individual rights to privacy. The premise of requiring a warrant before using FRT is rooted in the Fourth Amendment to the United States Constitution, which guards against unreasonable searches and seizures. Given that the use of FRT could be considered a form of search, it could be argued that law enforcement should be required to obtain a warrant before its use.

Implementing a warrant requirement could serve as an additional layer of protection against misuse of FRT, as it would necessitate an independent judicial oversight of law enforcement requests. This oversight would require law enforcement to demonstrate probable cause, thus reducing the likelihood of unwarranted or discriminatory use of the technology. However, the application of a warrant requirement to FRT use would be complex due to the technology's distinct features. For instance, the inherently broad and indiscriminate nature of FRT, which often involves scanning large databases to find a match, does not fit neatly within the traditional framework of search and seizure warrants which require specificity.

There would also be the challenge of defining what constitutes probable cause in the context of FRT. This could lead to varying interpretations and inconsistent application of the warrant requirement across jurisdictions, which in turn could result in unequal

protections for individuals. Finally, the warrant requirement might also slow down law enforcement processes and potentially hinder the technology's utility in certain situations where timeliness is a factor and exigency does not apply.

e. Status Quo

The final alternative is to maintain the current status quo of law enforcement's use of FRT, meaning no additional regulations or limitations would be introduced. This approach is based on the belief that the benefits derived from FRT in terms of enhancing public safety and efficiency in investigations wholly outweigh the potential negatives and risks. By continuing the status quo, law enforcement agencies would retain broad discretion in how and when to deploy FRT. This could enable the police to quickly identify suspects, locate missing persons, and solve crimes more efficiently. Additionally, existing oversight mechanisms like internal audits and checks, along with public scrutiny and potential litigation, may be sufficient to discourage abuse and ensure that agencies remain accountable.

However, maintaining the status quo also means that the ethical, privacy, and civil liberties concerns raised by FRT remain unaddressed. As it stands, law enforcement' use of FRT lacks a consistent national regulatory framework, resulting in wide variation in usage policies across jurisdictions.[129] This could lead to inconsistent protections for citizens, with some potentially facing higher levels of surveillance and infringement on their privacy than others. Without additional regulations, the potential for misuse or abuse of the technology persists. Biased algorithms, lack of transparency, and over-reliance on FRT could lead to wrongful arrests, violation of privacy rights, and the erosion of public trust.

Furthermore, the status quo fails to address the potential chilling effect on free speech and assembly, particularly if law enforcement uses FRT to monitor protesters or other public gatherings. The continuation of the current state of affairs also fails to rectify

[129] Kristin Finklea et al., *Federal Law Enforcement Use of Facial Recognition Technology*, CRS Report No. R46586 (Washington, DC: Congressional Research Service, 2020), 15, https://crsreports.congress.gov/product/details?prodcode=R46586.

the current lack of transparency, accountability, and due process surrounding the use of FRT.[130]

f. Conclusion

The discussion around law enforcement's use of FRT is not simply a choice between public safety and privacy, but a complex dialogue that requires considering the nuances of the technology, societal values, and the role of law enforcement in a democratic society. The most optimal pathway will ensure that law enforcement can leverage this tool to maintain safety, while citizens are protected from potential abuses and their rights are upheld. As this debate continues to unfold, it is crucial to keep in mind that the end goal is a society where technology serves the people, respecting and upholding their rights and freedoms, while also enhancing public safety and justice.

4. Select Criteria

Based on the evidence and the literature review, key criteria to evaluate policy alternatives are effectiveness, proportionality, cost, and public trust.

a. Effectiveness

The main objective of any law enforcement tool is to help in the prevention, detection, and resolution of crimes. FRT, as a tool, should demonstrably aid in these tasks. As part of this criterion, it is important to consider both the direct and indirect effects on crime rates. Direct effects would include increased identification and apprehension of suspects, while indirect effects might entail a potential deterrent effect on criminals who know that FRT is being used. It is also essential to weigh the effectiveness of the technology in terms of the type of crime. For instance, FRT may be more effective in preventing and solving certain crimes, such as identity theft or fraud, than others, such as crimes of passion, which are often spontaneous and not premeditated.

Moreover, effectiveness should not be limited to the immediate outcome of solving a crime but should also factor in the long-term benefits of using the technology. This could

[130] Garvie, Bedoya, and Frankle, "The Perpetual Line-Up."

include the deterrence value of FRT and the potential for FRT to help exonerate innocent persons more quickly. However, a key challenge in measuring effectiveness is that it can sometimes be difficult to establish a direct causal link between the use of FRT and a decrease in crime rates. Many other factors, ranging from social and economic conditions to other law enforcement strategies, can also impact crime rates.

The focus should therefore be on creating a robust, scientifically valid framework for evaluating the effectiveness of FRT in law enforcement. This could involve controlled experiments, rigorous data analysis, and independent audits, among other approaches. Ideally, it should be possible to compare the effectiveness of FRT with other law enforcement tools and approaches, to ensure that resources are being allocated in the most efficient and effective manner.

b. Proportionality

Proportionality is another crucial criterion in the evaluation of any policy pertaining to law enforcement's use of FRT. When applied to FRT, it insists that the benefits of using the technology should be balanced against the potential harm or intrusion into individual privacy and civil liberties. Proportionality, in the context of law enforcement's use of FRT, can be viewed from two perspectives—intrusiveness and accuracy.

First, it involves assessing whether the use of FRT is the least intrusive method to achieve the desired goal. In other words, law enforcement agencies should only resort to FRT when less invasive methods are incapable of producing the needed results. They should also ensure that FRT is only used in situations that warrant such intervention, such as in serious crimes or national security matters. Routine or indiscriminate use of FRT, particularly for minor offenses, would be deemed disproportional.

Second, the principle of proportionality also applies to the accuracy of FRT. Given the potential for FRT to infringe on individuals' privacy and liberty, law enforcement agencies have a responsibility to ensure the systems they use are accurate and reliable. Using an FRT system with a high rate of false positives or negatives, particularly across demographic groups, would be deemed disproportional, given the potential harm to individuals misidentified by the system.

c. Cost

The economic feasibility of a policy is key to its potential for successful implementation. The financial implications of a new policy can be multifaceted, including potential costs for additional training, necessary infrastructure upgrades, and the hiring of extra personnel. As such, if a policy necessitates significant expansion in these areas, it may require law enforcement agencies to increase their budgets to accommodate these needs. Conversely, if a policy suggests the discontinuation of FRT use, it may allow for a reallocation of funds that were initially dedicated to supporting this technology. These resources can then be redirected to other operational requirements within the agency.

The financial component of a policy is not solely about expenditure but also involves strategic financial management. Policymakers must consider whether agencies have the financial capacity to support the new demands or if new funding strategies are required. Therefore, the cost is a critical element when assessing the viability of a policy and its potential to bring about the desired change in practice.

d. Public Trust

Public trust is a central criterion for evaluating policy alternatives, particularly those that involve surveillance technologies like FRT. Public trust in law enforcement agencies is crucial for their effective functioning. When this trust erodes, it can hamper crime reporting, cooperation with investigations, and overall public safety. Therefore, any policy regarding law enforcement's use of FRT must consider its impact on public trust.

The use of FRT by law enforcement has triggered concerns over privacy, civil liberties, and potential misuse. Furthermore, false positives leading to wrongful arrests, such as the cases of Robert Williams and Nijeer Parks, exacerbate these concerns and further erode public trust. A policy that fails to address these concerns, or worse, amplifies them, may have long-term detrimental effects on law enforcement's relationship with the communities they serve. On the other hand, a policy that puts stringent checks on the use of FRT, ensures transparency in its deployment, and addresses demographic disparities can help foster public trust.

For instance, a policy that mandates law enforcement agencies to obtain a warrant before using FRT, with clear guidelines about the conditions under which a warrant can be obtained, could reassure the public about their privacy rights. Similarly, a policy that restricts the use of FRT to only serious crimes could strike a balance between public safety needs and civil liberties. Therefore, while evaluating the alternatives, it's essential to assess each one's potential to foster public trust. The perception of the policy's fairness, the degree of transparency it mandates, and its potential for misuse are all factors that would influence this trust.

5. Project the Outcomes

Projecting the potential outcomes for each of the five policy alternatives using the Nijeer Parks wrongful arrest as a base case provides a useful point of reference. It allows us to consider the practical implications of each alternative in a real-world situation. Below are potential outcomes for each policy alternative.

a. Comprehensive Regulation

The implementation of comprehensive regulation for FRT can significantly reshape law enforcement's use of the tool, possibly leading to more reliable and fair outcomes. In the context of the Nijeer Parks case, the existence of a comprehensive regulatory framework might have demanded an increased standard of evidence before law enforcement could proceed with an arrest. For instance, the rules might have required the cross-verification of FRT results with other types of evidence or eyewitness testimonies. This could have led to the early realization that Parks was not the correct suspect, therefore preventing his wrongful arrest.

Furthermore, such comprehensive regulation could mandate transparency and accountability in the use of FRT by law enforcement agencies. As a result, a thorough audit trail would be available for all FRT uses, possibly even revealing biases or errors in specific uses of the technology. This level of scrutiny could compel law enforcement to exercise caution when relying on FRT, leading to fewer instances of misuse and error. Additionally, comprehensive regulation often includes purpose limitation principles. These principles would set strict guidelines on the purposes for which FRT could be used. In the case of

Parks, law enforcement may have been required to justify why FRT was necessary for identifying a suspect, and if it was the least intrusive method available.

b. Outright Ban

In the Parks case, if an outright ban had been in place, the law enforcement officials would not have had access to FRT as a tool for identification. Consequently, Parks' wrongful arrest, primarily based on the faulty FRT match, would have been averted. However, an outright ban would also mean the removal of a tool that, when used properly, can be instrumental in expediting investigations and enhancing public safety. The absence of FRT could potentially delay the identification and apprehension of actual perpetrators, as law enforcement agencies would need to rely solely on traditional investigative methods.

c. Moratorium

In the Parks case, a moratorium in place at the time could have potentially prevented Parks' wrongful arrest. With FRT temporarily unavailable, the police would have had to rely on other investigative methods, possibly leading them away from Parks and towards the actual perpetrator. However, this pause would also mean that law enforcement agencies lose access to a potentially valuable investigative tool, possibly affecting the speed and efficiency of some investigations. The reallocation of resources would be a crucial aspect here as well; resources might need to be directed towards other investigative tools or practices in the interim.

d. Require a Warrant

If a warrant requirement was in place at the time of the Parks incident, officers would have been required to establish probable cause before using FRT. Assuming the standard for obtaining a warrant was effectively enforced, the warrant requirement could have potentially led the police to reconsider the available evidence and investigate further before resorting to FRT. The due diligence required to convince a judge of the necessity of using FRT might have exposed the discrepancy between the FRT result and Parks' alibi, possibly preventing his wrongful arrest. However, this policy would add an additional step in the investigative process, potentially slowing down law enforcement response times,

particularly in urgent, but non exigent, cases. While it is essential to ensure that civil liberties are not compromised, this policy could also impose significant resource demands on the justice system.

e. Status Quo

The Parks case was a result of the status quo; the absence of enhanced oversight, transparency requirements, or procedural safeguards could lead to more instances of wrongful arrests based on false positives from FRT. This would not only potentially violate individual rights but also undermine public trust in law enforcement agencies and the technologies they employ. As public awareness and concern about the use of FRT in law enforcement grows, maintaining the status quo could also engender a significant backlash from civil rights organizations, privacy advocates, and the public at large. This could lead to increased lawsuits and negative media attention. While the status quo may seem to be the path of least resistance, it may ultimately lead to greater costs, both socially and financially.

6. Confront the Trade-Offs

Each policy alternative will have both advantageous strengths and concerning weaknesses. No single policy option will be perfect, and there are inevitably difficult trade-offs involved in selecting the best approach. To evaluate the merits of each policy alternative thoroughly and objectively, policy makers must closely analyze the specific trade-offs between the positive strengths and negative weaknesses of each option. Evaluating the projected outcomes against the selected criteria will illuminate these trade-offs. Table 1 depicts the relative favorability of each alternative based on its projected outcome and its effect on the selected criteria.

Table 1. Relative Favorability Matrix

Outcomes Matrix				
	Effectiveness	Proportionality	Cost	Public Trust
Comprehensive Regulation				
Outright Ban				
Moratorium				
Require a Warrant				
Status Quo				

The table depicts the relative assessment of each alternative against the other alternatives based on their projected outcomes. Green represents most favorable, yellow represents favorable, and red represents least favorable.

7. Decide

Ultimately, this policy analysis emphasizes the decision-making process, necessitating a comprehensive evaluation of the most viable alternatives based on pragmatic considerations, and their potential public acceptance. It also involves planning for the long-term implementation of the chosen policy alternative. From the variety of alternatives presented for FRT in law enforcement, the comprehensive regulation alternative emerges as the most promising pathway, striking a balance between ensuring accountability, fairness, and upholding the effectiveness of law enforcement operations.

The comprehensive regulation alternative hinges on the establishment of a robust regulatory framework built around core principles of lawfulness, fairness, and accountability, coupled with purpose limitations. This would require laws that clarify when and how FRT can be used, standards to guide its deployment, and systems to monitor and enforce compliance. By doing so, this approach aims to mitigate the risks associated with

FRT, such as false positives and discriminatory outcomes, while still leveraging the technology's benefits for law enforcement. However, the feasibility and success of this policy will depend significantly on achieving legitimacy and wide adoption, which, in turn, require engaging with a broad spectrum of stakeholders. The spectrum encompasses law enforcement agencies, civil liberties groups, technology developers, policy makers, and, crucially, the general public. Each stakeholder group contributes essential perspectives that can help shape a balanced, effective, and widely accepted policy.

Law enforcement agencies offer practical insights into the operational benefits and challenges of using FRT, which can help shape practical guidelines. Civil liberties groups and the public provide critical perspectives on the societal implications of FRT, ensuring that the policy respects civil liberties and privacy rights. Technology developers contribute technical expertise, offering insights into what is feasible and how the technology may evolve. Lastly, policy makers bridge these perspectives and shape the legislative framework needed for effective regulation.

However, stakeholder engagement alone is not sufficient. Achieving political support for comprehensive regulation is equally vital, as lawmakers have the power to legitimize and enforce the policy. Advocacy efforts should focus on presenting compelling evidence of the risks and benefits associated with FRT, alongside a clear comparison of the trade-offs of different policy options. This evidence-based approach can help policymakers appreciate the necessity and urgency of regulating law enforcement's use of FRT.

Looking towards the long-term implementation and sustainability of comprehensive regulation, creating robust institutional mechanisms becomes paramount. This could include setting up a dedicated regulatory body to oversee FRT use in law enforcement. This body would be responsible for monitoring adherence to the established regulations, auditing law enforcement agencies' FRT practices, and ensuring transparency and accountability. Moreover, systems for lodging and addressing complaints can provide redress for those that FRT misuse adversely affects. Adequate funding will be crucial to support these institutional structures and mechanisms and would likely require increased budget allocations.

In addition, the long-term success of this policy will rely on a culture of continuous learning and improvement. FRT is a rapidly evolving technology, and the policy landscape must keep pace. The regulatory framework should thus be flexible and adaptable, able to respond to emerging evidence, technological advancements, and societal attitudes. Regular reviews and updates should be built into the policy, ensuring it remains relevant and effective over time.

The decision to pursue comprehensive regulation of FRT in law enforcement is not a one-off solution, but a commitment to ongoing oversight, stakeholder engagement, learning, and adaptability. It is about putting in place structures and processes that ensure the ethical, lawful, and effective use of FRT, and continually refining them to reflect changing realities. This approach, though complex, holds the promise of reconciling the power of FRT with the imperative of protecting civil liberties and maintaining public trust.

C. CONCLUSION

This policy analysis underscores the need for thoughtful, evidence-based approaches to regulating law enforcement applications of facial recognition technology. As illustrated, an outright ban or a maintenance of the status quo represent two extremes, neither adequately balancing public safety imperatives and civil liberties concerns. Meanwhile, a moratorium buys time but delays solutions, while imposing blanket warrant requirements overlooks situational complexities.

Of the options assessed, comprehensive regulation centered on principles of lawfulness, fairness, accountability, and purpose limitation emerges as the most prudent path forward. This approach, if properly governed, can constrain unfettered use while preserving facial recognition's benefits. The projections indicate comprehensive regulation has the highest potential for balancing effectiveness, proportionality, cost-efficiency, and building public trust. Yet comprehensive regulation is not a panacea. Success depends on flexible standards adaptable to evolving technologies and societal norms. Lawmakers must eschew reactionary stances and remain open to new evidence and ethical perspectives. A regulatory system anchored in continuous learning and stakeholder engagement is essential to create policies responsive to emerging realities. Furthermore, the long-term viability of

comprehensive regulation hinges on investment in oversight institutions and accountability mechanisms with appropriate enforcement powers. Coupling strong rules with robust supervision and redress systems can sustain public confidence. But under-resourced or toothless oversight will foster continued skepticism.

In the end, facial recognition's future trajectory will be shaped not solely by the specific regulations enacted, but also by the problem-solving mindsets that guide development of policies, procedures, and governance. If stakeholders can unite around evidence-based analysis, thoughtful trade-off evaluation, and genuine commitment to equitable outcomes, policies will evolve responsibly. But polarization, confirmation bias, and unwillingness to compromise risk flawed, ineffective policies.

Navigating facial recognition's societal impacts requires nuance beyond binary for/against arguments. With advanced technologies like facial recognition permeating daily life, the charge for policymakers is to pursue policies that realize societal benefits while mitigating risks. If done deliberatively, incorporating diverse perspectives, the possibilities are profound. But without care, facial recognition risks becoming an apparatus of injustice. By upholding principles of lawfulness, accountability, and fairness, governments can steer facial recognition toward its highest purpose—serving all people justly.

V. CONCLUSION

A. FINDINGS AND CONCLUSIONS

This research endeavor set out to address the core question of determining the optimal approach to regulating federal law enforcement agencies' use of FRT. The overarching aim was to identify policy solutions that maintain the operational effectiveness of FRT as an investigative tool while also addressing the significant civil liberty concerns associated with its use. Through an extensive review of the academic literature, analysis of regulatory approaches, and systematic policy analysis, this study derived several key findings that are summarized below.

The literature review provided crucial perspectives on the evolution of FRT capabilities, the proliferation of its usage within law enforcement, and the complex ethical debates surrounding its deployment. It revealed that while algorithms and technical accuracy have advanced considerably in recent years, concerns around demographic biases, transparency, consent, and privacy continue to persist. This highlights the urgent need for thoughtful governance frameworks that balance public safety imperatives with protections of civil rights. The review also underscored the lack of clear legal foundations guiding law enforcement's use of FRT, emphasizing the need for regulatory clarity.

By tracing the technological underpinnings of FRT's development, the literature illuminated both its growing identification capabilities as well as limitations that still remain. Comparing FRT algorithms against human facial examiners demonstrated parity in certain contexts, but also persistent gaps in more challenging scenarios. The review also highlighted promising strides made in mitigating demographic biases through improved training data and techniques. However, it also indicated the need for caution against overreliance on technology alone without human oversight.

The technology overview provided critical historical context about early FRT research and key innovations that enhanced its accuracy over time. Analyzing capabilities like one-to-one verification versus one-to-many identification shed light on specific applications of value to law enforcement. However, this overview of expanded FRT

capabilities also brought to focus profound ethical dilemmas around privacy, consent, racial bias, transparency, and accountability. The wrongful arrest of Robert Williams emerged as a seminal case underscoring the potential for misuse and disproportionate impact on marginalized groups in the absence of rigorous governance.

An in-depth comparative analysis of the EU's LED highlighted key principles such as purpose limitations, data minimization, storage restrictions and accountability measures. This provided insights into a privacy-focused regulatory approach. However, the analysis also noted barriers to direct implementation in the U.S. context, indicating the need for adaptations that account for operational realities of law enforcement agencies. Important lessons can be derived about employing principles of lawfulness, transparency, and fairness in the governance of law enforcement FRT use. But the research also emphasized the challenges of fragmentation in adapting broad EU regulations to specialized local contexts.

The final policy analysis section provided a systematic framework for evaluating alternatives ranging from an outright ban to comprehensive legislation. By analyzing projected outcomes against criteria of effectiveness, proportionality, cost, and public trust, it concluded that comprehensive regulation centered on core principles of lawfulness, fairness, transparency, accountability, and purpose limitation offered the most balanced policy pathway. This option constrained unfettered use while preserving public safety benefits of regulated FRT applications. The policy analysis underscored the need for nuanced governance attuned to complex, evolving technologies interacting with complex social realities within law enforcement.

In conclusion, this research dispelled notions of facial recognition as an intrinsic societal ill or panacea, demonstrating how merits and risks depend heavily on governing policies and practices. It highlighted the futility of one-size-fits-all prescriptions, emphasizing tailored legislation aligned to ethical principles as a more prudent path forward. Additionally, it revealed the foundational importance of transparency, accountability and addressing algorithmic bias for securing public trust. However, it also cautioned against demanding perfect accuracy at the expense of incremental benefits from a thoughtfully regulated technology. The findings emphasized constructive policymaking requires centering human dignity and equitable outcomes across diverse stakeholder

perspectives. With proper oversight and constraints, the research concludes, facial recognition technology can strengthen public safety without undermining civil liberties—provided the will to govern it responsibly prevails.

B. RECOMMENDATIONS

This research into policy pathways for regulating law enforcement applications of FRT culminates in proposing actionable recommendations based on the study's findings and conclusions. These recommendations aim to provide guidance to lawmakers, law enforcement agencies and other stakeholders seeking to leverage FRT's capabilities while upholding civil liberties.

The most fundamental recommendation is the enactment of comprehensive legislation at the federal level to govern law enforcement's use of FRT. This law should establish permissible uses of FRT based on principles of lawfulness, fairness, transparency, accountability, and purpose limitations. Explicit transparency standards like disclosures, audits, and civilian oversight should also be mandated. To be effective, the law must be neither overly expansive nor excessively restrictive, but rather tailored to the specific complexities of FRT capabilities and law enforcement realities.

Secondly, independent oversight boards comprising of diverse experts in law enforcement, civil rights advocacy, technology ethics, constitutional law, and computer science should be tasked with actively monitoring compliance with the legislation, auditing for misuse or disparate impacts, and instituting necessary reforms. They would provide vital perspectives to balance law enforcement interests with external considerations. The oversight boards could be granted sanctioning powers subject to judicial review, adding teeth to enforcement. They should also publish annual transparency reports on national compliance. Community participation in oversight boards and policy development processes is vital to instill public confidence. Channels for soliciting feedback and lodging grievances related to FRT should be instituted to make oversight mechanisms responsive and transparent. Building communal understanding of tradeoffs involved can enhance the legitimacy of balanced policies.

Additionally, law enforcement agencies must formally develop and continually update internal policies aligned with the federal legislation and input from oversight boards. These policies should cover areas like ethics training for FRT use, protocols for corroborating system outputs, disciplinary procedures for misuse, and community engagement initiatives. Internal controls with periodic reporting to oversight bodies will reinforce accountability. Agencies should be required to justify each use of FRT based on principles of proportionality and necessity.

Sustained investment should be directed towards refining FRT to minimize demographic biases and false positives through enhancements in training data, benchmarking, and algorithmic techniques. However, pursuing perfect accuracy should not take precedence over implementing thoughtfully regulated systems with oversight. The focus should be on concrete improvements that lead to more equitable and lawful outcomes.

In summary, comprehensive federal legislation in conjunction with robust tripartite oversight between lawmakers, communities and technologists offers the most prudent way forward. Realistic policies recognizing that initial governance models are unlikely to be perfect, but can evolve responsibly through sustained commitments to lawfulness, ethics and accountability will be key. With rigorous safeguards and evidence-based iterative improvements in oversight and technology, facial recognition technology can potentially strengthen public safety while protecting civil liberties. But achieving this goal requires shared dedication across stakeholders to transparency, purpose-driven design and equitable outcomes that respect diverse perspectives. Federal law enforcement agencies can navigate the risks and rewards of facial recognition responsibly through adaptable policies centered on justice, oversight, and democratic values.

C. FUTURE RESEARCH

While this research focused on examining policy pathways for governing federal law enforcement uses of FRT, the findings and recommendations point to several fruitful areas for future scholarly inquiry that could further inform the ethical and responsible development of FRT.

Assessing the long-term impacts of comprehensive FRT regulation on factors like crime rates, public perceptions, and infringement of civil liberties. Longitudinal studies could provide insights into the effectiveness and unintended consequences of regulatory approaches. Surveying law enforcement agencies to gauge preparedness and perspectives on potential new oversight requirements, transparency standards and internal policy changes mandated by FRT regulation. Evaluating the resource requirements, infrastructure needs, and composition models for effective independent oversight boards that balance law enforcement interests and external considerations. Developing standardized benchmarking metrics and test datasets to continually improve training and evaluation of FRT systems for minimizing algorithmic bias and enhancing demographic equity. Exploring community engagement initiatives surrounding FRT oversight boards to identify strategies for public education, facilitating input, and fostering transparency. Comparative analysis of regulatory approaches for FRT in other democratic countries to identify best practices and lessons for adaptation.

In summary, this initial research establishes a strong foundation and policy direction, but deeper inquiry into implementation mechanisms, validating impacts, and stakeholder perspectives can catalyze more robust, evidence-based governance of law enforcement uses of FRT. Furthermore, constant engagement with evolving legal frameworks, privacy norms and technological capabilities will remain essential for just, ethical, and socially responsible proliferation of this powerful technology.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Administrative Code – Acquisition of Surveillance Technology, 190110, S.F. Board of Supervisors § (2019). https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019.

Anthony, Samuel E., Maryam Vaziri Pashkam, and Ken Nakayama. "Comparing Computer and Human Performance on Identical Face Detection Tasks." *Journal of Vision* 12, no. 9 (August 13, 2012): 499. https://doi.org/10.1167/12.9.499.

Ballantyne, M., R.S. Boyer, and L. Hines. "Woody Bledsoe: His Life and Legacy." *AI Magazine*, 1996.

Bardach, Eugene, and Eric Patashnik. *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving.* 6th ed. Thousand Oaks, CA: CQ Press, 2020.

Benedict, T. J. "The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest." *Washington and Lee Law Review* 79, no. 2 (Spring 2022): 849–98. https://www.proquest.com/docview/2681520570/abstract/36373B0F5BA44746PQ/1.

Borchetta, Jenn Rolnick, and Brandon Chapman. "State and Local Governments Must Take Responsibility for Police Violence." ACLU, June 22, 2023. https://www.aclu.org/news/criminal-law-reform/state-and-local-governments-must-take-responsibility-for-police-violence.

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research* 81 (2018): 1–15.

Carpenter v. U.S., 138 S. Ct. 2206 (Supreme Court 2018).

Carter, Anthony M. "Facing Reality: The Benefits and Challenges of Facial Recognition for the NYPD." Master's thesis, Monterey, CA; Naval Postgraduate School, 2018. https://calhoun.nps.edu/handle/10945/60374.

Crumpler, William, and James Lewis. "How Does Facial Recognition Work? A Primer." Center for Strategic and International Studies (CSIS), 2021. https://www.csis.org/analysis/how-does-facial-recognition-work.

Dave, Paresh. "Focus: U.S. Cities Are Backing off Banning Facial Recognition as Crime Rises." *Reuters*, May 12, 2022. https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/.

Davies, A. Spencer. "A Californian Algorithm: Amending Assembly Bill 2261 to Regulate Law Enforcement's Use of Facial Recognition Technology in Post Hoc Criminal Investigations." *Berkeley Jounal of Criminal Law* 26, no. 2 (2021): 27–70. https://doi.org/10.15779/Z38SB3X03N.

Deng, Jia, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. "ImageNet: A Large-Scale Hierarchical Image Database." In *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 248–55, 2009. https://doi.org/10.1109/CVPR.2009.5206848.

Department of Homeland Security. *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*. DHS Directive 262–16. Washington, DC: Department of Homeland Security, 2022.

———. *Privacy Impact Assessment for the ICE Use of Facial Recognition Services*. Washington, DC: DHS, 2020. https://www.dhs.gov/publication/dhsicepia-054-ice-use-facial-recognition-services.

Directive (EU) 2016/680 Law Enforcement Directive, OJ L 119 § (2016). http://data.europa.eu/eli/dir/2016/680/oj/eng.

E-Government Act of 2002, Pub. L. No. 107–347, § 208 (2002).

European Data Protection Board. *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*. Brussels: EDPD, 2023. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

European Union Agency for Fundamental Rights. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018.

Exec. Order No. 13960, 85 FR § (2020). https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

Federal Privacy Council. "Fair Information Practice Principles (FIPPs)." Federal Privacy Council. Accessed July 29, 2023. https://www.fpc.gov/resources/fipps/.

Finklea, Kristin, Laurie Harris, Abigail Kolker, and John Sargent Jr. *Federal Law Enforcement Use of Facial Recognition Technology*. CRS Report No. R46586. Washington, DC: Congressional Research Service, 2020. https://crsreports.congress.gov/product/details?prodcode=R46586.

"FISWG," n.d. https://www.fiswg.org/index.html.

Garvie, Clare. "Garbage In, Garbage Out." Georgetown Law, Center on Privacy and Technology, May 16, 2019. https://www.flawedfacedata.com/.

Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." Georgetown Law, Center on Privacy and Technology, October 18, 2016. https://www.perpetuallineup.org/.

Goodwin, Gretta L. *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*. GAO-21-518. Washington, DC: Government Accountability Office, 2021.

Gray, David. "Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies." *SMU Science and Technology Law Review* 24 (Summer 2021): 3–63. Nexis Uni.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. *Face Recognition Vendor Test (FRVT) Part 2: Identification*. NISTIR 8271. Washington, DC: U.S. Department of Commerce, 2023.

———. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NISTIR 8280. Washington, DC: U.S. Department of Commerce, 2019.

GSA. *Introduction to the AI Guide for Government*. Washington, DC, 2022. https://coe.gsa.gov/coe/ai-guide-for-government/introduction/index.html.

Hill, Kashmir. "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match." *The New York Times*, December 29, 2020, sec. Technology. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

———. "Wrongfully Accused by an Algorithm." *The New York Times*, June 24, 2020, sec. Technology. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Hirose, Mariko. "Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology." *Connecticut Law Review* 49 (2017 2016): 1591. https://heinonline.org/HOL/Page?handle=hein.journals/conlr49&id=1635&div=&collection=.

H.R. *Law Enforcement's Use of Facial Recognition Technology: Hearing before the Committee on Oversight and Government Reform, House of Representatives*, House of Representatives, 115th Cong. 1 (2017), n.d. https://www.govinfo.gov/content/pkg/CHRG-115hhrg28689/pdf/CHRG-115hhrg28689.pdf.

Hupont, Isabelle, Songül Tolan, Hatice Gunes, and Emilia Gómez. "The Landscape of Facial Processing Applications in the Context of the European AI Act and the Development of Trustworthy Systems." *Scientific Reports (Nature Publisher Group)* 12, no. 1 (2022). https://doi.org/10.1038/s41598-022-14981-6.

Information Commissioner's Office. "Guide to Law Enforcement Processing." Information Commissioners Office. Accessed April 12, 2023. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/.

International Organization for Standardization. *ISO/IEC 2382–37 Information Technology – Vocabulary – Part 37: Biometrics*. Geneva: International Organization for Standardization, 2022.

Judicial Administration, 28 C.F.R. 20 § (1999). https://www.ecfr.gov/current/title-28/chapter-I/part-20.

Lee-Morrison, Lila. *Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face*. Bielefeld University Press, 2019. https://doi.org/10.14361/9783839448465.

Lin, Jianhong, Chaoyang Ye, Weinan Liu, Siqi Ren, this link will open in a new window Link to external site, Ye Wang, Wenrui Ma, Bin Xu, and Yifan Ding. "A Lightweight Face Verification Based on Adaptive Cascade Network and Triplet Loss Function." Edited by Liqin Shi. *Wireless Communications & Mobile Computing (Online)* 2022 (2022). https://doi.org/10.1155/2022/3017149.

Lochner, Sabrina. "Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans." *Arizona Law Review* 55 (Spring 2013): 201–33. Nexis Uni.

Lord, Paige. "The Cost of Possibility: U.S. Law Enforcement Use of Facial Recognition Technology and Violations of Civil Liberties." Master's thesis, Harvard University, 2022. https://dash.harvard.edu/handle/1/37371406.

Lovallo, Caroline. "Big Brother's Fall Brings Liberty to All: Addressing the Urgency for Strict Regulation Governing Law Enforcement Use of Facial Recognition Technology in Texas." *Thurgood Marshall Law Review* 46, no. 1 (2021).

Lu, Chaochao, and Xiaoou Tang. "Surpassing Human-Level Face Verification Performance on LFW with GaussianFace." arXiv, December 19, 2014. https://doi.org/10.48550/arXiv.1404.3840.

Lu, Peng, Baoye Song, and Lin Xu. "Human Face Recognition Based on Convolutional Neural Network and Augmented Dataset." *Systems Science & Control Engineering* 9, no. sup2 (May 3, 2021): 29–37. https://doi.org/10.1080/21642583.2020.1836526.

Madiega, Tambiama, and Hendrik Mildebrath. *Regulating Facial Recognition in the EU*. EPRS Report PE 698.021. Brussels: European Parliamentary Research Service, 2021.

Marquenie, Thomas, and Plixavra Vogiatzoglou. *Assessment of the Implementation of the Law Enforcement Directive*. Luxembourg: Publications Office of the European Union, 2022. https://data.europa.eu/doi/10.2861/691965.

Maurer, Diana. *Face Recognition Technology: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy*. GAO-17-489T. Washington, DC: Government Accountability Office, 2017.

National Institute of Justice. *History of NIJ Support for Face Recognition Technology*. Washington, DC: U.S. Department of Justice, 2020. https://nij.ojp.gov/topics/articles/history-nij-support-face-recognition-technology.

Nijeer Parks v. John McCormack, L-003672-20 (Passaic, NJ. 2020) (n.d.).

Office of Juvenile Justice and Delinquency Prevention. "National Center for Missing & Exploited Children." Office of Juvenile Justice and Delinquency Prevention, n.d. https://ojjdp.ojp.gov/programs/national-center-missing-and-exploited-children.

"Office of Privacy and Civil Liberties | Privacy Act of 1974," June 16, 2014. https://www.justice.gov/opcl/privacy-act-1974.

O'Toole, Alice J., P. Jonathon Phillips, Fang Jiang, Janet Ayyad, Nils Penard, and Herve Abdi. "Face Recognition Algorithms Surpass Humans Matching Faces Over Changes in Illumination." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29, no. 9 (September 2007): 1642–46. https://doi.org/10.1109/TPAMI.2007.1107.

Park, Ann. *Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses*. Washington, DC: Office of Science and Technology Policy, 2022. https://www.ai.gov/rfi/2022/86-FR-56300/NCMEC-Biometric-RFI-2022.pdf.

Patel v. Facebook, Inc., 932 F. 3d 1264 (Court of Appeals, 9th Circuit 2019).

Perols, Johan L., Robert M. Bowen, Carsten Zimmermann, and Basamba Samba. "Finding Needles in a Haystack: Using Data Analytics to Improve Fraud Prediction." *The Accounting Review* 92, no. 2 (2017): 221–45. http://www.jstor.org/stable/26550651.

Phillips, P. Jonathon, and Alice J. O'Toole. "Comparison of Human and Computer Performance across Face Recognition Experiments." *Image and Vision Computing* 32, no. 1 (January 1, 2014): 74–85. https://doi.org/10.1016/j.imavis.2013.12.002.

Phillips, P. Jonathon, Amy N. Yates, Ying Hu, Carina A. Hahn, Eilidh Noyes, Kelsey Jackson, Jacqueline G. Cavazos et al. "Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms." *Proceedings of the National Academy of Sciences* 115, no. 24 (June 12, 2018): 6171–76. https://doi.org/10.1073/pnas.1721355115.

Phillips, P.J., Patrick J. Rauss, and Sandor Z. Der. *FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results*. Report Number ARL-TR-995. Arlington, VA: DARPA, 1996. https://apps.dtic.mil/sti/citations/ADA315841.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119 § (2016).

Ringrose, Katelyn. "Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns." *Virginia Law Review Online* 105 (2019): 57–66.

Sawant, Manisha M., and Kishor M. Bhurchandi. "Age Invariant Face Recognition: A Survey on Facial Aging Databases, Techniques and Effect of Aging." *The Artificial Intelligence Review* 52, no. 2 (August 2019): 981–1008. https://doi.org/10.1007/s10462-018-9661-z.

Schuetz, Peter N.K. "Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework." *Law and Inequality* 39 (Winter 2021): 221–54. Nexis Uni.

Shackelford, Scott J., and Rachel Dockery. "Governing AI." *Cornell Journal of Law and Public Policy* 30 (Winter 2020): 279–333. Nexis Uni.

Stevens, Nikki, and Os Keyes. "Seeing Infrastructure: Race, Facial Recognition and the Politics of Data." *Cultural Studies* 35, no. 4/5 (July 2021): 833–53. https://doi.org/10.1080/09502386.2021.1895252.

Turk, M.A., and A.P. Pentland. "Face Recognition Using Eigenfaces." In *1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Proceedings*, 586–91, 1991. https://doi.org/10.1109/CVPR.1991.139758.

United States v. Jones, 565 U.S. 400 (2012).

Valentino-DeVries, Jennifer. "How the Police Use Facial Recognition, and Where It Falls Short." *New York Times*, January 12, 2020, sec. Technology. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103–322, § 210402 (1994).

Woodward, John D., Christopher Horn, Julius Gatune, and Aryn Thomas. "Biometrics: A Look at Facial Recognition." RAND Corporation, January 1, 2003. https://www.rand.org/pubs/documented_briefings/DB396.html.

Yeung, Douglas, Rebecca Balebako, Carlos Ignacio Gutierrez Gaviria, and Michael Chaykowsky. *Face Recognition Technologies: Designing Systems That Protect Privacy and Prevent Bias*. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR4226.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California