2022-12

THE ETHICAL USE OF FACIAL RECOGNITION TECHNOLOGY: A CASE STUDY OF U.S. CUSTOMS AND BORDER PROTECTION

Best, Jeni M.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE ETHICAL USE OF FACIAL RECOGNITION TECHNOLOGY: A CASE STUDY OF U.S. CUSTOMS AND BORDER PROTECTION

by

Jeni M. Best

December 2022

Co-Advisors: Nadav Morag (contractor)
Kathryn J. Aten

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
THE ETHICAL USE OF FACIAL RECOGNITION TECHNOLOGY:
A CASE STUDY OF U.S. CUSTOMS AND BORDER PROTECTION

5. FUNDING NUMBERS

6. AUTHOR(S) Jeni M. Best

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)

After the events of 9/11, facial recognition technology (FRT) emerged as a security solution for identifying and verifying individuals in a homeland security setting. Although FRT demonstrates security benefits, the public has not widely accepted the government's use of the technology. FRT critics raise ethical and societal concerns regarding the negative impact of the technology on the public, including privacy concerns, constitutional rights violations, biased and inaccurate technology, and data management. How can FRT be implemented in a way that is both efficient and ethical? This thesis analyzes FRT through a three-pronged approach. First, the thesis applies the "How to Do It Right" ethical framework to a government agency's decision-making process. The second step identifies ethical operating principles through a crosswalk of the varied and often inconsistent operating principles published by the security industry, government audit agencies, and watchdog groups. Finally, the thesis utilizes a real-world case study to explore an operational FRT program and illustrate best practices. It recommends that following an ethical framework during decision-making and incorporating ethical principles and best practices into FRT programs during development and implementation mitigates the public's ethical and societal concerns.

14. SUBJECT TERMS biometrics, ethics, customs and border protection, facial recognition technology, FRT, biometric entry, biometric exit	**15. NUMBER OF PAGES** 105
	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.

THE ETHICAL USE OF FACIAL RECOGNITION TECHNOLOGY: A CASE STUDY OF U.S. CUSTOMS AND BORDER PROTECTION

Jeni M. Best
Supervisory CBP Officer, U.S. Customs and Border Protection, Department of Homeland Security
BSCJ, Sam Houston State University, 1997
MCJ, Boston University, 2006

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 2022**

Approved by: Nadav Morag
Co-Advisor

Kathryn J. Aten
Co-Advisor

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

After the events of 9/11, facial recognition technology (FRT) emerged as a security solution for identifying and verifying individuals in a homeland security setting. Although FRT demonstrates security benefits, the public has not widely accepted the government's use of the technology. FRT critics raise ethical and societal concerns regarding the negative impact of the technology on the public, including privacy concerns, constitutional rights violations, biased and inaccurate technology, and data management. How can FRT be implemented in a way that is both efficient and ethical? This thesis analyzes FRT through a three-pronged approach. First, the thesis applies the "How to Do It Right" ethical framework to a government agency's decision-making process. The second step identifies ethical operating principles through a crosswalk of the varied and often inconsistent operating principles published by the security industry, government audit agencies, and watchdog groups. Finally, the thesis utilizes a real-world case study to explore an operational FRT program and illustrate best practices. It recommends that following an ethical framework during decision-making and incorporating ethical principles and best practices into FRT programs during development and implementation mitigates the public's ethical and societal concerns.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

1:1	One-to-one matching
1:N	One-to-many matching
ACLU	American Civil Liberties Union
ATL	Atlanta Hartsfield International Airport
BEE	Biometric Entry-Exit Program
CBP	U.S. Customs and Border Protection
CPO	Chief Privacy Officer
CSIS	Center for Strategic International Studies
DHS	Department of Homeland Security
DPIAC	Data Privacy Integrity Advisory Committee
EFF	Electronic Frontier Foundation
ELSI	Ethical, Legal and Societal Issues
EPIC	Electronic Privacy Information Center
FIPP	Fair Information Practice Principle
FPF	Future of Privacy Forum
FRT	facial recognition technology
GAO	U.S. Government Accountability Office
GDPR	General Data Protection Regulation
HSE	Homeland Security Enterprise
IBIA	International Biometrics + Identity Association
LPR	license plate reader
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PII	personally identifiable information
SIA	Security Industry Association
S&T	DHS Science and Technology Directorate
TSA	Transportation Security Administration
TVS	Traveler Verification Service

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The tragic events of 9/11 fundamentally changed how the United States approached personal and homeland security. American citizens questioned how terrorists could operate undetected for so long in the United States and how such events could happen on U.S. soil. In congressional testimony after 9/11, Dianne Feinstein responded to those questions with, "we could not identify them. We did not know they were here. Only if we can identify terrorists planning attacks on the United States do we have a chance of stopping them."[1] In response to the attacks, the United States and the Homeland Security Enterprise (HSE) began to seek, identify, and close gaps in existing security practices that criminals and terrorists could exploit. Feinstein and others believed biometrics could have prevented 9/11. The idea that the nation failed to identify terrorists was the impetus for the widespread development and implementation of biometric systems. The security gap allowed facial recognition technology (FRT) to emerge as a security solution for identifying and verifying individuals.

Although FRT materialized as a common and efficient security measure in the private sector over the last decade, the public has not widely adopted or accepted the government's use of the technology. As with any new technology, the public, advocacy groups, and government oversight entities are skeptical and raise concerns about FRT's purpose and intent, how accuracy impacts the public, and how the technology impinges on privacy and other civil rights. When emerging technology raises privacy and other public concerns, government decision-makers can explore ethical, societal, and legal issues (ELSI) during decision-making to identify common ground with the public to resolve and mitigate the public's concerns.[2] When regulations do not exist to guide the development

[1] *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism*, Senate, 117th Cong., 1st sess., November 14, 2001, https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/html/CHRG-107shrg81678.htm.

[2] Jean-Lou Chameau, William F. Ballhaus, and Herbert S. Lin, eds., *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal and Societal Issues*. (Washington, DC: National Academies Press, 2014), 1, https://pubmed.ncbi.nlm.nih.gov/25032403/.

of new technology, policy and decision-makers can weigh emerging technology's benefits against the public's interest to determine the best path forward for all parties.

A methodology to think about and evaluate ethical dilemmas benefits HSE officials in making difficult choices that impact society.[3] Ethical frameworks provide a set of standards for behavior that decision-makers can use to decide how to act in a range of situations, how to make decisions, and the reasons behind decisions.[4] When decision-makers anticipate and identify problems before implementing novel technology, they can mitigate them, improving public perception and adoption. This research aims to analyze facial biometrics and their relationship with public interest through an ethical framework and a real-world case study to determine how FRT can be implemented in a way that is both efficient and ethical.

This research takes a multi-pronged approach to analyze FRT and outline steps for responsible usage. First, this study explores the decision-making process using the "How to Do it Right" framework. Through the framework, the thesis identifies values and the corresponding vulnerabilities, risks, and mitigation measures. Next, the research reviews academic and security industry literature to identify cross-cutting operational principles that can be applied to FRT programs. Finally, this study explores best practices through a case study of U.S. Customs and Border Protection's (CBP) Biometric Entry-Exit (BEE) program. The goal is to equip homeland security leaders with a framework to identify issues associated with FRT and align the decision-making process with adjudicating and mitigating ethical and societal concerns to produce a beneficial solution for society.

Mohamed Abomhara et al. developed the "How to Do It Right" framework to analyze biometric technology in border settings. The "How to Do It Right" framework is a four-tiered process. The top tier includes ethical, social, and legal challenges. It is followed by the values affected (by the technology) tier, an assessment tier, and considerations at

[3] Aaron Nelson, "Ethical Decision Making for Homeland Security" (master's thesis, Naval Postgraduate School, 2013), https://calhoun.nps.edu/handle/10945/37684.

[4] Sheila Bonde and Paul Firenze, "A Framework for Making Ethical Decisions" (Lecture, Making Choices: Ethical Decisions at the Frontier of Global Science, Brown University, May 2013), https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions.

the bottom level.[5] However, this thesis excludes legal issues from the analysis. The framework links the challenges to the value(s) affected by technology and allows an impact assessment to mitigate the values affected.[6] This analysis adapts the "How to Do It Right" framework and applies it to the U.S. government's use of FRT. It takes the basic framework and incorporates four overarching categories into the challenge tier. The four categories are derived from the literature and criticisms of FRT. The challenges include privacy implications, constitutional protections, data management, and bias and accuracy. Once decision-makers identify issues falling within the four value categories, they can assess the risks, vulnerabilities, and mitigation measures.

Decision-makers promote ethical and efficient programs when developing and implementing safeguards and mitigation measures that correspond to ethical operating principles; these principles are presented in the considerations or final tier of the framework. The operational principles in the final tier originate as ethical guidelines in the biometrics and security industry literature. The adapted framework allows decision-makers to consider the broad implications of FRT and then extrapolate best practices that can mitigate the challenges and establish responsible biometric collection and usage. Government decision-makers can formulate decisions regarding FRT by thinking through the ethical framework before, during, and after technology implementation.

[5] Mohamed Abomhara et al., "How to Do It Right: A Framework for Biometrics Supported Border Control," in *E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age*, ed. Sokratis Katsikas and Vasilios Zorkadis (Cham, Switzerland: Springer, 2019), 6.

[6] Abomhara et al., 99.

Security industry organizations and watchdog groups have developed ethical principles, referred to as operational guidelines, to govern the use of facial biometrics.[7] Each organization has proposed guidelines with many common elements, but no accepted standardized principles exist. A crosswalk of the different principles reveals common patterns that evolve into standardized and best practices for government agencies using FRT. Once a common principle is established as an operating guideline, it can be characterized as an ethical operational practice. The "How to Do It Right" framework incorporates these common themes as mitigation measures. The common themes extracted from the crosswalk are privacy by design, transparency, clear and defined purpose, accurate technology, data security, training and access, and accountability. It is up to each agency to do its due diligence and implement as many ethical principles as possible to balance the security benefits and the public impact. Applying these principles and operating guidelines leads to the responsible use of FRT.

The final prong of this research is a case study on CBP's BEE. CBP's BEE represents an efficient and ethical FRT program. CBP's BEE was selected as a case study because the program includes FRT in a border security environment and incorporates ethical operating principles. Although the agency continually improves and enhances the program, it exemplifies an agency that thoughtfully implemented a program through testing, pivoting approaches, internalizing audit recommendations, and due diligence. The program incorporates ethical principles and enhances security. The CBP case study

[7] As seen in the following literature: Security Industry Association, *Sia Principles for the Responsible and Effective Use of Facial Recognition Technology* (Silver Springs, MD: Security Industry Association, 2020), https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/; International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles* (Washington, DC: International Biometrics and Identification Society, 2021), https://www.ibia.org/resources/white-papers; Future of Privacy Forum, *Summary of Privacy Principles* (Washington, DC: Future Privacy Forum, 2018), https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf; James Andrew Lewis and William Crumpler, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape* (Washington, DC: Center for Strategic and International Studies, 2021), https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape; and, World Economic Forum, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations* (Geneva, Switzerland: World Economic Forum, 2021), https://www.weforum.org/whitepapers/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations.

demonstrates how the government can deploy an FRT program that embodies safety and security while considering and addressing public perception.

By implementing safeguards and countermeasures, government agencies can balance the benefits of FRT with public concern. Overall, when government decision-makers adhere to ethical decision-making frameworks and operating principles, FRT can be used responsibly and efficiently. This thesis makes four recommendations for government agencies considering or using FRT programs. These recommendations apply to decision-makers at all process phases, including technology consideration, development, implementation, and post-implementation assessments or enhancements of FRT. The four recommendations include: following the "How to Do It Right" framework; incorporating ethical operating principles; applying sustainable policy and federal regulations; and exploring and implementing FRT best practices. The four recommendations promote the ethical and efficient use of FRT.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

As I entered this program, I had no idea what to expect. It had been over fifteen years since I attended academic classes, but my cohort and the CHDS staff made the transition back to school easy. This part is difficult because there are so many people I would like to thank and acknowledge. First and foremost, I would like to thank my amazing husband, Jeff, for putting up with me during my academic endeavors. His patience, encouragement, and outright support for everything I do helped me complete this program. I could not have done it without him. I also want to thank my mom and dad for instilling an unwavering work ethic that helped get me where I am today. They have been my biggest cheerleaders.

I would be remiss if I did not acknowledge and thank my coworkers (you know who you are) and bosses who put up with my absence from the office each quarter, picked up the slack, and allowed me to bounce ideas off them. I need to send a special shout-out to Larry Panetta and Roberto Vaquero for writing my recommendation letters, listening to me complain, and always keeping it real with me.

Finally, I would like to thank 2103 for being the best cohort, 2104 for being a very close second, and all our instructors. I enjoyed spending 18 months with each and every one of you. You taught me so much and made me question the status quo. I had some of the best conversations after hours or in the hallways on breaks. I appreciated this the most about our cohort and the program in general. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The tragic events of 9/11 fundamentally changed how the United States approached personal and homeland security. American citizens questioned how terrorists could operate undetected for so long in the United States and how such events could happen on U.S. soil. In congressional testimony after 9/11, Dianne Feinstein responded to those questions with, "we could not identify them. We did not know they were here. Only if we can identify terrorists planning attacks on the United States do we have a chance of stopping them."[1] In response to the attacks, the United States, and the Homeland Security Enterprise (HSE) began to seek, identify, and close gaps in existing security practices that criminals and terrorists could exploit. Feinstein and others believed biometrics could have prevented 9/11 even though biometrics, especially facial recognition, was not commonly used in the private and public sectors at that time, nor was the technology advanced enough.[2] Although some attributed Feinstein's beliefs to *technostalgia* or "the desire to revise the past to redetermine the present by harnessing technology," the idea that the nation failed to identify terrorists was the impetus for the widespread development and implementation of biometric systems.[3] The security gap allowed facial recognition technology (FRT) to emerge as a security solution for identifying and verifying individuals.

A. PROBLEM STATEMENT

Although FRT materialized as a common and efficient security measure in the private sector over the last decade, the public has not widely adopted or accepted the government's use of the technology. The U.S. government's use of FRT continues to be a

[1] *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism*, Senate, 117th Cong., 1st sess., November 14, 2001, https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/html/CHRG-107shrg81678.htm.

[2] Kelly Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: New York University Press, 2016), 2, https://doi.org/10.18574/nyu/9780814732090.001.0001.

[3] Technostalgia is defined as "the desire to revise the past to redetermine the present by harnessing technology toward human ends, all the while recognizing the impossibility of the endeavor," as seen in Kelly Gates, *Our Biometric Future*; and, Pat Gill, "Technostalgia: Making the Future Past Perfect," *Camera Obscura: Feminism, Culture, and Media Studies* 14, no. 1–2 (May 1, 1997): 161–79, https://doi.org/10.1215/02705346-14-1-2_40-41-161.

controversial topic and has gained the attention of the public, civil rights advocates, and policymakers. The technology has garnered negative press, accusations of misuse and inaccuracy, and calls for outright usage bans. Headlines calling out the dangers and challenges of FRT—"Another Arrest and Jail Time Due to a Bad Facial Match," "Detroit Police Face Suit Over Facial Recognition Software," and "Amazon's Facial Recognition Technology Falsely Match 28 Members of Congress with Mugshots"—are prevalent in the media and shape the public's perception of the government's use of FRT.[4] Despite the negative press, criticisms, and allegations of misuse, FRT has presented many benefits to society, from criminal identification to medical advancements.

Although typically prefaced with terms like "controversial," the media recognizes FRT as beneficial in many circumstances. For example, in 2019, FRT led the New York Police Department to an alleged rapist within 24 hours and identified a potential subway bomber.[5] FRT is not only used for criminal identification but also victim identification. Security agencies and public organizations also recognize the benefits of FRT. Between 2015 and 2020, a non-profit organization used facial recognition software in 40,000 trafficking and exploitation cases in North America, identifying 17,000 human traffickers and rescuing 15,000 children.[6] Popular artist Taylor Swift has used FRT to identify stalkers at her events.[7] U.S. Customs and Border Protection (CBP) has used FRT to identify over

[4] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020, sec. Technology, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Drew Harwell, "Detroit Police Face Suit over Facial Recognition Software," *Washington Post*, April 14, 2021, https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots," *ACLU NorCal* (blog), July 26, 2018, https://www.aclunc.org/blog/amazon-s-face-recognition-falsely-matched-28-members-congress-mugshots.

[5] Craig McCarthy, "Facial Recognition Leads Cops to Alleged Rapist in Under 24 Hours," *New York Post*, August 5, 2019, https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/.

[6] Jake Parker, "Facial Recognition Success Stories Showcase Positive Use Cases of the Technology," Security Industry Association, July 16, 2020, https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/.

[7] Samuel D. Hodge Jr., "The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector Technology in the Business Sector," *DePaul Law Review* 71, no. 3 (2022): 731, https://via.library.depaul.edu/law-review/vol71/iss3/2.

1600 imposters attempting to enter the United States.[8] Despite the public criticism of FRT, these use cases demonstrate beneficial outcomes and tangible security and safety benefits.

As with any new technology, the public, private sector, privacy advocates, and government oversight entities are often skeptical and raise concerns about topics such as FRT usage, how the accuracy may impact the public, and how the technology may impinge on privacy and security. When emerging technology raises privacy and other public concerns, government decision-makers can explore ethical, societal, and legal issues (ELSI) to identify common ground with the public to resolve the concerns.[9] At times, the concerns prompted by these ELSI are new and prompted by the technology, but at other times they are familiar challenges. When the ELSI are familiar challenges, they must be reexamined in the light of the new technology.[10] Researchers and critics acknowledge that biometric technology raises ELSI challenges for the HSE.[11] In the ELSI context, ethical issues and criticisms refer to concerns that are a matter of principle (what is regarded as right), and societal issues and criticisms refer to concerns that are a matter of interest to society (what is viewed as desirable).[12] In relation to FRT, societal and ethical concerns to be considered by decision-makers are derived from the literature and classified into four broad categories: privacy implications, constitutional protections, bias and accuracy, and data management and accountability.

Privacy is the first category of criticism and concern. Privacy implications are entrenched in the use of facial recognition. Facial images are ubiquitous. Individuals can avoid iris and fingerprint collection, but it is more difficult to hide one's face. Facial images can be captured covertly, without an individual's knowledge or consent, and from afar.

---

[8] "CBP Biometrics," CBP Biometrics, accessed December 27, 2021, https://biometrics.cbp.gov.

[9] Jean-Lou Chameau, William F. Ballhaus, and Herbert S. Lin, eds., *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal and Societal Issues*. (Washington, DC: National Academies Press, 2014), 1, https://pubmed.ncbi.nlm.nih.gov/25032403/.

[10] Chameau, Ballhaus, and Lin, 245.

[11] Mohamed Abomhara et al., "How to Do It Right: A Framework for Biometrics Supported Border Control," in *E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age*, ed. Sokratis Katsikas and Vasilios Zorkadis (Cham, Switzerland: Springer, 2019), 99.

[12] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 18.

Biometric identifiers, including facial images, contain personal information that, when extracted, can link directly back to the individual.[13] The impacts of technology on privacy and anonymity equate to societal and ethical issues raised by the public.

Freedom of speech, movement, and assembly are constitutionally protected activities. Although freedom of speech, movement, and assembly are classified as constitutional issues, they are not mutually exclusive and correspond with privacy implications. Civil Rights advocates assert that FRT impacts our First Amendment rights to unabridged free speech, peaceful assembly, and the right to movement.[14] The potential for surveillance causes individuals to change their behavior leading to censorship.[15] Constitutional matters impact society and societal behaviors causing consternation despite the security benefits.

Another ELSI is bias and inaccuracy within FRT. Inaccurate or biased facial recognition algorithms can adversely affect the public. Misidentification has led to false incarceration, denied access, and benefit delays. Rigorous reporting on the performance metrics, environmental factors, and an understanding of the algorithm are essential to a successful program.[16] Understanding how facial recognition algorithms perform within the public sphere allows policy and decision-makers to foster public trust and technology acceptance.

The final societal and ethical consideration category is data management and accountability. Facial images are identified as PII and, therefore, are subject to

[13] Blaz Meden et al., "Privacy-Enhancing Face Biometrics: A Comprehensive Survey," *IEEE Transactions on Information Forensics and Security* 16 (2021): 4191, https://doi.org/10.1109/TIFS.2021.3096024.

[14] Clare Garvie and Laura Moy, *America under Watch: Face Surveillance in the United States* (Washington, DC: Georgetown Law Center on Privacy and Technology, 2019), https://www.americaunderwatch.com/.

[15] Garvie and Moy.

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

safeguarding.[17] Data transmission, storage, sharing, and usage should be limited, transparent, and secure. Data protection is imperative to the government's use of FRT.

The final element of ELSI is legal implications. Legal implications are an intrinsic element in ethical and societal concerns, but there is very little law regulating the use of FRT. This research does not discuss or analyze the legality or ethical foundations of existing laws related to biometrics, but it recognizes a lack of regulation and industry standardization for using FRT in security settings. In FRT's case, the technological advancement rate outpaces the law.[18] When technology, public perception, and legal foundations evolve at disparate rates, decision-makers need a tool to guide decision-making. Decision-makers can rely on ethical frameworks to formulate technology programs that balance security benefits with public protections.[19] Considering the social and behavioral sciences in developing emerging technology and implementation helps produce better and more informed outcomes for policy and decision-makers.[20] The lack of regulations governing FRT allows for the technology's immoral or corrupt application, creating ethical dilemmas and public contention for the HSE. Ethical frameworks incorporating ethical and societal issues mitigate ethical dilemmas.

Employing FRT as a security measure is an ethical dilemma the HSE faces. Because there are multiple approaches to resolving security challenges with varying degrees of societal impact, a methodology to think about and evaluate ethical dilemmas benefits HSE officials in making difficult choices that impact society.[21] Ethical frameworks provide a method and a set of standards for behavior that decision-makers can use to decide how to act in a range of situations, how to make decisions, and the reasons

[17] DHS Privacy Office, *Privacy Incident Handling Guidance* (Washington, DC: Department of Homeland Security, 2017), https://www.dhs.gov/publication/privacy-incident-handling-guidance-0.

[18] Hodge Jr., "The Legal and Ethical Considerations of FRT," 745.

[19] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 19.

[20] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*.

[21] Aaron Nelson, "Ethical Decision Making for Homeland Security" (master's thesis, Naval Postgraduate School, 2013), https://calhoun.nps.edu/handle/10945/37684.

behind decisions.[22] Ethical frameworks provide a mechanism to examine the thought processes used to contemplate actions outside normative approaches to issues and determine holistic resolutions.[23] Furthermore, the National Academies of Science contends that ethical frameworks encompassing questions addressing ethical, legal, and societal concerns during the decision-making process provide an apparatus to identify ethical problems and challenges during the initial phases of technology development.[24] The Academy further states that a systematic search for ethical, legal, and societal issues is important for anticipating and predicting areas of concern.[25] When decision-makers anticipate and identify problems before implementing novel technology, they possess the ability to mitigate the issues, improving public perception and adoption.

When regulations do not exist to guide the development of new technology, policy- and decision-makers must weigh emerging technology's benefits against the public's interest to determine the best path forward. Based on a review of media publications, advocacy group inquiries to government agencies, and other literature, common public interest topics includes privacy, constitutional violations, bias and accuracy, and data accountability. This research aims to analyze facial biometrics and its relationship with public interest through an ethical framework and a real-world case study.

B. RESEARCH QUESTION

How can facial recognition technology be implemented in a way that is both efficient and ethical?

---

[22] Sheila Bonde and Paul Firenze, "A Framework for Making Ethical Decisions" (Lecture, Making Choices: Ethical Decisions at the Frontier of Global Science, Brown University, May 2013), https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions.

[23] J. Luke Wood and Adriel A. Hilton, "Five Ethical Paradigms for Community College Leaders: Toward Constructing and Considering Alternative Courses of Action in Ethical Decision Making," *Community College Review* 40, no. 3 (July 2012): 196–214, https://doi.org/10.1177/0091552112448818.

[24] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 162–65.

[25] Chameau, Ballhaus, and Lin, 165.

C. RESEARCH DESIGN

This research takes a multi-pronged approach to analyze FRT and outline steps for responsible usage. First, this study explores the decision-making process using the "How to Do It Right" framework. Through the framework, the thesis identifies values and the corresponding vulnerabilities, risks, and mitigation measures. Next, the research reviews academic and security industry literature to identify cross-cutting themes about operational guideline that can be applied to FRT programs. Finally, this study explores best practices through a case study of CBP's BEE program. The goal of this research is to equip homeland security leaders with a framework to identify issues associated with FRT and align the decision-making process with adjudicating and mitigating ethical and societal concerns to produce a beneficial biometric security solution for society.

The first prong looks at the decision-making process. Ethics serve as a mechanism to rationalize human behavior, provide conceptual clarity in a moral sphere, and validate rules, actions, and decisions.[26] There are many ethical paradigms, underscoring different points and perspectives, such as outcome prediction and how one adheres to societal obligations to reach an ethically correct decision.[27] Mohamed Abomhara et al. proposed the "How to Do It Right" framework to analyze biometrically supported border control stations in the European Union. The thesis will utilize the "How to Do It Right" framework and apply it to the U.S. government's use of FRT. Assessing the use of FRT through the "How to Do It Right" ethical framework allows decision-makers to categorically address and mitigate the challenges, risks, and concerns about FRT before, during, and after deployment of FRT programs. The framework is a layered approach focusing first on societal, ethical, and legal issues and then on how to mitigate those issues. However, this thesis will exclude legal issues from the analysis. Figure 1 charts the steps in the "How to Do It Right" framework. This thesis will take the framework and insert principles found throughout the literature associated with FRT.

[26] Patrici Calvo, "The Ethics of Smart City: Moral Implications of Hyperconnectivity, Algorithmization and the Datafication of Urban Digital Society," *Ethics and Information Technology* 22, no. 2 (June 2020): 145, https://doi.org/10.1007/s10676-019-09523-0.

[27] Abomhara et al., "How to Do It Right."

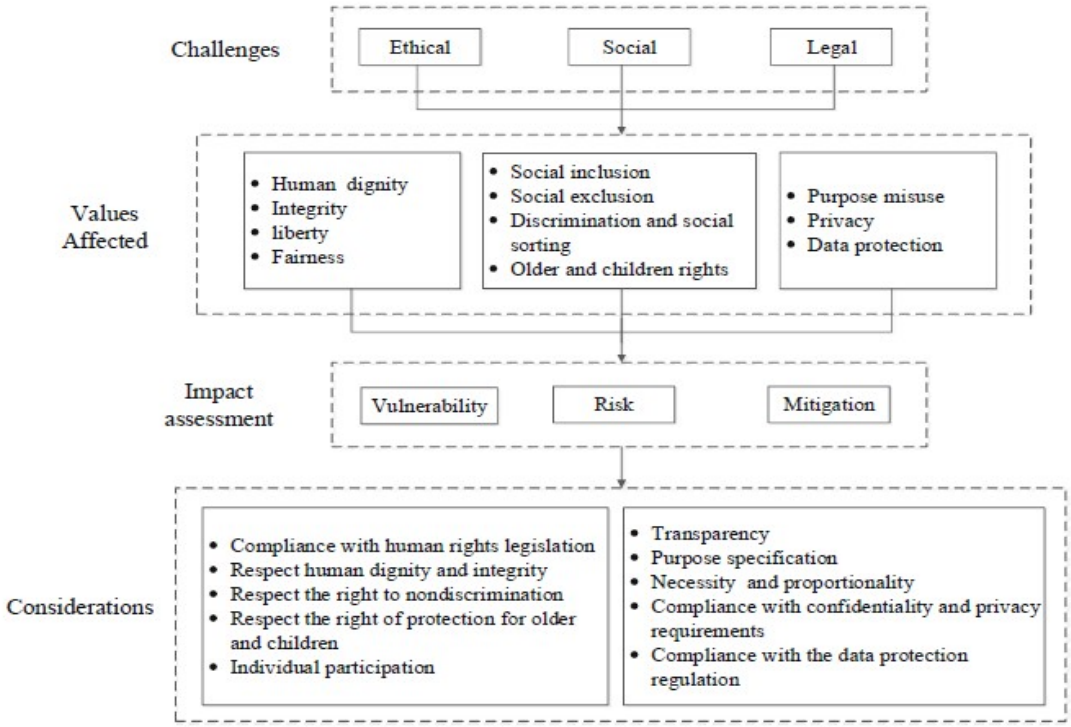

Figure 1. "How to Do It Right" Framework.[28]

The second prong of this research compares multiple operating principles proposed by the security industry for implementing FRT and identifies cross-cutting themes to be applied to FRT usage. Due to limited regulations governing the use of FRT, ethical principles play an essential role in the responsible usage of technology that impacts the public. Scientific and security industry groups propose various operating principles related to using FRT in public settings. There is no consensus on standardized and consistent principles. While the principles and guidelines are inconsistent across organizations, common elements exist within the proposed principles. When comparing the proposed industry principles, seven common themes emerge. These themes map to the "How to Do It Right" consideration tier. The cross-cutting principles are the foundational elements of employed mitigation measures that lead to responsible usage in the BEE program and apply to the broader use of FRT.

[28] Source: Abomhara et al.

Finally, the third prong examines CBP's Biometric Entry-Exit (BEE) program and uses the program as a case study to examine ethical program tenants, best practices, and operating principles. CBP's BEE was selected as a case study because it is an operational use of FRT in a security setting. Unlike other government programs, BEE is no longer considered a pilot or a technological test but rather a program of record, making it a more mature program. The BEE program has been the model and set the standards for other government agencies in the United States and abroad.[29] Furthermore, internal and external advocacy groups, stakeholders, Congress, the media, the U.S. Government Accountability Office (GAO), and the Office of Inspector General (OIG) have scrutinized the BEE program. The coverage has been both positive and negative, but overall, government audit groups have assessed the program positively.[30] Since its inception and through the iterative process based on auditing, the BEE program has identified ethical and societal concerns and mitigated them through a privacy-by-design approach, constitutional considerations, algorithm review, and data protection measures. When assessed through an ethical framework, the BEE program will demonstrate best practices and issue mitigation measures that have garnered some public trust in the program.

This research aims to bridge the gap between benefits, ethical and societal impacts, and technology by outlining principles that, when implemented, constitute the responsible use of facial recognition. It will analyze publicly available information on biometrics, facial recognition, and the BEE program. This information includes news articles, government studies, reports and audits, white papers, congressional testimony, and advocacy group publications.

---

29 "CBP Biometrics," CBP Biometrics, accessed December 27, 2021, https://biometrics.cbp.gov; Department of Homeland Security, "Biometrics," Department of Homeland Security, October 24, 2016, https://www.dhs.gov/biometrics; and, Rebecca Gambler, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, DC: Government Accountability Office, 2020).

30 Candice Wright and Gretta Goodwin, *Facial Recognition Technologies: Current and Planned Uses by Federal Agencies*, GAO-21-526 (Washington, DC: Government Accountability Office, 2021), https://www.gao.gov/products/gao-21-526; Office of Inspector General, *CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports*, OIG-22-48 (Washington, DC: Department of Homeland Security, 2022); and, Rebecca Gambler, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, DC: Government Accountability Office, 2020).

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Facial recognition is a subcategory within the field of biometrics. Biometrics are measurable biological and behavioral characteristics that can be used for identification, including fingerprints, gait, voice, DNA, and facial images.[31] While all biometrics may be discussed or mentioned throughout this thesis, the literature review focuses on research and documentation associated with facial images and the technology used to match faces to identities. The origins of FRT stem from the work conducted in the 1960s by William Bledsoe, but the widespread use of FRT in law enforcement has emerged as a more recent phenomenon.[32] As an emerging technology with a long historical evolution, literature is available addressing technical, operational, legal, ethical, and societal topics and challenges. This review will narrow the scope and examine the literature regarding ethical and societal issues.

This research categorizes the literature into three areas: challenges and benefits, operating principles, and ethical frameworks. The first two categories relate specifically to FRT systems and programs. The challenges and benefits section examines academic, industry, government, and media documents to identify FRT perceptions and criticisms. The second section reviews the literature assessing and proposing operating principles for FRT. The third category encompasses a general ethics discussion and identifies ethical frameworks that apply to case study analysis and the FRT decision-making process.

A. CHALLENGES AND BENEFITS

In the last decade, with critical advancements in technology and matching algorithms, FRT has emerged as the future of biometric systems. Emerging technologies are often coupled with uncertainty about the impacts of the technology on society, generating fear and criticism. The foundational research for FRT began in the 1960s when scientists attempted to train a computer to see human faces and distinguish those faces from

[31] Department of Homeland Security, "Biometrics."

[32] Gates, *Our Biometric Future*.

other faces.[33] There was sporadic development of automated face and pattern recognition over the following decades, typically funded by the military. It was not until the 1990s that companies began to market commercial facial recognition systems to law enforcement.[34] The first use of FRT in the public realm was at the 2001 Super Bowl. The technology made 14 face matches, but the police made no arrests.[35] The Super Bowl use case sparked controversy and evoked fear among the public and civil rights advocates laying the foundation for the FRT criticisms espoused today. This section outlines the common challenges and criticisms found in academic papers, white papers, security industry reports, legal documents, and media accounts.

Common criticisms of FRT and facial recognition systems in the literature focus on a few broad areas, including privacy implications, impediments of movement and speech, and securitization of identity. Privacy implications are frequently cited by members of Congress, advocacy groups, and the academic literature.[36] For instance, Senator Al Franken said he has "serious concerns about facial recognition technology and how it might shape the future of privacy."[37] The word "privacy" does not appear in the United States Constitution, but many legal scholars contend that privacy is a right inferred from

[33] Gates, *Our Biometric Future*, 3.

[34] Gates, 12.

[35] John D. Woodward, *Biometrics: Facing up to Terrorism* (Santa Monica, CA: RAND Corporation, 2001), 10, https://www.rand.org/pubs/issue_papers/IP218.html.

[36] As seen in the following examples: Clare Garvie and Laura Moy, *America under Watch: Face Surveillance in the United States* (Washington, DC: Georgetown Law Center on Privacy and Technology, 2019); Electronic Privacy Information Center, "EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures)," EPIC, accessed December 28, 2021, https://www2.epic.org/foia/dhs/cbp/alt-screening-procedures/#background; Data Privacy and Integrity Advisory Committee, *Privacy Recommendations in Connection with the Use of Facial Recognition Technology*, Report 2019–01 (Washington, DC: Data Privacy and Integrity Advisory Committee, 2019), https://www.hsdl.org/?view&did=847055; Thorin Klosowski, "Facial Recognition Is Everywhere. Here's What We Can Do About It," *Wirecutter: Reviews for the Real World* (blog), July 15, 2020, https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/; Washington Post, "Forcing Facial Recognition Is a Mistake," *Washington Post*, February 7, 2022, https://www.proquest.com/newspapers/forcing-facial-recognition-is-mistake/docview/2625929250/se-2?accountid=12702.

[37] Sharon Naker and Dov Greenbaum, "Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy," *Boston University Journal of Science and Technology* 23 (2017): 96, https://www.bu.edu/jostl/files/2017/04/Greenbaum-Online.pdf.

numerous amendments in the Bill of Rights and supported in case law.[38] In the Fourth Amendment case Carpenter v. The United States, Supreme Court Chief Justice John Roberts stated, "a person does not surrender all Fourth Amendment protection by venturing into the public sphere."[39] In his opinion, Chief Justice Roberts refers to the reasonable expectation of freedom from governmental intrusion inherent in the Fourth Amendment. Privacy advocates within the Electronic Privacy Information Center (EPIC), the Data Privacy and Integrity Advisory Committee (DPIAC), the Electronic Frontier Foundation (EFF), and the Georgetown Law Center on Privacy and Technology claim FRT violates the privacies of life afforded by the Constitution and confirmed in Carpenter because FRT can track whereabouts, effectively revealing a person's family, political, social, professional, religious, and sexual affiliations.[40] Government officials recognize that facial images are ubiquitous, more difficult to conceal or avoid collection than fingerprints and iris, and can be captured from a distance without an individual's knowledge or consent.[41] Because of the ubiquity of a face, critics assert FRT is invasive and violates privacy.

When technology can identify individuals from a distance, the idea of anonymity is diminished.[42] Susan Herman argues that privacy and freedom go hand and hand. In her book, *Taking Liberties: The War on Terror and the Erosion of American Democracy*, she contends that the framers of the Constitution penned the Fourth Amendment with privacy specifically in mind to protect citizens from government intrusion; after 9/11, Herman claims, the government began to erode those protections in the name of security.[43] The right to privacy is front and center when discussing facial recognition, but freedom of

[38] Griswold v. Connecticut, 381 U.S. 479 (1965).

[39] Carpenter V. United States, 81 (2018).

[40] Garvie and Moy, *America under Watch: Face Surveillance in the United States*.

[41] Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service," Department of Homeland Security, November 15, 2018, 9, https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

[42] Eric Z. Wynn, "Privacy in the Face of Surveillance: Fourth Amendment Considerations for Facial Recognition Technology" (master's thesis, Naval Postgraduate School, 2015), 2, http://hdl.handle.net/10945/45279.

[43] Susan N. Herman, *Taking Liberties: The War on Terror and the Erosion of American Democracy*, *Taking Liberties* (Cary, UK: Oxford University Press, 2011).

movement and freedom of speech are closely linked and often debated concurrently by privacy advocates and other critics of the technology.

Privacy and civil rights advocates assert that facial recognition may have "a chilling effect on our First Amendment rights to unabridged free speech and peaceful assembly."[44] Many people assume that if you are not doing anything wrong, government surveillance should not be an issue, but Claire Garvie and Laura Moy argue that "the mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."[45] Building on Garvie and Moy's arguments, the Chicago Review published an article declaring, "when…technologies are deployed to preemptively enforce the law—to detect where we go, with whom we engage, and even to identify us within large gatherings—it can become an affront to our civil rights and liberties."[46] Similarly, the EFF asserts that, as law enforcement increases the number of photos in their databases, anyone could end up in a database without their knowledge because they are in the wrong place at the wrong time, fit a stereotype, or engage in activities such as political protest.[47] Some advocacy groups call for outright bans on facial recognition technology, while others want more oversight or governing policy to protect civil rights and liberties.[48] Regardless of a desire for an outright ban or restrictions, critics express concerns over law enforcement's use of facial recognition at rallies and protests and question the constitutionality of its use.

Another challenge associated with FRT is the potential to impede an individual's right to free movement. The U.S. Constitution and the Supreme Court recognize freedom

---

[44] Garvie and Moy, *America under Watch: Face Surveillance in the United States*.

[45] Garvie and Moy.

[46] Andres Crucetta Nieto, "Is Facial Recognition Inhibiting Our Freedom of Speech?," *Chicago Policy Review*, October 12, 2020, https://chicagopolicyreview.org/2020/10/12/is-facial-recognition-inhibiting-our-freedom-of-speech/.

[47] Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology* (San Francisco: Electronic Frontier Foundation, 2018), 7, https://www.eff.org/wp/law-enforcement-use-face-recognition.

[48] Aaron Schaffer, "The Cybersecurity 2022: Activists and Lawmakers Increase Calls for Ban on Federal Use of Facial Recognition Technology," *Washington Post*, July 2, 2021, https://www.washingtonpost.com/politics/2021/07/02/cybersecurity-202-some-activists-lawmakers-want-ban-federal-government-using-facial-recognition-technology/.

of interstate movement without government abridgment.[49] Richard Sobol argues that photo identification requirements and other government technology, including FRT, impede the inherent right of movement.[50] The limitations of movement can inhibit a person's freedoms and ability to express their religious, professional, political, or sexual affiliations without government interference.

Critics argue that biometrics offer the public and the private sectors the ability to associate disembodied identities with physical bodies (names to faces) and vice versa, forming official identities. Biometrics further offers both sectors the capability to securitize identity. By securitizing identity, politicians shift the social issue of identity into an area of existential threats that require extraordinary measures or policies outside the normal political procedure.[51] According to Nikolas Rose, the securitization of identity is a means to contain individuals into delineated in- and out-groups by classifying identity as either law-abiding, self-governing citizens or problematic persons subject to repressive government strategies.[52] Rose further argued that individuals now require proof of legitimate identity to exercise freedoms and participate in any contemporary practice.[53] Because FRT can associate faces with names, providing an official identity, securitization can further exacerbate the idea that FRT violates privacy and constitutional freedoms.

Advocacy groups and academics often cite bias and misidentification as significant risks to FRT. Studies conducted by the National Institute of Standards and Technology (NIST) show that face recognition technology may perform differently on different demographics and poorly identifies individuals with darker skin color; but

[49] Richard Sobol, "The Right to Travel and Privacy: Intersecting Fundamental Freedoms," *John Marshall Journal of Information Technology & Privacy Law* 30, no. 4 (2014): 639–68, https://repository.law.uic.edu/jitpl/vol30/iss4/1.

[50] Sobol, 641.

[51] Barry. Buzan, Waever Ole, and Jaape de Wilde, *Security: A New Framework for Analysis*, *Security : A New Framework for Analysis* (Boulder, CO: Lynne Rienner Pub., 1998), 24.

[52] Nikolas S. Rose, *Powers of Freedom: Reframing Political Thought*, *Powers of Freedom : Reframing Political Thought* (Cambridge: Cambridge University Press, 1999), 240.

[53] Rose, 240.

depending on the algorithm quality, the differences are negligible.[54] Despite NIST's disclaimer that demographic differentials depend on algorithm quality, academics and privacy advocates focus on the idea that there may be bias. For example, the American Civil Liberties Union (ACLU) used an off-the-shelf facial recognition tool from Amazon that matched 28 members of Congress, mostly members of color, to mugshots.[55] According to Amazon, the ACLU utilized the facial matching algorithm at a confidence threshold of 80%, which is well below the 95% threshold Amazon recommends for law enforcement activities.[56] Garvie and Moy from Georgetown University express concerns that the "risks of face surveillance are likely to be borne disproportionately by communities of color."[57] The prominent Detroit, Michigan case of Michael Oliver, a man of color that was falsely accused and charged with a crime he did not commit based on FRT, is cited by Garvie and Moy, as well as the ACLU.[58] In response, the Detroit Police Department stated, "facial recognition software is an investigative tool used to generate leads only. Additional investigative work, corroborating evidence, and probable cause are required before an arrest."[59] Scientific studies indicate that there can be bias within facial recognition systems, but any bias or poor identification rates depend on the algorithm's quality.

---

[54] U.S Congress. House of Representatives, *Examining the Department of Homeland Security's Use of Facial Recognition and Other Technologies.*, House of Reps, 116th Congress, First Session, July 10, 2019; Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (Gaithersburg, MD: National Institute of Standards and Technology, December 2019), https://doi.org/10.6028/NIST.IR.8280; U.S Congress. House of Representatives, *Facial Recognition Technology: Part I Its Impact on Our Civil Rights and Liberties*, House of Reps, 119th Congr., First session, May 22, 2019; Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, "Perpetual Line Up" (Washington, DC: Georgetown Law Center on Privacy and Technology, October 18, 2016), https://www.perpetuallineup.org/findings/racial-bias; Sandra Taylor, *Response to DHS 2019–00001, DHS Data Privacy and Integrity Advisory Council* (Washington, DC: Center for Democracy and Technology, 2019).

[55] Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots."

[56] William Crumpler, "How Accurate Are Facial Recognition Systems and Why Does It Matter?," *Strategic Technology* (blog), accessed September 2, 2022, https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

[57] Garvie and Moy, *America under Watch: Face Surveillance in the United States*.

[58] Elisha Anderson, "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit," *Detroit Free Press*, July 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

[59] Bobby Allyn, "'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man," NPR: America Reckons with Racial Injustice, June 24, 2020, https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

Contrary to the criticisms outlined in the literature, the security industry, academics, and government agencies have published literature highlighting FRT's benefits and positive public perception. For example, a Pew Research report contends that over 60% of Americans believe traveling in public without being identified is a worthwhile social endeavor, but the same report finds that "a majority of Americans (56%) trust law enforcement agencies to use these technologies responsibly. A similar share of the public (59%) believes it is acceptable for law enforcement to use facial recognition tools to assess security threats in public spaces."[60] The Pew research illustrates that the public supports FRT but at the same time has some reservations about the technology. It further demonstrates that responsible usage and transparency garner public support. Sara Katsansis et al. conducted a study on FRT in the public health sector and found similar results. According to the survey, 63% of respondents approved of using FRT for identification purposes of staff and patients, 57% approved of FRT to track people entering and leaving hospitals, and 52% approved of using FRT in pharmacies to prevent fraud and identity theft.[61] These surveys show that, in many instances, the public supports using FRT.

The RAND Corporation, the security industry, government entities, and media outlets identify beneficial uses of FRT in law enforcement and the private sectors. The common uses identified include, but are not limited to, access to secured areas, computer or network access, financial transactions, contactless access and processes in hospitals, voting, passport, and visa issuance, prison access and inmate identification, preventing identity theft and fraud, counterterrorism efforts, and identifying suspects.[62] Although often preempted with phrases like "the controversial technology" or "hot-button" topic,

[60] Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly* (Washington, DC: Pew Research Center, 2019), https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

[61] Sara H. Katsanis et al., "A Survey of U.S. Public Perspectives on Facial Recognition Technology and Facial Imaging Data Practices in Health and Research Contexts," ed. Renuka Sane, *PLOS ONE* 16, no. 10 (October 14, 2021): 1–16, https://doi.org/10.1371/journal.pone.0257923.

[62] As seen in the following articles: Sean O'Connor, "Biometrics and Identification After 9/11," *Bender's Immigration Bulletin* 7 (February 2002): 150–73, https://doi.org/10.2139/ssrn.299950; John D. Woodward, *Biometrics: Facing up to Terrorism* (Santa Monica, CA: RAND Corporation, 2001), https://www.rand.org/pubs/issue_papers/IP218.html; and, David Dunlap, "Securing Our Hospitals and Protecting Your Privacy," *Campus Security and Life Safety*, March 2019, https://campuslifesecurity.com/digital-edition/2019/04/digital-edition_march_april/asset.aspx.

extensive reports and news articles tout the benefits and FRT success stories. The Security Industry Association (SIA) published a report outlining FRT success stories which included the identification of over 15,000 exploited children, the arrest of over 17,000 traffickers, the identification of the New York City Subway Bomber, the apprehension of over 1,500 imposters attempting to enter the United States, the use by the Innocence Project to rectify witness misidentifications, and the arrest of the Capital Gazette Killer.[63] A 2019 New York Post article stated, "police used controversial facial-recognition technology to track down an accused rapist fewer than 24 hours after he tried to force a woman into sex at knife-point."[64] These examples demonstrate that FRT embodies a public benefit, despite the criticisms.

B. OPERATING PRINCIPLES: MITIGATING THE CHALLENGES

As FRT becomes widely accepted as the standard identity verification or authentication method in security settings, ethical issues arise regarding the technology's overall impact on society and the environment. According to Anthony Carter and Eric Baker, there are no universal policies or regulations governing biometric data collection, usage, sharing, and storage, which raises ethical concerns regarding how law enforcement uses or plans to use FRT.[65] Debates and discussions around these ethical and societal impact issues are avenues to introduce moral principles that govern technology implementation and usage.[66] At the same time, there are outstanding questions regarding the best mechanisms to mitigate the challenges and fears of FRT. Security organizations, academics, and government agencies have published operating principles designed to minimize public concern and ensure the technology's ethical implementation. Section two

[63] Parker, "Facial Recognition Success Stories."

[64] McCarthy, "Facial Recognition Leads Cops to Alleged Rapist in Under 24 Hours."

[65] Anthony Carter, "Facing Reality: The Benefits and Challenges of Facial Recognition of the NYPD" (master's thesis, Naval Postgraduate School, 2018), http://hdl.handle.net/10945/60374; and Eric Baker, "I've Got My AI on You: Artificial Intelligence in the Law Enforcement Domain" (master's thesis, Naval Postgraduate School, 2021), http://hdl.handle.net/10945/67100.

[66] Matt Lovegrove, "Why We Need to Talk about Ethics in Technology," Hello World, 2020, https://helloworld.raspberrypi.org/articles/HW06-why-we-need-to-talk-about-ethics-in-technology.

of this review introduces, compares, and contrasts various operating principles charted in the literature.

There are security organizations that support the use of FRT but propose similar operating principles. One such organization is SIA, a non-profit trade association representing over 1,200 companies that aim to promote success within the global security industry through information, insight, and influence.[67] SIA identifies ten core principles: "transparency, clear and defined purpose, accurate technology, human oversight, non-discrimination, data security, privacy by design, training and education, ethical acquisition, and targeted public policy."[68] SIA further supports legal and well-defined use, consistent with morals, constitutional rights, policies, and regulations, of FRT by government entities.[69] Another organization proposing principles is the International Biometrics + Identity Association (IBIA), an international trade group representing the identification technology industry.[70] The IBIA principles include collection limitation, purpose specification, data quality, user access limitations, security safeguards, openness, accountability, and redress. IBIA introduces the idea of accountability and redress, but purpose, transparency, and data quality principles overlap with SIA and other industry organizations.

Other organizations are indifferent to the usage of FRT but endorse public awareness and propose privacy principles. The Future of Privacy Forum (FPF) is a non-profit organization focused on exploring challenges posed by technological innovation and privacy protections, ethical standards, and best practices that mitigate the challenges. FPF

67 "About SIA," Security Industry Association, accessed August 27, 2022, https://www.securityindustry.org/about-sia/.

68 Security Industry Association, *Sia Principles for the Responsible and Effective Use of Facial Recognition Technology* (Silver Springs, MD: Security Industry Association, 2020), https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

69 Security Industry Association.

70 International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles* (Washington, DC: International Biometrics and Identification Society, 2021), https://www.ibia.org/resources/white-papers.

proposes its own set of principles.[71] The FPF principles include consent, context, transparency, data security, privacy by design, data integrity and access, and accountability.[72] FPF advocates that their seven principles provide essential safeguards and are critical to any basis for collecting and using facial recognition data.[73] As with other organizations, privacy, data protection, accuracy, and transparency are key and common principles.

The Center for Strategic and International Studies (CSIS) has also published responsible use principles for FRT. CSIS is a non-profit policy research organization committed to advancing realistic concepts to address the world's most significant challenges.[74] The CSIS principles include authorized use, consent, transparency, data retention, independent use, redress, oversight and auditing, algorithm review, and training.[75] As with the other three organizations, CSIS includes data integrity and transparency, but where CSIS diverges is the category of algorithm review. Algorithm review could fall into the data accuracy category, but CSIS surmises maintaining a high-quality algorithm is imperative to FRT success.

This literature review focused on four well-respected organizations. Still, there are numerous other guiding principles from organizations like the World Economic Forum, National Telecommunications and Information Administration, DPIAC, and the Canadian Government. The four documented organizations articulated different principles, but overall, there are common threads throughout all the organizations. The research method in this thesis attempts to crosswalk the various organizational principles and provide a

71 "About," Future of Privacy Forum, accessed August 27, 2022, https://fpf.org/about/.

72 Future of Privacy Forum, *Summary of Privacy Principles* (Washington, DC: Future Privacy Forum, 2018), https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf.

73 Future of Privacy Forum.

74 "About Us," Center for Strategic and International Studies, accessed August 27, 2022, https://www.csis.org/programs/about-us.

75 James Andrew Lewis and William Crumpler, *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape* (Washington, DC: Center for Strategic and International Studies, 2021), https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape

standard set of operating principles that can be incorporated into and viewed through an ethical framework when implementing FRT.

C. ETHICS AND ETHICAL FRAMEWORKS

The discipline of ethics is a wide-ranging field of study. To narrow the scope of this literature review, it will focus on standards that influence behaviors and decision-making. From an emerging technology perspective, ethical principles are necessary to help professionals determine what they should and should not do with the technology they create. These principles also play a role in clarifying normative social and professional behavior.[76] Andrea North-Samardzic asserts that one of the main questions regarding the implementation of technology is who should be responsible for the ethical implications of that technology, and she concludes that "the organizations that deploy the technology should be accountable."[77] Adhering to ethical principles and concepts can be a mechanism to guide the ethical implementation and mitigate the criticism and societal impacts of FRT.

Western moral philosophers have advanced three moral philosophies useful in analyzing moral problems and making decisions: consequentialism, deontological ethics, and virtue ethics.[78] Consequentialism is a common approach to ethical decision-making, especially decisions that impact large groups.[79] Consequentialism explores the consequences of actions and asks what action will provide the greatest good for the greatest number of people, accounting for harms and benefits.[80] Deontological ethics judge the morality of actions in compliance with duties, rights, and justice.[81] The third ethical

[76] Desmond C. Ong, "An Ethical Framework for Guiding the Development of Affectively-Aware Artificial Intelligence," in *2021 9th International Conference on Affective Computing and Intelligent Interaction (ACII)* (IEEE, 2021), 2.

[77] Andrea North-Samardzic, "Biometric Technology and Ethics: Beyond Security Applications," *Journal of Business Ethics* 167, no. 3 (2019): 433–50, https://doi.org/10.1007/s10551-019-04143-6.

[78] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 119.

[79] Bonde and Firenze, "A Framework for Making Ethical Decisions."

[80] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 119.

[81] Joseph Migga Kizza, *Ethical and Social Issues in the Information Age*, Texts in Computer Science (Cham, Switzerland: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-70712-9.

philosophy that applies to decision-making is an agent-centered virtue philosophy, which, unlike consequentialism and deontological ethics, focuses on individuals' or agents' overall ethical status.[82] These three broad categories contain a variety of approaches to ethics, which may be used to derive ethical frameworks to aid in the decision-making process.

The literature presents various ethical frameworks for decision-making that incorporate classical ethical theories. Joseph Kizza outlines an ethical framework that outlines a set of questions and reflections to consider during the decision-making process. Kizza's set includes recognizing inherent ethical conflicts, understanding the challenge, knowing the participants, exhibiting knowledge of ethical practices, identifying alternative solutions, understanding how decisions are instituted, and understanding the impact on all parties involved.[83] Kudina and Verbeek recommend using technomoral scenarios to analyze and anticipate the societal impacts of technology, wherein technomoral scenarios are structured in a way that anticipates "consequences based on empirical research and analyses of the current practices that will be affected by new technologies."[84] Abomhara et al. propose the "How to Do It Right" framework. The "How to Do It Right" framework is a four-tiered framework with ethical, social, and legal challenges on top, values affected by the change in the next tier, a third tier including a value assessment, and a bottom level which includes corresponding considerations.[85] Each of these ethical frameworks draw from one of the three classical theories and present a singular ethical approach to decision-making.

There are also comparative frameworks that explore ethics from different schools of thought at the same time. For example, Sheila Bonde and Paul Firenze propose a comparative framework using consequentialist, duty, and virtue frameworks as the basis for making decisions.[86] The consequentialist framework aims to produce the most good

[82] Bonde and Firenze, "A Framework for Making Ethical Decisions."

[83] Kizza, *Ethical and Social Issues in the Information Age*, 39.

[84] Kizza, 295.

[85] Abomhara et al., "How to Do It Right," 6.

[86] Bonde and Firenze, "A Framework for Making Ethical Decisions."

for those affected by considering all the potential impacts of the decision or action.[87] The duty framework focuses on a decision-maker's duties and obligations in a situation and identifies what the ethical obligations are and what behaviors are inappropriate in the situation. Finally, the virtue framework identifies the character traits that might motivate decision-making in any situation.[88] The Markkula framework also identifies multiple theories or lenses to make ethical decisions. The Markkula framework allows the decision-maker to choose the appropriate lens and then asks the user to follow five steps: 1. identify the problem, 2. get the facts, 3. evaluate alternatives, 4. opt for action and testing, and 5. implement the decision and reflect on the outcome.[89] Also, according to the Markkula method, making good ethical decisions requires "a practiced method for exploring the ethical aspects of a decision and weighing the considerations that should impact our choice of a course of action."[90] In summary, utilizing an ethical framework helps guide the decision-making process, especially when implementing new technologies that impact society.

D. CONCLUSION

Overall, ample literature explores FRT, its challenges, and its ethical implications. The literature identifies criticism and documents shortfalls of the technology, and while mentioning benefits, it fails to balance the criticisms with the benefits. The literature provides limited solutions to mitigate the objections or standardized guidelines and practices to implement the technology. Although the challenges and benefits are laid out in the security industry literature, there is little research using FRT case studies to analyze the societal and ethical criticisms existing in the literature.

In North-Samardzic's review of the biometric literature, she specifically points out that there has not been "sufficient attention given to ethical frameworks in the literature on

[87] Bonde and Firenze.

[88] Bonde and Firenze.

[89] Markkula Center for Applied Ethics, "A Framework for Ethical Decision Making," Markkula Center for Applied Ethics: Ethics Resources, November 8, 2021, https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/.

[90] Markkula Center for Applied Ethics.

biometrics in organizational contexts."[91] This literature review supports her claims and reveals very few case studies on operational FRT programs in law enforcement. Very little literature uses ethical frameworks to analyze specific FRT programs.

[91] North-Samardzic, "Biometric Technology and Ethics: Beyond Security Applications."

III. FACIAL RECOGNITION TECHNOLOGY BACKGROUND

The use of biometric indicators for identification purposes is not new. Biometric indicators uniquely identify individuals. They include fingerprint patterns, voice timbre, and facial characteristics. As a form of identification, biometrics has a longstanding legacy. The first credited systematic use of fingerprints dates back to 1858 in India, and historical accounts show the Babylonians using handprints as a form of identification as far back as 500 BC.[92] The International Association of Chiefs of Police established a National Bureau of Criminal Identification program designed to exchange arrest information in 1896, and on December 21, 1911, the Illinois State Supreme Court upheld "the admissibility of fingerprint evidence concluding that fingerprints are a reliable form of identification."[93] Modern FRT was founded in 1960 when Woodrow Wilson Bledsoe established a measurement system to classify photos.[94] FRT has evolved since 1960. Its evolution adhered to a natural progression of emerging technology regardless of 9/11's influence on technological advancement.[95] In the 21st century, the face is fast becoming the biometric of choice in security settings. This chapter will provide an overview of FRT by explaining how FRT works, the types of FRT, and the ethical implications FRT generates.

A. HOW FRT WORKS

The first step in understanding how biometric identification works is to define biometrics. Biometrics are "measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition."[96] Facial recognition uses software to determine the similarity between two face images to evaluate an identity

[92] Mark A. Acree, "People V. Jennings: A Significant Case for Fingerprint Science in America," *Journal of Forensic Identification* 65, no. 4 (2015): 600–602.

[93] Acree.

[94] Klosowski, "Facial Recognition Is Everywhere. Here's What We Can Do About It."

[95] Gates, *Our Biometric Future*, 45.

[96] Department of Homeland Security, "Biometrics."

claim.[97] FRT uses the spatial geometry of facial features to create a template based on numerical computations. A template is distinct from a photograph (referred to as a photo throughout this document) because it limits the number of details to only those that can be used to distinguish one face from another.[98] An algorithm or system will generate a similarity score (threshold) to determine a match between a live image (probe photo) or video footage and a known image (source photo). A basic FRT system includes the capture device, the software, and an algorithm. A quality algorithm will allow the matching thresholds or criteria to be configurable based on the use case.

There are four basic steps to a facial recognition system. The first step begins with capturing the probe photo. The probe photo can be a live image, a still photo, or a photo captured from a live stream video. Once the system captures an image, the software extracts the face attributes to generate a template. The template is compared to database source photos, which are translated into templates for comparison purposes. Finally, the software decides on matching results based on algorithmic criteria. There may be variations to the four-step process outlined in Figure 2, but the final step always provides an identification result to the user.

[97] William Crumpler and James Andrew Lewis, *How Does Facial Recognition Work?* (Washington, DC: Center for Strategic and International Studies, 2021), https://www.csis.org/analysis/how-does-facial-recognition-work.

[98] Lynch, *Face Off*.

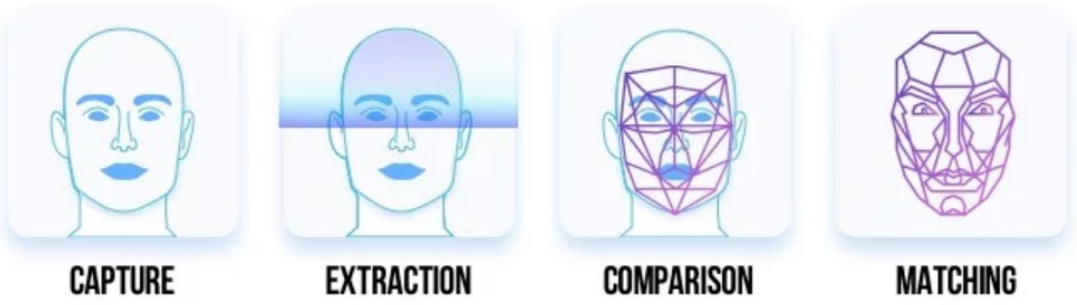

Figure 2. The Four-Step Process.[99]

FRT returns four types of results: a true positive (an accurate match), a true negative (an accurate rejection), a false positive (a misidentification), and a false negative (a false non-match).[100] When analyzing bias and inaccuracy, false positive and false negative results both raise security concerns. A false positive results in a misidentification. A false negative can fail to identify an individual. Algorithmic acceptance thresholds are set to determine an acceptable rate of false positives and false-negative results. For example, higher thresholds reduce the likelihood of a misidentification or false positives, but higher thresholds can increase the possibility of a no-match when a match should be made or what is deemed a false negative.[101] The FRT system owner must balance threshold levels against the security or threat level and the efficacy of the match results.

B. TYPES OF FRT

The operational use cases of FRT may be diverse, but recognition technology operates within the confines of two capabilities: identification and verification. The two terms are often used interchangeably but have distinct scientific meanings.

[99] Source: Deepti Chamoli, "Deep Learning-Based Live-Streaming Face Recognition," *Analytics Vidhya* (blog), November 14, 2019, https://medium.com/analytics-vidhya/deep-learning-based-live-streaming-face-recognition-31e9b005ffb.

[100] Kristin Finklea et al., *Federal Law Enforcement Use of Facial Recognition Technology*, CRS Report No. R46586 (Washington, DC: Congressional Research Service, 2020).

[101] Joy Buolamwini et al., *Facial Recognition Technologies: A Primer* (Chicago: The McArthur Foundation, 2020), https://www.ajl.org/federal-office-call.

1. Identification (1:N)

Face identification asks the question, "whose face is this?"[102] It determines an unknown individual's identity by comparing submitted face imagery to reference or source face imagery.[103] Face matching in the identification environment is referred to as one-to-many matching, one-to-many comparison, or simply 1:N. Examples of face identification include criminal investigations, terrorist identification, and victim identification.

2. Verification (1:1)

Face verification asks, "does this face belong to person X?"[104] It confirms an individual's claimed identity by comparing submitted face imagery to reference or source face imagery associated with the claimed identity or limited gallery of expected individuals seeking verification. Essentially, verification confirms that a person is who they say they are.[105] Face verification is typically referred to as one-to-one matching or 1:1. Smartphone access, banking access, and building access are forms of verification, making it the most used format of FRT.

The difference between verification and identification occurs after the live photo is captured and templatized. A live photo is compared to either a known, stored image to verify identity or a set or group of photos to determine an identity. Figure 3 illustrates the differences between identification and verification once a live photo is captured and templatized.

---

[102] Buolamwini et al., 6.

[103] Crumpler, "How Accurate Are Facial Recognition Systems and Why Does It Matter?"

[104] Buolamwini et al., *Facial Recognition Technologies: A Primer*, 6.

[105] Crumpler, "How Accurate Are Facial Recognition Systems and Why Does It Matter?"

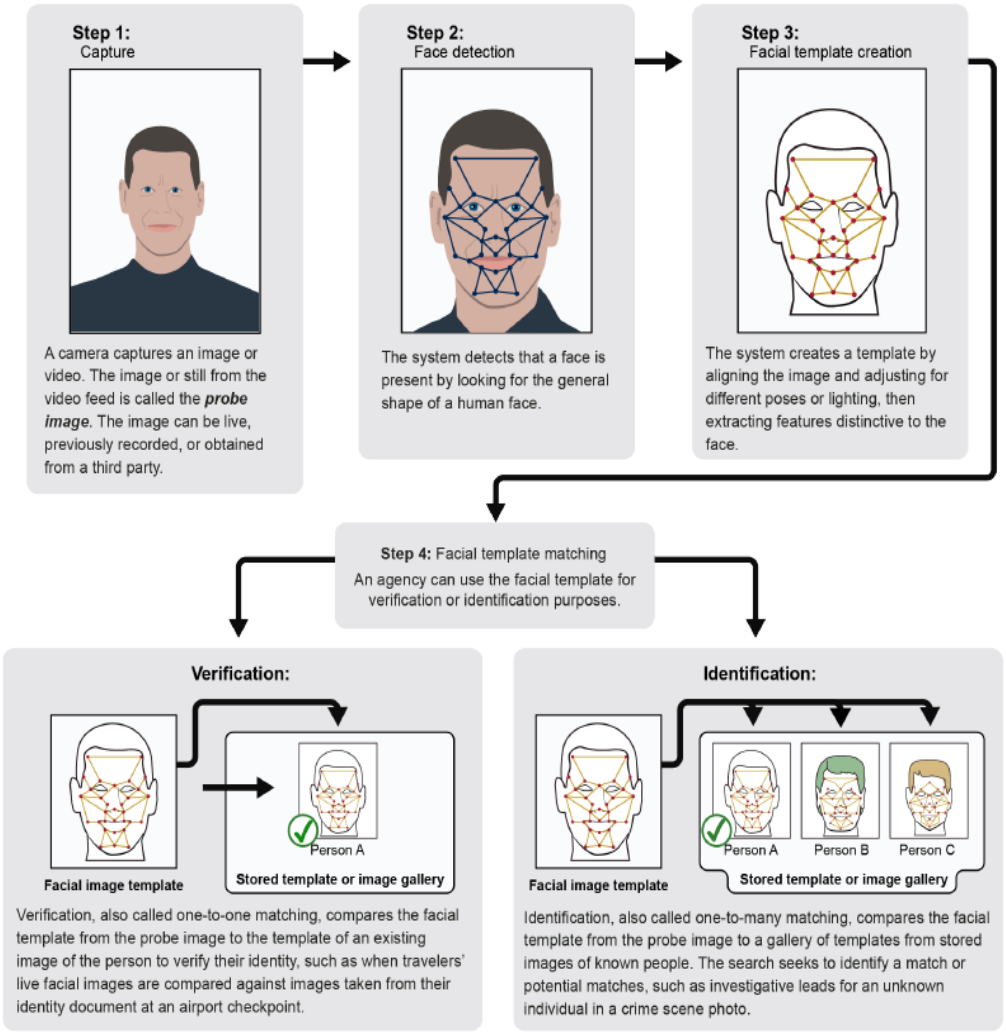

Figure 3. Verification and Identification.[106]

C. ETHICAL IMPLICATIONS OF TECHNOLOGY

An increasing number of organizations have begun to use FRT, and the technology is becoming more and more commonplace in the public and private sectors. Corporations like Disney use facial recognition to enter parks, and Apple uses the technology to unlock mobile devices and pay for purchases. Department stores use the technology to prevent

[106] Source: Finklea et al., *Federal Law Enforcement Use of Facial Recognition Technology*.

theft and fraud.[107] According to a 2020 GAO survey of 24 government agencies, 19 used or planned to use FRT in some manner.[108] As government use of FRT expands biometric identification usage to the public sphere, the technology has gained the attention of the public, civil rights advocates, and policymakers. As an emerging technology, biometrics are disruptive with the capacity to "restructure, reorganize, disrupt current social and institutional norms and standards, operations, production, trends not limited to a particular market or industry."[109] The disruptive nature of new technology can cause friction between the technology and the public. As with any new technology, public and private sectors are often skeptical and raise concerns about how the government uses technology, how the accuracy may impact the public, and the technology's impacts on privacy and security. The following section outlines four commonly cited concerns that decision-makers should consider when implementing FRT.

1. Privacy Implications

The responsible use of FRT requires privacy protection considerations. By definition, biometric data is unique and traces to specific individuals. Biometric identifiers contain personal data that, once extracted, allows the government to infer meaningful personal and private information from the data itself.[110] Facial images are ubiquitous; it is more difficult to conceal or avoid collection of facial images than fingerprints and irises, and facial images can be captured from a distance without an individual's knowledge or consent.[111] Because biometric data contains unique personal information that generally cannot be changed, unauthorized access can cause irreparable harm to an individual; privacy experts consider biometrics to be sensitive, personally identifiable information

---

[107] "About Face ID Advanced Technology," Apple Support, accessed December 28, 2021, https://support.apple.com/en-us/HT208108; "Disney Uses Facial Recognition to Guard Its Magic Kingdom," *Biometric Technology Today* 2021, no. 4 (April 2021): 1–1, https://doi.org/10.1016/S0969-4765(21)00038-2; and Dave Gershgorn, "Retail Stores Are Packed with Unchecked Facial Recognition," The Verge, July 14, 2021, https://www.theverge.com/2021/7/14/22576236/retail-stores-facial-recognition-civil-rights-organizations-ban.

[108] Goodwin and Wright, *Facial Recognition Technology*, 9.

[109] North-Samardzic, "Biometric Technology and Ethics: Beyond Security Applications," 1.

[110] Meden et al., "Privacy-Enhancing Face Biometrics: A Comprehensive Survey," 4191.

[111] Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service," 9.

(PII).[112] The implementation of FRT must consider the risks and benefits associated with privacy and PII protection. DPIAC proposes the following equation as a risk assessment:

Integrity Benefit + Privacy Benefit > Risk to Integrity + Risk to Privacy.[113]

The Federal Government is required by regulation, law, and official policies to safeguard PII but is also required to give public notice of the collection, use, and retention of PII.[114] It is difficult for public sector agencies to mitigate privacy concerns because there are no universal policies or regulations governing biometric collection and FRT.[115] For decision-makers to address privacy concerns and protect data integrity, all vested parties must be informed about the utility of the collection and an agency's ability to safeguard the information. Use cases should be clear, and the public should be informed and possess the ability to consent.

2. Constitutional Protections

Freedom of speech, assembly, and movement are fundamental rights afforded to citizens by the United States Constitution. Civil Rights advocates assert that "facial recognition may have a chilling effect on our First Amendment rights to unabridged free speech and peaceful assembly" and the right to movement, which predates the Constitution.[116] Government use of technology must ensure that implementation does not infringe on inherent freedoms.

While this concern may apply to facial recognition in some circumstances, the blanket assertion about civil rights violations does not differentiate between overt and covert use cases, nor whether the public consents. Algorithms, authorities, policies, and public perception differ in overt and covert use cases. Nonetheless, decision-makers maintain the responsibility of protecting constitutional freedoms.

---

[112] Data Privacy and Integrity Advisory Committee, *Privacy Recommendations*.

[113] Data Privacy and Integrity Advisory Committee, 5.

[114] DHS Privacy Office, *Privacy Incident Handling Guidance*, 8.

[115] Carter, "Facing Reality," 64.

[116] Garvie and Moy, *America under Watch: Face Surveillance in the United States*.

The notion of consent is relevant when discussing public protections from emerging technology. Policy and decision-makers need to decide how one participates in data collection. An opt-in model requires a user to perform an affirmative action before data collection begins. Alternatively, an opt-out model collects data by default and requires the user to take an action to opt out of or otherwise bypass the data collection. Overt facial data collection may provide the user with the option to partake or not partake in the data collection. For example, users can provide a facial image (opt-in) as an identity verification means to access a bank account. TSA allows travelers to opt out of using FRT and show a physical form of identification instead. Covert FRT, more often than not, does not provide consent options. There is also voluntary and involuntary enrollment into facial recognition databases. Opt-in versus opt-out and voluntary versus involuntary enrollment options become a decision point for policy makers when collecting data.

3. Bias and Accuracy Rates

A third and significant risk raised regarding the ethical application of FRT is bias and misidentification. NIST refers to bias and misidentification as demographic differentials.[117] Critics often cite instances of erroneous matches and misidentifications to bolster this criticism. The most famous example is the ACLU test that used an off-the-shelf facial recognition tool matching 28 members of Congress (primarily members of color) to criminal mugshots.[118] There is also the prominent Detroit, Michigan case of Michael Oliver, a man of color who was falsely accused and charged with a crime he did not commit based on FRT.[119] While any miscarriage of justice deserves attention, data suggests critics often use misleading arguments.

A 2019 NIST report found that facial algorithms could differ in performance based on race or country of birth, sex, and age, but these differences varied by what kind of

[117] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST IR 8280 (Gaithersburg, MD: National Institute of Standards and Technology, 2019), https://doi.org/10.6028/NIST.IR.8280.

[118] Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots."

[119] Anderson, "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit."

matching was performed and the algorithm vendor.[120] A close look at the NIST data reveals that the best facial recognition algorithms "are highly accurate and have small differences in their rates of false-positive or false-negative readings across demographic groups."[121] Overall, the NIST study found that high-performing algorithmic matching is exceptionally accurate with negligible demographic differences.[122] The NIST findings are significant to decision-makers when determining the efficacy of algorithm vendors and mitigating any demographic differential concerns.

Another element that factors into the accuracy of FRT is algorithm fairness. Algorithm fairness refers to the "different contextual assumptions and optimizations for accuracy."[123] Probe or source photo quality, lighting, angles, facial obstructions, and other environmental factors impact accuracy. The degree of accuracy is contingent on environmental factors and conditions such as consistent lighting, positioning, and unobstructed facial features.[124] Rigorous reporting on the performance metrics, environmental factors, and an understanding of the algorithm are essential to a successful program.[125] Policy-, decision-, and law-makers should endorse the development, deployment, and responsible use of FRT by understanding algorithm performance.

4. Data Management and Accountability

Data accountability and protections are a final area of concern when dealing with FRT. Data protection can be considered part of the privacy implications, but this thesis treats data protection as an independent concern because mitigation is technical. Biometric

120 Grother, Ngan, and Hanaoka, *Face Recognition Vendor Test Part 3*.

121 Michael McLaughlin and Daniel Castro, *The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist* (Washington, DC: Information Technology and Innovation Foundation, 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

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

123 Buolamwini and Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."

124 Crumpler, "How Accurate Are Facial Recognition Systems and Why Does It Matter?"

125 Buolamwini and Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."

data has been identified as PII and therefore is subject to safeguarding and permissible usage. Biometric technologies collect massive amounts of data, but the limitations on data usage are inconsistent and often unclear.[126] Therefore, decision-makers must address and share with the public those policies governing data retention, storage, protection, sharing, and usage.

When evaluating data transmission, storage, sharing, and usage, it is important to focus on privacy, data encryption, and cyber-security best practices to safeguard biometric data. FRT systems should subscribe to limited collection principles and storage of encrypted digital image templates instead of original photos to reduce vulnerabilities.[127] Furthermore, FRT data security should incorporate appropriate safeguards and best practices to protect the security, privacy, confidentiality, and integrity of PII and prevent inappropriate disclosure.[128] Data protection is a key criterion for securing public trust.

D. CONCLUSION

As FRT becomes entrenched as a security measure in the public sector, its impact on society increases. Public trust and understanding become increasingly relevant to the acceptance of the technology. Furthermore, it is ever more important to understand how the public sector uses and implements FRT across different agencies. Decision-makers can incorporate ethical frameworks and standard operating principles into the development and deployment of FRT to ensure ethical, legal, and societal issues are addressed.

[126] Lewis and Crumpler, *Facial Recognition Technology*.

[127] Security Industry Association, *SIA Principles*.

[128] Data Privacy and Integrity Advisory Committee, *Privacy Recommendations*.

IV. ANALYSIS: IMPLEMENTING AN ETHICAL AND EFFICIENT FACIAL RECOGNITION PROGRAM

FRT is a powerful tool that presents advantages and challenges. Using FRT fills a security gap in the public sector but raises serious questions regarding civil rights and civil liberties. The public's concerns about the technology heighten the responsibilities of government agencies using the technology. Researchers assert that government agencies implementing emerging technology are responsible and accountable for that technology's ethical and societal implications and impacts.[129] Decision-makers developing and implementing FRT must balance the benefits against the effects on society. During the decision-making process, ethical frameworks incorporating questions addressing ethical, legal, and societal concerns provide a mechanism to identify ethical problems and challenges during the initial phases of technology development.[130] When decision-makers anticipate and identify issues before implementing emerging technology, they can mitigate them, improving public perception and fostering better adoption rates. With little regulation and standardized practices, adhering to ethical frameworks and operating principles guides decision-makers in the ethical implementation of FRT.

This research takes a multi-pronged approach to implementing an ethical and efficient FRT program and outlines principles for responsible usage. The following section of this chapter applies the "How to Do It Right" framework to the government's use of FRT to identify values and the subsequent vulnerabilities, risks, and mitigation measures. The vulnerabilities, risks, and mitigation measures adapted into the framework derive from the biometric literature and security industry practices. Following the "How to Do It Right" framework provides decision-makers with a guide to implementing an ethical and efficient FRT program. The next section categorizes and applies cross-cutting operational guidelines to the FRT technology to standardize operational criteria and mitigate the societal and ethical challenges of using biometrics. The operational guidelines are drawn

[129] North-Samardzic, "Biometric Technology and Ethics: Beyond Security Applications."

[130] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 162–65.

and compiled from operating principles published by security industry organizations. The third prong of this research, captured in Chapter V, explores best practices through a case study of CBP's BEE program. The goal is to identify and encourage best practices and standard operational guidelines for government decision-makers when developing, implementing, and operating FRT.

A. "HOW TO DO IT RIGHT" FRAMEWORK

Mohamed Abomhara et al. (2019) developed the "How to Do It Right" framework to analyze biometric technology in border settings. The framework is a layered approach that focuses on societal, ethical, and legal challenges arising from the use of biometrics. However, this thesis excludes legal issues from the analysis. Abomhara et al.'s framework identifies ethical and societal values impacted by technology and then identifies considerations to be used when assessing biometrics in a border security setting. The framework provides guidance for border officials to "do it right" when faced with challenges. It links the challenges to the value(s) affected by technology and allows an impact assessment to mitigate the values affected.[131] While Abomhara et al.'s framework focuses on border security biometrics, as does the BEE case study, the analysis in this thesis uses the framework to guide the decision-making process on facial biometrics from a broader law enforcement perspective. Setting ethical guidelines and using a regulatory framework when implementing biometrics technology allows decision and policy makers to avoid negative impacts on society while allowing the technology to benefit society.[132] The values and considerations included in the modified "How to Do It Right" framework are drawn from literature about FRT concerns, challenges, and criticisms and then applied to FRT.

1. The Framework Overview

As decision-makers in the government seek to implement FRT programs, the "How to Do It Right" framework allows them to ascertain ELSI before implementation and then

[131] Abomhara et al., "How to Do It Right," 99.

[132] Abomhara et al., 95.

apply specific considerations to advance the technology responsibly. The original framework devised by Abomhara et al. addresses biometric collection in a European Union border security setting. The framework is a tiered approach that begins with broad challenges (ethical, societal, and legal) that impact any emerging technology program. The top layer compels officials to scrutinize basic ethics, social issues, and legal concepts regarding biometrics, and brings a conscious awareness of these issues.[133] The next layer identifies values impacted by biometric collection at the border. The third layer provides a mechanism for officials to assess the risks, vulnerabilities, and mitigation measures. This tier asks the decision-maker what the consequences of biometrics are, what risks arise with technology implementation, and how the challenges can be mitigated.[134] The fourth and final tier outlines the considerations that officials can use to minimize the challenges. Figure 4 illustrates the original "How to Do It Right" framework. Overall, the framework provides a guide for decision-makers to think broadly about an issue, narrow the scope to focus on specific issues, and anticipate and lessen the impacts on the public.

[133] Abomhara et al., "How to Do It Right," 100.

[134] Abomhara et al., 101.

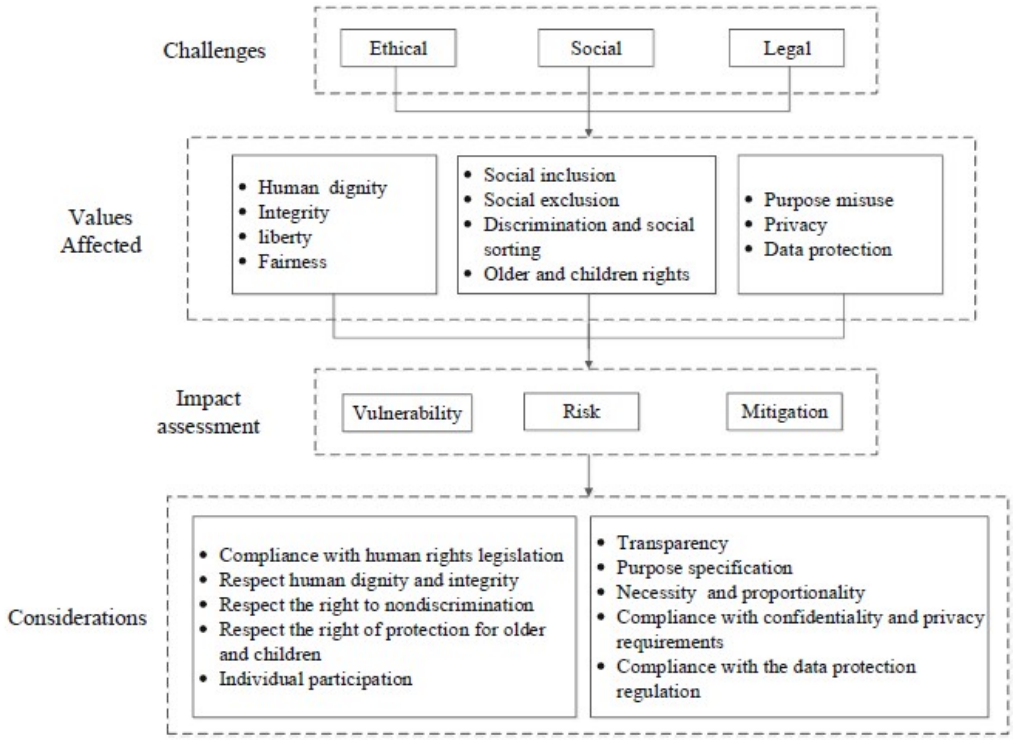

Figure 4. "How to Do It Right" Framework.[135]

2. Adapting the Framework

This thesis adapts the "How to Do It Right" framework and applies it to the U.S. government's use of FRT. Figure 5 illustrates the application of the "How to Do It Right" framework to the FRT program decision-making process. It takes the basic framework and incorporates the four overarching challenge categories derived from the literature and criticisms of FRT into the values tier: privacy implications, constitutional protections, data management, and bias and accuracy. Once decision-makers identify the issues within the four value categories, they can assess the risks, vulnerabilities, and mitigation measures. Finally, decision-makers promote ethical and efficient programs by developing and implementing safeguards corresponding to ethical operating guidelines presented in the considerations tier. The operational principles originate as ethical guidelines in the biometrics and security industry literature. This research explores the operational

[135] Source: Abomhara et al., "How to Do It Right."

principles in the next section's crosswalk. The adapted framework allows decision-makers to consider the broad implications of FRT and then extrapolate best practices that can mitigate the challenges and establish responsible biometric collection and usage. Government decision-makers can formulate decisions regarding FRT by thinking through the ethical framework before, during, and after technology implementation.

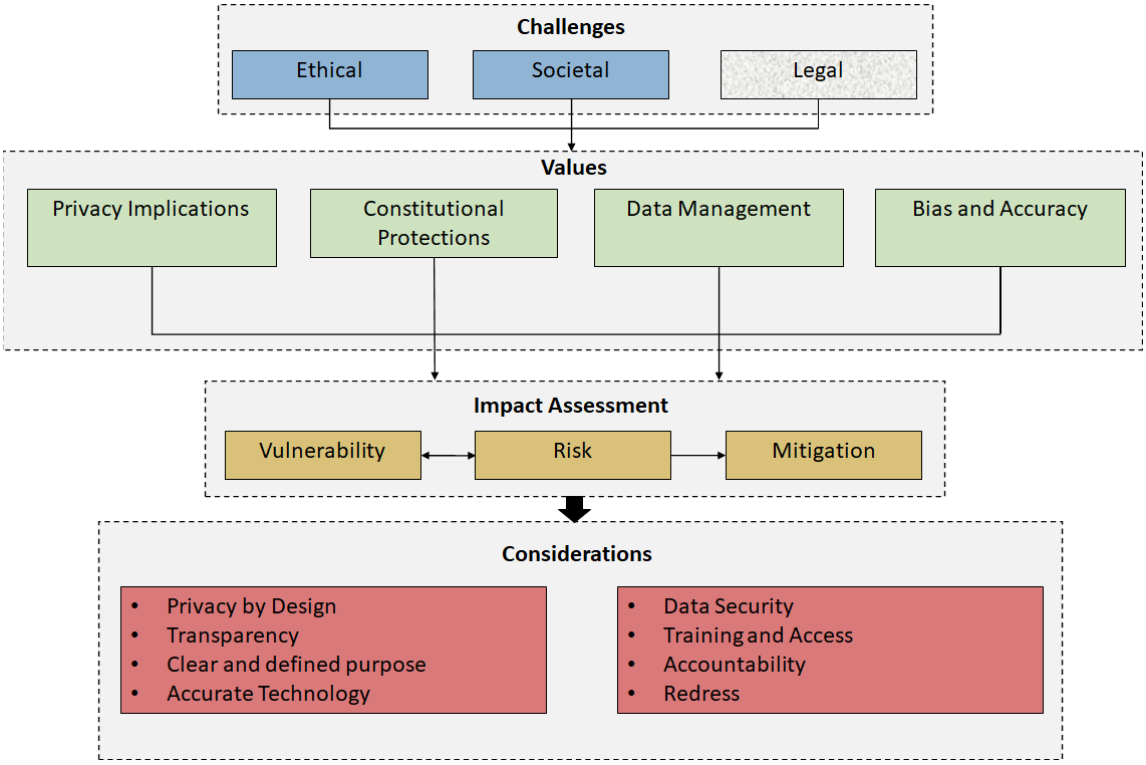

Figure 5. The "How to Do It Right" Framework Applied to FRT.[136]

B. OPERATIONAL GUIDELINES

Security industry organizations and watchdog groups have developed ethical principles, referred to in this document as operational guidelines, to govern the use of facial

[136] Adapted from: Abomhara et al.

biometrics.[137] Each organization has proposed different guidelines with many common elements, but no accepted standardized principles exist. The values and considerations identified by decision-makers using the "How to Do It Right" framework translate into ethical principles, operational standards, or best practices. Table 1 outlines operational guidelines from five prominent security industry organizations and watchdog groups. The goal is to compare and adopt the most common principles into standardized operational practices that promote responsible FRT usage.

Table 1. Crosswalk of Operational Guidelines.[138]

	Security Industry Association	International Biometrics and Identity Association	Future of Privacy Forum	Center for Strategic and International Studies	World Economic Forum
1.	Transparency	Openness	Transparency	Transparency	Transparency
2.	Clear and Defined Purpose	Purpose Specification	Context	Permissible Use	Necessary and proportional
3.	Accurate Technology	Data Quality		Algorithmic Review	System Performance
4.	Human Oversight			Autonomous Use	Human Oversight
5.	Non-Discrimination				Respect for Human Rights
6.	Data Security	Security Safeguards	Data Security	Data Retention	Data Integrity
7.	Privacy by Design	Collection Limits	Privacy by Design		

[137] As seen in the following literature: Security Industry Association, *SIA Principles*; International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles* (Washington, DC: International Biometrics and Identification Society, 2021), https://www.ibia.org/resources/white-papers; Future of Privacy Forum, *Summary of Privacy Principles*; Lewis and Crumpler, *Facial Recognition Technology*; and, World Economic Forum, *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations* (Geneva, Switzerland: World Economic Forum, 2021), https://www.weforum.org/whitepapers/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations..

[138] This crosswalk was compiled with data from the following sources: Security Industry Association, *SIA Principles*; International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles*; Future of Privacy Forum, *Summary of Privacy Principles*; Lewis and Crumpler, *Facial Recognition Technology*; and, World Economic Forum, *A Policy Framework for Responsible Limits on Facial Recognition*.

	Security Industry Association	International Biometrics and Identity Association	Future of Privacy Forum	Center for Strategic and International Studies	World Economic Forum
8.	Training and Education	User Access Limitations	Integrity and Access	Training	Training
9.	Ethical Acquisition				Lawful Usage
10.	Targeted Public Policy				Risk Mitigation
11.		Accountability	Accountability	Oversight and Auditing	Accountability
12.		Redress		Redress	
13.			Consent	Consent	

The five organizations delineate principles that are crucial to responsible biometric collection. Other groups have published principles, such as the Biometric Institute, EFF, and DPIAC. Regardless of the organization, the principles are designed to guide FRT's ethical and efficient use. These groups were not highlighted in the crosswalk because the ethical principles are similar or the same as the included principles.

The crosswalk reveals common themes that can be extracted and generalized into standardized practices within FRT programs. The "How to Do It Right" framework incorporates these common themes as considerations or mitigation measures. Once a common principle is established as an operating guideline, it can be characterized into operating practice. The common themes extracted from the crosswalk are privacy by design, transparency, clear and defined purpose, accurate technology, data security, training and access, and accountability. It is up to each agency to do its due diligence and implement as many ethical principles as possible to balance the security benefits and the public impact. Applying these principles and operating guidelines leads to the responsible use of FRT. The principles and potential implementation methods are outlined below.

1. Privacy by Design

Privacy by design is a concept that aims to embed privacy principles and concepts into technology development. Privacy by design aligns with privacy and data management values identified in the ethical framework process and serves as one of the mitigating considerations. There is a burgeoning understanding that innovation and creativity must be approached from a "design-thinking" perspective.[139] Privacy should be approached the same way. The privacy-by-design methodology demands that privacy is incorporated into technologies during the development by default. Furthermore, ethical technology usage prevails when privacy principles become fundamental to organizational priorities, objectives, and planning operations.[140] Privacy is one of the underlying foundations for each of the following operating principles.

2. Transparency

In the United States, the Privacy Act of 1974 classifies transparency as a Fair Information Practice Principle (FIPP). Transparency aligns with the privacy implication values identified in the ethical framework. While most private sector entities provide privacy policies, they are written with intentionally vague language, fail to define terms and exclude specific language about usage and collection.[141] To mitigate the risk and vulnerabilities associated with FRT, the government cannot be ambiguous in its privacy policies. Public notification of biometric data collection, use, dissemination, and maintenance of PII leads to public awareness, understanding, and acceptance.[142] At a minimum, government agencies using FRT can inform the public of the following: clear definition of use and objectives, algorithm vendor, the reference database used, data-

139 Atheer Aljeraisy et al., "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective," *ACM Computing Surveys* 54, no. 5 (2022): 1–38, EBSCOhost.

140 Aljeraisy et al.

141 Elizabeth McClellan, "Facial Recognition Technology: Balancing the Benefits and Concerns," *Journal of Business & Technology Law* 15, no. 2 (2020): 377, Ebscohost.

142 Department of Homeland Security, "The Fair Information Practice Principles," Department of Homeland Security, May 26, 2022, https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

sharing, retention periods, data security measures, and available redress. Informing the public leads to understanding and a better likelihood of acceptance and adoption.

3. Clear and Defined Purpose

A clear and defined purpose intersects with transparency but is a category by itself. In biometrics, a clear and defined purpose outlines the specific cases when and where the technology may be used to prevent misuse and protect civil rights and civil liberties. This principle aligns with privacy and constitutional protection values in the ethical framework. The balance between deploying the latest technologies, safeguarding society against security threats, and protecting human rights guides the development of ethical and efficient FRT systems.[143] Government agencies can establish clearly articulated use cases and the legal authorities to operate the technology in the given use case. Generally, FRT should never be used without a security or law enforcement need. Government agencies that understand the capabilities and constraints of the technology are better suited to select the technology most appropriate for the defined purpose.[144] Agencies are also better suited to identify the legal authorities to operate such programs. When regulations are lacking, ethical principles formulate behavior and work to ensure the ethical application of the technology that aligns with constitutional protections.

4. Accurate Technology

Government agencies that endeavor to develop or procure high-performing FRT solutions encounter more accurate and efficient FRT results. Performance can be validated through sound scientific methods offered by NIST or similar groups and by continuous metric and algorithmic review. The government should be prepared to upgrade algorithms, systems, and equipment as technology improves.[145] The capability to accurately identify or verify an individual and eliminate an imposter is key to filling a security gap and is one

[143] Hodge Jr., "The Legal and Ethical Considerations of FRT," 763.

[144] Security Industry Association, *SIA Principles*.

[145] World Economic Forum, *A Policy Framework for Responsible Limits on Facial Recognition*, 17.

of the most prominent benefits of FRT.[146] Additionally, there may be instances when government agencies need to set up review boards or teams to verify and validate facial matches, especially in sensitive law enforcement situations. Due diligence in utilizing a high-performing algorithm ensures minimal demographic differentials and misidentification. Accurate technology protects the public and mitigates the bias value found in the framework.

5. Data Security

The management and security of biometric data is also classified as a FIPP. Data security aligns with the data management challenge. According to the Department of Homeland Security (DHS), government agencies must ensure that "security controls are put in place in technology systems that are commensurate with the sensitivity of the information they hold."[147] Biometric data is sensitive PII and must be secured accordingly.[148] There are a variety of cyber-security measures the government can take to protect biometric data. Simultaneously, following "a distributed data approach by limiting biometric data stored in central repositories and storing the data in the form of encrypted templates rather than images" promotes data security and harm reduction.[149] Data minimization is a key component of data security and management. FRT systems should not collect any more data than necessary to achieve the prescribed goal.[150] Policy and applicable rules and regulations govern biometric data retention. Overall, the government is responsible for securing and safeguarding biometric data. Therefore, implementing cyber-security and other data protection measures to protect PII is imperative in ethical and accountable biometric programs.

---

[146] Abomhara et al., "How to Do It Right," 3.

[147] Department of Homeland Security, "The Fair Information Practice Principles."

[148] DHS Privacy Office, *Privacy Incident Handling Guidance*, 51.

[149] Security Industry Association, *SIA Principles*.

[150] International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles*.

6. Training and Access

Training and access are broad categories that apply to developers, users, administrators, and other interested parties. These categories relate to the data management values identified through the ethical framework. Government organizations can train system users and anyone who interfaces with the FRT system on the appropriate use of the technology. Developers, system designers, and users working together to develop and provide training to FRT operators promulgate effective and responsible technology use.[151] Facial match adjudicators, along with those who develop algorithms, maintain systems, configure the thresholds require more in-depth training. Some algorithms use machine learning, which involves training on large data sets to ensure accuracy. It is crucial to ensure that training data is diverse and collected with consent to avoid bias. Decision-makers should ensure the algorithms selected are trained and tested on large, diverse data sets.

Not only should training be provided, but access should be limited. Physical and digital access control measures limit data access to trained and authorized personnel.[152] Finally, organizations that restrict and monitor data flow tend to avoid data breaches.[153] Building training programs for developers, technology, managers, and users works together with access controls to govern access and usage, leading to data protection.

7. Accountability

All government programs are subject to oversight and accountability. Until federal laws are enacted to regulate FRT, government agencies abiding by operational guidelines cultivate a culture of accountability and responsible data collection, usage, and retention. Promoting accountability through voluntary actions and disclosures paves the way for FRT's ethical and efficient use.[154] FRT system analysis, audits, and review by NIST or

---

[151] Security Industry Association, *SIA Principles*.

[152] International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles*.

[153] DHS Privacy Office, *Privacy Incident Handling Guidance*.

[154] International Biometrics and Identification Society, *Identification Technology & Privacy Policy Principles*.

GAO demonstrates accountability. Internal audits also contribute to accountability. Reviewing and auditing internal processes and metrics provides insight into system performance and accuracy. Government agencies can publish annual reports on FRT accuracy and other performance measures when applicable. Although different use cases and government agencies will need different audit and reporting measures, incorporating accountability into all FRT programs exhibits transparency and responsibility to the public.

8. Other Considerations and Implementation

A government agency puts itself on the path to ethical and efficient use of FRT by utilizing an ethical framework during decision-making and incorporating the seven operational practices as mitigation measures. There are other principles that government agencies can contemplate to further ethical usage. These principles include redress and consent. The use of FRT can have severe implications for society, especially in the case of misidentification. Redress programs provide a mechanism to remedy misidentification or inaccurate information in government systems. Consent to data collection is an option in some use cases, but not all. For example, airport travelers can opt out of facial recognition at security checkpoints and boarding gates, but a suspect cannot opt out of facial recognition during a police investigation. Agency-specific use cases (e.g., surveillance, identity, and victim identification) dictate the mode in and extent to which the seven principles are incorporated into a program, but all seven principles are important to responsible technology use.

Security industry organizations and watchdog groups propose ethical principles in some form, but there is no standardization. When comparing the five group's principles, patterns emerge, creating common principles that evolve into standardized and best practices for government agencies using FRT to address societal and ethical challenges. Government agencies following an ethical decision-making process incorporate ethical operating principles as measures to manage and mitigate challenges presented by FRT technology.

V. THE CASE STUDY: CBP'S BIOMETRIC ENTRY-EXIT PROGRAM

After the events of 9/11, DHS was mandated, through a series of rules, regulations, and executive orders to develop a comprehensive entry and exit program that verifies the identity of travelers entering and departing the United States using biometrics rather than biographic information.[155] Before the mandate, DHS used biographic information for identification. DHS struggled to develop an effective and cost-efficient biometric entry and exit system that fulfilled the congressional mandate for over ten years.[156] In 2013, Congress transferred the biometric entry and exit mandate to CBP. Since that time, CBP has worked to implement an ethical and efficient facial recognition program. CBP's BEE program exemplifies an FRT program that has carefully thought through challenges, considered the impact on public values, and made efforts to lessen the impact on society. This chapter provides an overview of the BEE program (including the history of the Traveler Verification Service (TVS) program), outlines current program status, and analyzes the program's incorporation of the ethical operating considerations identified in the "How to Do It Right" framework.

A. HISTORY OF BEE

Because CBP encounters over one million travelers daily, the agency requires an efficient yet secure biometric solution.[157] With the assistance of the DHS Science and Technology Directorate (DHS S&T), CBP explored a range of biometric capabilities, including fingerprinting, iris scans, and facial recognition technology, conducted biometric trials in several environments, and reviewed more than 150 biometric devices

[155] U.S. Customs and Border Protection, "Collection of Biometric Data from Aliens Upon Entry to and Departure From the United States," No. USCBP–2020–0062 (Federal Register Notice Vol. 85, No. 224 November 19, 2020).

[156] Marcy Mason, "Biometric Breakthrough: How CBP Is Meeting Its Mandate and Keeping America Safe," *Frontline*, December 8, 2018, https://www.cbp.gov/frontline/cbp-biometric-testing.

[157] "About CBP," Customs and Border Protection, February 24, 2022, https://www.cbp.gov/about.

and algorithms before establishing a finalized version of the agency's BEE.[158] In the end, FRT emerged as a safe and efficient method to verify identity in a security setting for CBP.[159] It took some time, but FRT became the primary method of identity verification. Figure 6 outlines the timeline leading up to the implementation of BEE, from the underlying regulations to initial implementation.

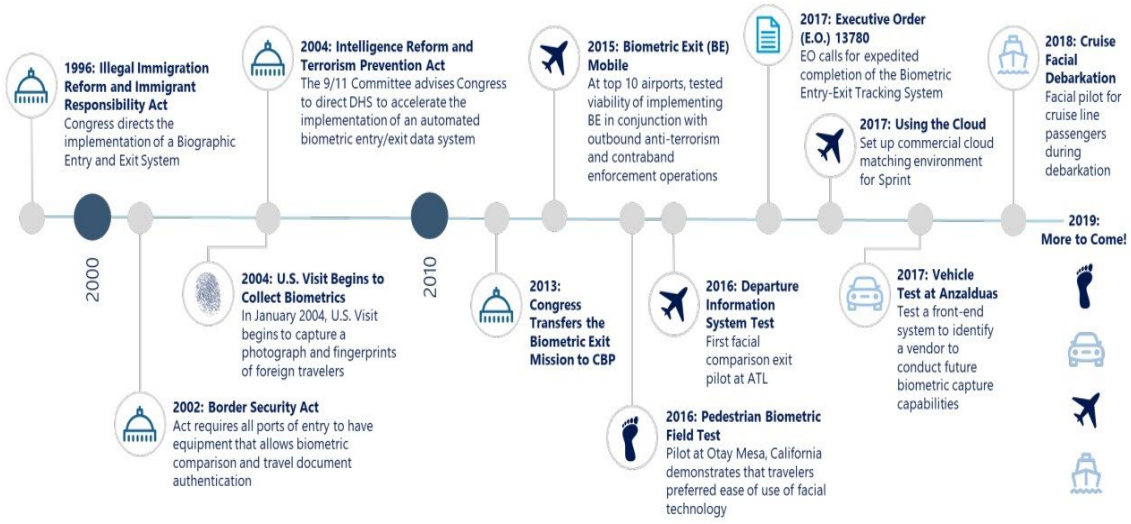

Figure 6. Timeline: How CBP Changed the Face of Travel.[160]

The use of biometric indicators was not new to CBP. In 2004, CBP began collecting fingerprints and photographs of non-United States citizens upon entry into the United States. With this collection, the U.S. started to build a biometric repository of non-criminal entities.[161] The biometric repository became crucial to developing and applying facial biometrics for identity verification at border crossings. Until BEE was realized, manual

158 "Examining the Department of Homeland Security's Use of Facial Recognition and Other Technologies, Part II," House of Reps, 116th Congress, Second Session, February 6, 2020; and Marcy Mason, "Biometric Breakthrough: How CBP Is Meeting Its Mandate and Keeping America Safe," *Frontline*, December 8, 2018, https://www.cbp.gov/frontline/cbp-biometric-testing.

159 "CBP Biometrics."

160 Source: Larry Panetta, "Simplified Arrival: A Stakeholder Overview" (Presentation, Port of Seattle, 2020), https://www.portseattle.org/sites/default/files/2020-08/Simplified_Arrival_Overview_CBP_Field_Ops_presentation.pdf.

161 Department of Homeland Security, "Biometrics."

identification checks were the primary source of identity verification for all legitimate travel and purposes not related to law enforcement.

At the outset of the development of a comprehensive biometric system, CBP established five principles that were necessary for a comprehensive solution to be feasible and realistic: "avoid adding any new processes, utilize existing infrastructure, leverage existing stakeholder systems and business models, leverage traveler behavior and expectations, and use existing traveler data and technology infrastructure within CBP."[162] According to CBP, the technology aspect was only part of the problem. The more significant challenge was incorporating the technology into existing infrastructure at airports and other ports of entry without costly construction and negative operational impacts.[163] Working within the five principles, CBP determined that "facial recognition technology is currently the best available method for biometric verification, as it is accurate, unobtrusive, and efficient."[164] To get to this point, the agency conducted numerous tests and met with travel and security industry representatives, technology experts, and privacy advocates.

In 2014, the agency set up a Maryland lab to enable controlled biometric technology testing. According to Arun Vermy of DHS S&T, CBP assessed over 150 different biometric devices and algorithms to determine the best approach to biometric capture and the most efficient and accurate technology.[165] CBP used the results of the DHS S&T testing to run biometric collection tests in operational environments. In June 2016, CBP launched a biometric system pilot, the Departure Information System Test, at the Atlanta Hartsfield International Airport (ATL) to "assess whether facial comparison technology could confirm a traveler's exit from the United States."[166] During the summer of 2017,

[162] Electronic Privacy Information Center, "EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures)."

[163] Mason, "Biometric Breakthrough."

[164] Customs and Border Protection, "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States."

[165] Mason, "Biometric Breakthrough."

[166] Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service," 2.

CBP continued technical demonstrations of the technology at ATL, Boston Logan International Airport, and the John F. Kennedy International Airport. These pilots and technical demonstrations led to the development of TVS and evolved into the current BEE program.

B. THE TRAVELER VERIFICATION SERVICE

CBP developed the TVS as the matching backbone for all biometric operations. TVS uses "existing advance passenger information along with photographs which have already been provided by travelers to the government to create 'galleries' of facial image templates to correspond with who is expected to be arriving or departing the United States on a particular flight, voyage, etc."[167] The government sources the photographs from prior interactions at the border and passport or visa applications. Once a photo gallery is created from advanced passenger information, the FRT compares a template probe or live traveler photos to the gallery of facial image templates.[168] The live probe photo is captured either by a CBP officer upon arrival at an airport or a pedestrian land border lane or by an airline official upon departure at an airport. A facial match indicates the identity has been verified.

If a gallery source photo cannot be found or matched, CBP utilizes a 1:1 matching process. In this instance, the live image will be compared to the document photo that was retrieved either through the e-chip in the document or by using the biographical information on the passport to locate a photo in DHS holdings. In locations where manifest information is unavailable, such as the land border, CBP uses TVS to conduct a 1:1 verification of a live photograph and a document photograph to determine identity and document authenticity.[169] Currently, CBP does not use FRT on passengers arriving or departing at a land border, afoot, or in a vehicle.

[167] Customs and Border Protection, "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States."

[168] U.S Congress. House, "Examining the Department of Homeland Security's Use of Facial Recognition and Other Technologies, Part II."

[169] Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service."

The process begins with a live photo capture of a traveler entering or departing the United States. CBP parameters and criteria determine whether to conduct a 1:1 or a 1:N match. The live photos are either compared to a flight-specific photo gallery created with manifest data and DHS source photos or to a document photo accessed through an e-chip or biographic data. The process concludes with a match result. Figure 7 illustrates the CBP matching process in detail.

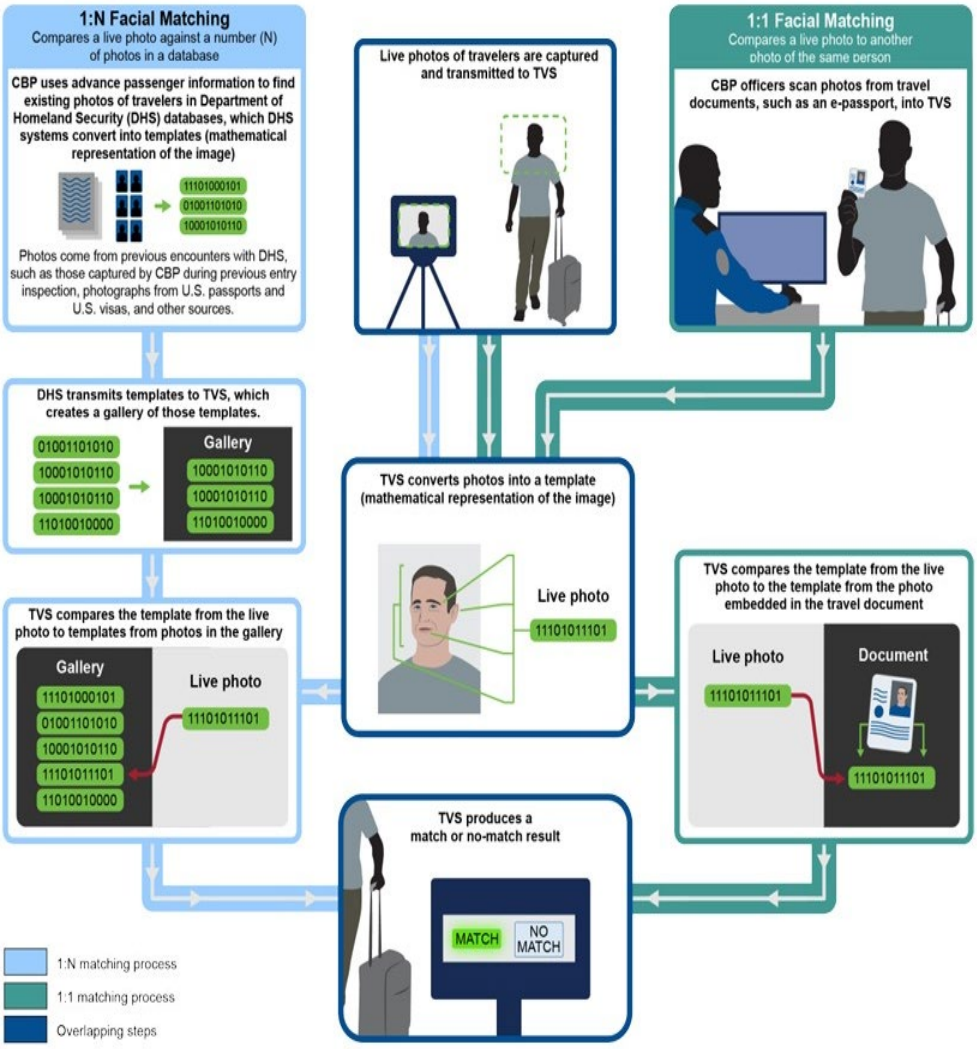

Figure 7. Process Flow of 1:N and 1:1 Facial Matching.[170]

[170] Source: Gambler, *Facial Recognition: CBP and TSA Are Taking Steps*.

C. BIOMETRIC COLLECTION IN LAND BORDER VEHICLE LANES

CBP has adopted facial biometrics to verify identity at seaports, airports, and pedestrian lanes at land border ports of entry but has been unsuccessful in implementing the technology in land border vehicle lanes. The agency has conducted multiple pilots and technology demonstrations to tackle this challenge to no avail. In 2018, the agency conducted its first test on travelers entering the United States by vehicle at Anzalduas, Texas. The Anzalduas Biometric Test collected face biometrics voluntarily from travelers entering or departing the United States in moving cars. The test was designed to determine and evaluate the FRT's effectiveness in capturing a quality facial image for vehicle occupants, analysis of the match rates, and evaluate transaction time for matching the images.[171] The test was conducted in the background of normal traveler processing, in that matching results were not shared with the CBP officers processing the passengers. A contract technical team analyzed the matching results. CBP then analyzed those results.

Figure 8 outlines the biometric test process flow. The process begins when a vehicle approaches an entry booth. Cameras will capture driver and passenger photos and the license plate with a License Plate Reader (LPR). The facial images are separated from the arrival process, sent to the vendor for quality analysis, and then forwarded to TVS for matching. The biometric process occurred outside and separate from traditional vehicle and passenger processing for test purposes.

171 "Test to Collect Facial Images from Occupants in Moving Vehicles at the Anzalduas Port of Entry (Anzalduas Biometric Test)," *Federal Register Notice* 83, no. 220 (November 14, 2018): 56862–64, https://www.govinfo.gov/content/pkg/FR-2018-11-14/pdf/2018-24850.pdf.

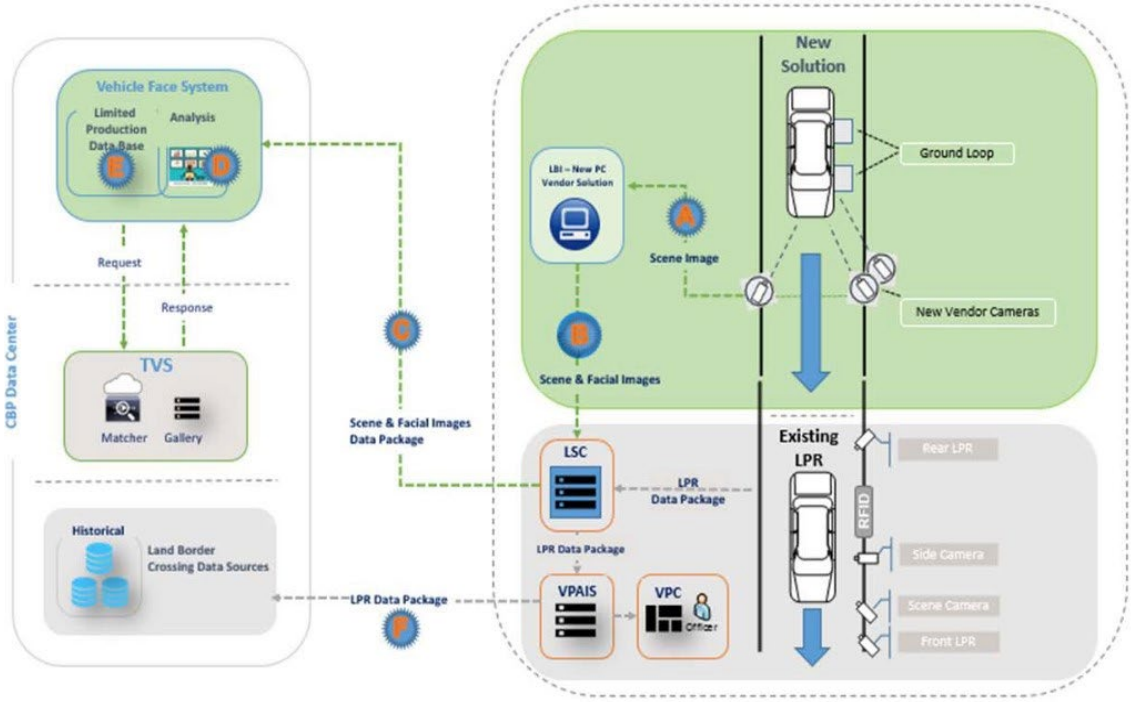

Figure 8. The Anzalduas Biometric Test Process Flow.[172]

The accuracy and quality of the photo capture results are unclear. CBP did not publish the results because the subcontractor violated CBP's data protection provisions by transferring copies of biometric data, such as traveler images, to its company network, prompting an investigation.[173] The data breach did not deter CBP, and they reimagined the vehicle test in 2019.

In 2019, CBP relaunched a biometric pilot in the vehicle lanes at Anzalduas, Texas. CBP declared the "enhanced process for international travel…uses facial biometrics to automate the manual document checks that are already required for admission into the

[172] Source: Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service," 34.

[173] Office of Inspector General, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot*, OIG-20-71 (Washington, DC: Department of Homeland Security, 2020), 3, https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

United States and provides travelers with a secure, touchless travel experience."[174] The new pilot captures face biometrics of travelers approaching two vehicle lanes at the Anzalduas Port of Entry. The camera attempted to photograph the vehicle's occupants and match the photo to its corresponding travel document photos in government holdings. CBP provides an opt-out lane for travelers who do not choose to participate in biometric testing.[175] The second biometric test concluded in February 2022, but the results were not public at the time of the thesis research. CBP continues to partner with DHS to explore options. The 2022 DHS S&T Biometric Rally focused on unattended high throughput scenarios and group processing, requiring the biometric capture solution to rapidly secure biometric images from multiple individuals simultaneously. The biometric rally can extrapolate the results into high throughput vehicles. CBP continues to explore options for biometric capture in the vehicle lanes.

D. CURRENT STATUS

CBP has institutionalized FRT as the primary identity verification tool through the BEE program. CBP deployed 1:N matching at all 238 international airports within the United States, 14 Preclearance locations abroad, and 26 seaport locations.[176] 1:N FRT has also been implemented through a partnership with airports and airlines to verify biometrically individuals departing the United States at 32 locations. CBP partnered with the Transportation Security Administration (TSA) to provide ATL and the Detroit Metropolitan Wayne County Airport with biometric capabilities. A 1:1 process has been deployed at all pedestrian crossings on the Southwest and Northern borders. CBP is currently exploring FRT in vehicle environments.

[174] "CBP Announces Facial Biometric Pilot for Inbound Vehicle Travelers at Anzalduas International Bridge | U.S. Customs and Border Protection," National Media Release, September 20, 2021, https://www.cbp.gov/newsroom/national-media-release/cbp-announces-facial-biometric-pilot-inbound-vehicle-travelers.

[175] Customs and Border Protection, "CBP Biometrics."

[176] Customs and Border Protection.

E. THE CASE STUDY: AN ETHICAL AND EFFICIENT IMPLEMENTATION OF FRT

CBP's BEE is representative of an efficient and ethical FRT program. CBP has embraced the use of FRT at U.S. international borders and supported efforts by TSA and the travel industry to incorporate FRT throughout the travel continuum. CBP's BEE was selected as a case study because the program includes FRT in a border security environment and incorporates ethical operating principles. GAO and OIG have audited the program individually and as a part of the widespread government use of FRT. Additionally, NIST, DPIAC, and DHS S&T audited CBP's algorithms. Although CBP continually improves and enhances the program, it exemplifies an agency that thoughtfully implemented a program through testing, pivoting approaches, internalizing audit recommendations, and overall due diligence.

When the comprehensive biometric entry-exit mandate was transferred to CBP, the agency tackled the challenge through extensive technology testing and establishing at the onset the five criteria ("avoid adding any new processes, utilize existing infrastructure, leverage existing stakeholder systems and business models, leverage traveler behavior and expectations, and use existing traveler data and technology infrastructure") under which to operate to achieve an effective and efficient solution.[177] CBP implemented BEE before the proposal of the "How to Do It Right" framework, but the agency regardless followed a path similar to the framework and has established best practices that align with the operational guidelines outlined in the framework. While the five criteria established by CBP do not correlate precisely to the seven ethical operational guidelines derived from the "How to Do It Right" framework, they are reminiscent of the guidelines and led CBP to a privacy-by-design approach. In turn, FRT program best practices and ethical operating principles can be observed throughout CBP's BEE.

CBP employed due diligence in developing an FRT program. The agency deployed FRT in an iterative manner that integrates audit recommendations. This section will

[177] Electronic Privacy Information Center, "EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures)."

provide an overview of the oversight audits and their recommendations and identify best practices employed by the agency within the seven operational principles.

1. The Audit Process

Generally, CBP is subject to numerous audits and reviews by GAO, OIG, and Congress on all things border related. CBP underwent GAO and OIG audits and a DPIAC privacy review regarding biometrics and the BEE. This section reviews three BEE-focused audits and the recommendations stemming from the reports. At times the audits were critical of CBP's operations but typically made general observations and recognized the beneficial elements of the program. CBP used the recommendations to enhance, update, and modify the program demonstrating a continual evaluation of the program to maintain ethical and efficient operations. An overview of the audit recommendations and CBP's response exemplifies how an agency can collaborate and improve procedures to satisfy the public and ensure security.

a. GAO Audit: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues

The GAO audit was published in September 2020 after the CBP BEE program was operational and expanding to additional locations. The report addressed "the status of CBP's deployment of FRT, the extent to which CBP has incorporated privacy protection principles, the extent to which CBP has assessed the accuracy and performance of its FRT, and the status of TSA's testing and deployment of FRT."[178] GAO visited air, land, and sea ports of entry, reviewed program documents, and spoke with DHS officials to complete the audit. According to the GAO, although the observations ascertained by the site visits "are not generalizable to all locations testing or using facial recognition technology, the observations provide useful insights about the status of testing and deployment, how privacy protections were implemented at these locations, and the accuracy of facial

178 Gambler, *Facial Recognition: CBP and TSA Are Taking Steps*, 1.

matching."[179] Based on the observations, the GAO issued five recommendations for improvement. The five recommendations include the following:

1. CBP should ensure that the BEE privacy signage and other public notices contain current and accurate information. The notifications should also include locations where facial recognition operates and an opt-out process explanation.
2. CBP should ensure that the BEE privacy signage is available and visible when using FRT.
3. CBP should conduct privacy audits of vendors, commercial partners, and other parties, assessing the use of PII.
4. CBP should implement a plan to confirm that the biometric capabilities meet the established photo capture requirement in the operational requirements document.
5. CBP should create an alert system that notifies officials when facial recognition performance drops below established thresholds.[180]

CBP concurred with the GAO recommendations and submitted an action plan to address the issues. CBP disputed recommendation five by asserting that the program has a "suite of tools for system and operational performance management" and requested recommendation closure.[181] Furthermore, CBP stated that in addition to ensuring the accuracy of the FRT systems, CBP remains committed to sustaining privacy protections.[182] In July 2022, GAO made a statement regarding the audit results before the Subcommittee on Border Security, Facilitation, and Operations, Committee on Homeland Security, House of Representatives. GAO testified that CBP's BEE incorporated privacy protection principles consistent with FIPPs, met its accuracy requirements during

179 Gambler, 6.

180 Gambler, *Facial Recognition: CBP and TSA Are Taking Steps*, 72–73.

181 Gambler, 73.

182 Gambler, 89.

operational testing, and the agency enlisted NIST to assess whether there were differences in the accuracy of TVS based on traveler demographics.[183] Overall, CBP accepted and sought to remedy recommendations made by GAO.

b. OIG Audit: CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports

DHS OIG conducted this audit on July 5, 2022. OIG conducted the audit to "determine whether CBP complied with its policies and procedures when resolving facial biometric discrepancies" found during usage.[184] Essentially the audit examined system accuracy and CBP's process to resolve differences. The auditors analyzed 51.1 million traveler encounters between May 2019 and September 2021. They determined that CBP complied with its policies and procedures to resolve misidentification and inaccurate information.[185] The audit made no recommendations to the agency regarding accuracy and usage, demonstrating that CBP has instituted accountability measures and data management.

c. Report 2019–01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology

DPIAC conducted this audit at the behest of the DHS Chief Privacy Officer (CPO). The CPO requested guidance on best practices for CBP's use of FRT for identification purposes. The advisory committee sought to answer whether CBP provides adequate and meaningful notice about biometric collection, the reliability of matches and usability of photos, whether there are sufficient measures to reduce bias, and how CBP can leverage private industry to facilitate biometric collection.[186] DPAIC met with DHS officials to provide a thorough assessment, attended public briefings on BEE, met with the Center on

---

[183] Rebecca Gambler, *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*, GAO22106154 (Washington, DC: Government Accountability Office, 2022), https://www.gao.gov/assets/gao-22-106154.pdf.

[184] Office of Inspector General, *CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports*, 1.

[185] Office of Inspector General.

[186] Data Privacy and Integrity Advisory Committee, *Privacy Recommendations*, 2.

Privacy and Technology at Georgetown Law, reviewed documents, and conducted site visits.[187] DPIAC looked at CBP's program through four perspectives on facial recognition: "transparency, data minimization, data quality and integrity, and accountability & auditing."[188] The four perspectives align with the seven operational guidelines included in the "How to Do It Right" considerations tier.

DPIAC made several recommendations to CBP:

1. Institute public notification that is readable and effective by accommodating different learning levels and languages.
2. Partner with NIST to leverage existing standards and practices, address new or nuanced FRT challenges, and create new industry standards.
3. DHS should research the efficacy and degradation of images over time.
4. CBP should only retain and use PII necessary to deliver its legally mandated obligations.
5. DHS should aggregate metrics and performance reports into a single annual report that is releasable to the public.
6. Provide transparency around the accuracy of the biometric system.
7. Develop guidelines governing data use and retention and establish appropriate prohibitions on usage beyond the stated purposes.
8. Work with S&T, NIST, and other research organizations to identify the most accurate algorithm and maintain technical standards.
9. Continue to work with DHS components and the travel and security industry to explore new technologies.[189]

DPIAC believes using FRT to screen travelers is a "technology that enhances the overall security of the U.S., speeds up screening processes, and may identify security

[187] Data Privacy and Integrity Advisory Committee, *Privacy Recommendations,* 3.

[188] Data Privacy and Integrity Advisory Committee, 4.

[189] Data Privacy and Integrity Advisory Committee.

risks."[190] The committee further believes "the introduction of biometric screening technology should continue to be open and transparent, focus on mitigating privacy concerns, be operationally sound from an efficacy and screening perspective, and ensure data integrity."[191] DPIAC provided extensive recommendations to CBP but failed to address countermeasures already in place. The recommendations, albeit useful, were generalized, high-level recommendations that apply to any FRT. CBP opted to adopt a robust public notification campaign and conduct regular audits on signage.

2. Best Practices and the Operational Guidelines

CBP aims to enhance security through innovation, intelligence gathering, partnerships, and trust.[192] The agency encounters close to half a million individuals a day.[193] Identity establishment is integral to border security, and CBP uses FRT as the primary mechanism to verify identity. CBP requires an efficient and effective system that operates ethically and responsibly. The following section depicts best practices within the seven operational principles found in the adapted "How to Do It Right" framework.

a. Privacy by Design

As biometrics become widely used by the government, governments must address and balance the impacts of information systems and privacy protections. A privacy-by-design approach defaults privacy assurances into operations. CBP approached the BEE in this manner. CBP accomplished this approach by embedding a privacy officer and principles into the planning and decision-making process.[194] The agency states, "we're committed to the privacy of all travelers, which has been at the core of our entry-exit efforts from the very beginning…we have built in the privacy and security safeguards and conduct

---

[190] Data Privacy and Integrity Advisory Committee, *Privacy Recommendations,* 12.

[191] Data Privacy and Integrity Advisory Committee, 12.

[192] "About CBP," Customs and Border Protection, accessed October 22, 2022, https://www.cbp.gov/about.

[193] "About CBP."

[194] Department of Homeland Security, *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies* (Washington, DC: Department of Homeland Security, 2019), 20, https://www.tsa.gov/sites/default/files/biometricsreport.pdf.

regular audits and penetration testing to ensure that compliance and privacy impact assessments are available publicly."[195] Privacy by design encompasses the other six operational guidelines, so by embracing this approach, CBP protects data, promotes constitutional protections, ensures data accuracy, and fosters transparency.

b. Transparency

According to a CBP Privacy Evaluation Report, the BEE program is aggressively transparent in its purpose and intent.[196] The agency has published privacy compliance documentation for all programmatic changes. The agency has published thirteen Privacy Threshold Assessments and six Privacy Impact Assessments.[197] CBP asserts that the BEE program is out in the open with cameras and signage visible in common areas where all travelers can see them and stay informed.[198] CBP has made efforts to ensure that the public signage and notifications explaining the technology, legal authorities, and opt-out options are up to date and visible.[199] The agency developed the robust public notification campaign in part as a response to audit recommendations. Public notification of FRT occurs in many ways, such as through public-facing websites and signage. Signage can be posted in areas where FRT is active. In some sensitive law enforcement circumstances, not all usage or system information can be made available to the public—still, every effort to disclose as much information as possible fosters transparency. CBP's public awareness campaign, which has appeared in national publications such as The Economist and The Hill, is designed to raise and increase the general knowledge of CBP's biometric usage.[200] CBP

---

195 Justin Doubleday, "CBP, TSA Expanding Facial Recognition for Traveler Identity Verification," *Federal News Network*, October 11, 2022, https://federalnewsnetwork.com/technology-main/2022/10/cbp-tsa-expanding-facial-recognition-for-traveler-identity-verification/.

196 Privacy and Diversity Office, "CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program" (Customs and Border Protection, August 15, 2022), https://biometrics.cbp.gov/privacy.

197 Privacy and Diversity Office, 6.

198 CBP, "Biometrics Privacy," accessed September 20, 2022, https://biometrics.cbp.gov/privacy.

199 Gambler, *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*, 10–11.

200 Privacy and Diversity Office, "CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program," 7.

also maintains a website designated to biometrics that provides extensive information about the program and downloadable signage and tear sheets. Public notification leads to responsible use and good practices regardless of how the public is notified.

c. Clear and Defined Purpose

CBP has the authority to collect biometrics pursuant to various regulations, orders, and rules, including the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, which authorizes CBP to use "an automated system to record arrivals and departures of non-U.S. citizens at all air, sea, and land ports of entry;" the 2002 Enhanced Border Security and Visa Entry Reform Act; the Implementing Recommendations of the 9/11 Commission Act of 2007; the Consolidated Appropriations Act of 2016, which authorized CBP "to expend up to $1 billion in certain visa fees for biometric entry and exit implementation"; and Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States," which requires "DHS to expedite the performance of a biometric entry and exit tracking system."[201] Other immigration laws also authorize CBP to collect biometric entry and exit data. As part of the privacy-by-design approach, CBP clearly outlines these authorities on signage, privacy compliance documentation, proposed regulations, and other documents. Understanding the legal authorities under which it operates allows CBP to incorporate biometrics in the least intrusive manner to meet the mission.

d. Accurate Technology

The efficiency and utility of FRT depend on the accuracy of the technology. The technology's accuracy depends on the algorithm used for matching and the thresholds incorporated into the process. Conservative match criteria mitigate false matches. Organizations should select the strictest matching threshold criterion possible to meet operational goals.[202] CBP has accepted these notions and incorporated high-quality algorithms and conservative thresholds. In his congressional testimony, John Wagner,

[201] Department of Homeland Security, "DHS/CBP/PIA-056 Traveler Verification Service," 1.

[202] McLaughlin and Castro, *The Critics Were Wrong*.

former Deputy Assistant Commissioner of CBP, affirmed that CBP uses an NEC algorithm.[203] NIST evaluated the NEC algorithm. It was ranked first or second in most categories, and NIST classified the algorithm as high-performing.[204]

Furthermore, Wagner's testimony stated, "CBP continuously monitors its biometric matching service and conducts a variety of statistical tests and manual evaluations to gauge algorithm results and ensure optimal accuracy and performance." CBP leverages NIST and DHS S&T to determine threshold measures. The CBP Privacy Office determined that the CBP has implemented several assessment mechanisms designed to ensure the quality and integrity of the data collected.[205] CBP continues due diligence in deciding algorithm quality and threshold measures to ensure the program operates efficiently.

e. Data Security

CBP applies four safeguards to secure biometric data: encryption and authentication, biometric templates instead of actual biometrics, limited retention periods, and secured storage.[206] CBP utilizes a two-factor authentication system and encrypts all data during transfer between cameras, TVS, and other DHS systems. Furthermore, the cloud service provider adheres to NIST's security and privacy controls. CBP creates biometric templates of all photos for matching, sharing, and storage. The templates cannot be reverse-engineered and are not recognizable outside the TVS system. CBP discards the images of U.S. citizens and biometric-capture-exempt individuals after identities are verified. As required by law, CBP retains eligible photos in the DHS biometric repository, Automated Biometric Identification System (referred to as IDENT), as a biometrically

---

[203] U.S. House, "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technology Part II," *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technology Part III*, House, 116th Cong., 2nd sess., February 6, 2020.

[204] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*, NIST IR 8238 (Gaithersburg, MD: National Institute of Standards and Technology, 2018), https://doi.org/10.6028/NIST.IR.8238.

[205] Privacy and Diversity Office, "CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program," 13.

[206] "Biometric Exit Frequently Asked Questions," Customs and Border Protection, accessed December 30, 2021, https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

confirmed arrival or departure. CBP partners with airlines, airport authorities, and participating organizations (e.g., vendors or systems integrators), and enforces privacy standards by prohibiting partners from retaining the photos collected on behalf of CBP.[207] Finally, DHS stores all facial images in secured government systems.

f. Training and Access

The training and access operating principle is the least transparent of the seven operating principles within the BEE program. While elements of the training and access principle are found in public-facing documents, CBP does not explicitly discuss training and data access. According to an internal audit, the CBP Privacy Office found that the BEE program maintains the appropriate oversight measures to ensure only authorized personnel can access the biometric data collected. These measures include annual privacy awareness, PII safeguarding training, and a process to provide access based on a need to know.[208] Redacted training presentations have been made available to the public through an EPIC Freedom of Information Act request, but the training frequency is not made public.[209] In CBP's push to remain transparent, the agency could publish more information about training.

g. Accountability

Government agencies are accountable to the public and demonstrate this accountability through audits and reporting. CBP complies with congressional reporting and internal and external audits by both public and private entities. Part one of this section includes examples of compliance. Additionally, CBP has developed a signage audit to

[207] Customs and Border Protection, "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States."

[208] Privacy and Diversity Office, "CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program," 15.

[209] Electronic Privacy Information Center, "EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures)."

evaluate signage and public notification at the ports of entry.[210] CBP's active participation in audits and reporting exemplifies a commitment to accountability.

CBP partners with private entities, such as airlines and airport authorities, on biometric exit operations. It is CBP's responsibility to ensure partners are held to the same standards and comply with the same principles as the agency. To accomplish this, CBP has developed business requirements, enters into compliance agreements, and conducts security audits of partner processes.[211] As of July 2022, CBP conducted eight assessments on partners to determine levels of compliance and resolve non-compliance.[212] By auditing partners, CBP ensures they maintain the operating standards necessary for an ethical and efficient program.

h. Other Considerations and Summary

The seven operating principles do not include redress, but redress plays a role in ethical and efficient programs. The ability to inquire about and resolve difficulties experienced during government interactions increases transparency and public acceptance. According to research, well-designed and implemented redress mechanisms ensure government programs and policies minimize harmful effects on the public, address harmful practices early on, and help prevent legal or other challenges.[213] CBP has established multiple mechanisms for redress. The DHS Traveler Redress Inquiry Program, or DHS TRIP, is the primary source for traveler complaints and inquiries, including biometrics.[214] CBP also operates the CBP Info Center, which provides frequently asked questions and accepts inquiries, and at each port of entry, a Professional Services Manager resolves

---

[210] Privacy and Diversity Office, "CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program," 6.

[211] Data Privacy and Integrity Advisory Committee, *Privacy Recommendations*, 10.

[212] "Statement for the Record on Assessing CBP's Use of Facial Recognition Technology," Congressional Testimony, accessed October 29, 2022, https://www.cbp.gov/about/congressional-resources/testimony/statement-record-assessing-cbps-use-facial-recognition-technology.

[213] Suchi Pande and Naomi Hossain, *Grievance Redress Mechanisms in the Public Sector a Literature Review* (Washington, DC: Open Government Partnership, 2022), 3.

[214] "Traveler Redress Inquiry Program," Traveler Redress Inquiry Program, accessed October 30, 2022, https://www.dhs.gov/dhs-trip.

issues. Redress mechanisms empower the public and enhance transparency within the government.

F. CONCLUSION

CBP leadership asserts the agency continues to work closely with key stakeholders, including NIST, S&T, Congress, and industry, to share lessons learned and best practices, seek the most innovative technologies, streamline processes, and strengthen border security operations.[215] The agency accomplishes these goals through adherence to ethical operating principles. As technology advances, CBP adapts to embrace new procedures and technology enhancements. While CBP's BEE has room for improvement, the program incorporates ethical principles and enhances security. The CBP case study demonstrates how the government can deploy an FRT program that embodies safety and security while considering and addressing public perception.

[215] Customs and Border Protection, "Statement for the Record."

VI. CONCLUSION

The use of FRT is fast becoming commonplace technology built into security processes. FRT will continue to advance in quality and capabilities, and government agencies will continue incorporating facial biometrics into security and other programs. Despite growing usage and popularity in the public and private sectors, FRT continues to evoke public criticism and introduce ELSI challenges. The criticisms and challenges do not immediately disappear from the public sphere. Research reveals that while decision-makers must mitigate the ELSI to garner public approval, FRT has demonstrable security benefits.

Government decision-makers can use tools when considering, developing, implementing, and assessing FRT programs. These tools provide a mechanism for decision-makers to address and mitigate the ELSI concerns. By implementing safeguards and countermeasures, government agencies can balance the benefits of FRT with public concern. Overall, when government decision-makers adhere to ethical decision-making frameworks and operating principles, FRT can be used responsibly and efficiently.

A. RECOMMENDATIONS

This thesis makes four recommendations for government agencies considering or using FRT programs. These recommendations apply to decision-makers at all process phases, including technology consideration, development, implementation, and post-implementation assessments or enhancements of FRT.

1. Recommendation One: Follow the "How to Do It Right" Framework

Government agencies implementing FRT are responsible to the people they serve to consider and assess the negative ramifications of the technology on society.[216] Following an ethical framework affords decision-makers a mechanism to identify, evaluate, and mitigate ethical, legal, and societal issues raised by the public, Congress, and

[216] Chameau, Ballhaus, and Lin, *Emerging and Readily Available Technologies and National Security*, 251.

advocacy groups. The "How to Do It Right" framework provides a cascading approach to decision-making that satisfies the government's obligation to the public. It focuses on and identifies high-level issues, paves a path to analyze them, and finally identifies countermeasures. When decision-makers use ethical frameworks to anticipate and identify problems before implementing technology, they can mitigate the issues, improving public perception and adoption.

2. Recommendation Two: Incorporate Ethical Operating Principles

The increased use of FRT in government programs is a sensitive use case for the technology because of the potential impacts on society. There is a critical need to incorporate robust governance to mitigate the effects on society and optimize security benefits. The seven operational principles outlined in this thesis govern responsible usage and mitigate challenges. Government agencies can adapt the seven operational principles to their specific needs but should implement them in some form. For example, public notification and algorithmic thresholds can vary. While there are more than the seven ethical operating principles advocated for by the security industry, adopting the seven, at minimum, ensures ethical and efficient usage.

3. Recommendation Three: Sustainable Policy and Federal Regulations

The second recommendation goes hand and hand with the third recommendation. Government agencies must develop long-term policies governing technology usage that address ELSI. Once an agency uses an ethical decision-making framework to identify issues, it must decide how to proceed with implementation around the issues. This requires scrutiny of those issues and the best way to address each issue in the policy. Ethical frameworks and operating principles support sustainable policies. Long-term policies must not create a bureaucracy that inhibits technology and program advancement but should follow ethical operating principles. In the absence of regulation, policy governs and promotes responsible FRT usage.

Concurrently, government agencies should explore and lobby for regulations that standardize FRT. Like policy, regulations should not be so restrictive that they hinder technological advancement. Without federal guidelines, state or local legislation will fill in

the gaps causing disparate application of ethical guidelines, principles, and technology. Regulation, along with sustainable policy and ethical principles, cultivate an environment that encourages public acceptance of FRT.

4. Recommendation Four: Explore and Implement FRT Best Practices

A GAO report found that 19 of 24 federal agencies are currently using FRT, and 10 out of the 24 agencies intend to expand the use of FRT.[217] These numbers demonstrate that FRT programs are prevalent in the government. An agency seeking to implement or expand an FRT program has various programs to study. While CBP's BEE illustrates many best practices, there are other agencies and use cases that can shape a new program. An agency must conduct due diligence and ascertain appropriate best practices that support its specific use case. Regardless of the program model used, exploring existing practices keeps an agency from reinventing the process and promotes responsible implementation.

B. FUTURE RESEARCH

There are several avenues for additional research on FRT-related topics in the private and public sectors, especially in law enforcement environments, that this research does not address. This research focuses on the ethical and efficient implementation of FRT. It does not include discussion topics such as the legal elements of FRT, technical efficacy and other technical aspects of biometric collection, or comparisons to foreign biometric programs. Since technology constantly evolves, FRT research should keep pace with the evolution and maturation of the technology and associated policies.

Technology often outpaces the law, so it is common for emerging technology to lack governing regulations.[218] It is also common for existing regulations to conflict with or raise concerns about emerging technology. Research into the legal ramifications of FRT on society is a viable research path. For example, how does FRT impact privacy laws, or is FRT a violation of the Fourth Amendment? Research into the types of legislation necessary to govern and standardize FRT also adds to the legal literature.

---

[217] Goodwin and Wright, *Facial Recognition Technology*, 25.

[218] Hodge Jr., "The Legal and Ethical Considerations of FRT," 745.

Biometrics and facial recognition comprise a broad category. Numerous scientific avenues can contribute to the literature, which includes threshold assessment, biometric spoofing countermeasures, and environmental impacts on match rates. Further studies can look at multimodal biometric technology systems, such as using a combination of facial and iris recognition to augment security. Analysis of algorithms, artificial intelligence enhancements, bias and accuracy, and match rates provide data that aids the decision-making process

Another potential research avenue involves comparative studies. FRT is not exclusive to the United States. FRT has been implemented in various government agencies across the globe. Different countries follow different rules and procedures. For example, the European Union's General Data Protection Regulation (GDPR) governs data and biometrics collection and use. The GDPR is more restrictive than U.S. privacy laws. Then there are other surveillance state extremes like China. Comparative studies identify practices and models to avoid or replicate. Furthermore, a decision-maker can use comparative research to provide a frame of reference for technology implementation.

Finally, the ethical operating principles outlined throughout this analysis warrant additional research. This thesis identifies common public criticisms of FRT and countermeasures to mitigate the concerns, but the seven principles and derivative best practices can be discussed in greater detail. Ethical and societal concerns evolve as the technology matures and society becomes more accustomed to technology. Updating and modernizing the ethical principles may be necessary to accommodate changing public perception. Furthermore, government agencies can benefit from a step-by-step implementation guide incorporating ethical frameworks and operating principles.

LIST OF REFERENCES

Abomhara, Mohamed, Sule Yildirim Yayilgan, Anne Hilde Nymoen, Marina Shalaginova, Zoltán Székely, and Ogerta Elezaj. "How to Do It Right: A Framework for Biometrics Supported Border Control." In *E-Democracy–Safeguarding Democracy and Human Rights in the Digital Age*, edited by Sokratis Katsikas and Vasilios Zorkadis, 94–109. Cham, Switzerland: Springer, 2019.

Acree, Mark A. "People v. Jennings: A Significant Case for Fingerprint Science in America." *Journal of Forensic Identification* 65, no. 4 (2015): 600–602.

Aljeraisy, Atheer, Masoud Barati, Omer Rana, and Charith Perera. "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective." *ACM Computing Surveys* 54, no. 5 (2022): 1–38. EBSCOhost.

Allyn, Bobby. "'The Computer Got It Wrong': How Facial Recognition Led to False Arrest of Black Man." NPR: America Reckons with Racial Injustice, June 24, 2020. https://www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig.

Anderson, Elisha. "Controversial Detroit Facial Recognition Got Him Arrested for a Crime He Didn't Commit." *Detroit Free Press*, July 10, 2020. https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

Apple. "About Face Id Advanced Technology." Apple Support. Accessed December 28, 2021. https://support.apple.com/en-us/HT208108.

Baker, Eric. "I've Got My AI on You: Artificial Intelligence in the Law Enforcement Domain." Master's thesis, Naval Postgraduate School, 2021. http://hdl.handle.net/10945/67100.

Biometric Technology Today. "Disney Uses Facial Recognition to Guard Its Magic Kingdom." *Biometric Technology Today* 2021, no. 4 (April 2021): 1. https://doi.org/10.1016/S0969-4765(21)00038-2.

Bonde, Sheila, and Paul Firenze. "A Framework for Making Ethical Decisions." Lecture presented at the Making Choices: Ethical Decisions at the Frontier of Global Science, Brown University, May 2013. https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions.

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

Buolamwini, Joy, Vincent Ordonez, Jamie Morgenstern, and Erik Learned-Miller. *Facial Recognition Technologies: A Primer*. Chicago: The McArthur Foundation, 2020. https://www.ajl.org/federal-office-call.

Buzan, Barry, Waever Ole, and Jaape de Wilde. *Security: A New Framework for Analysis*. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Pub., 1998.

Calvo, Patrici. "The Ethics of Smart City: Moral Implications of Hyperconnectivity, Algorithmization and the Datafication of Urban Digital Society." *Ethics and Information Technology* 22, no. 2 (June 2020): 141–49. https://doi.org/10.1007/s10676-019-09523-0.

Carter, Anthony. "Facing Reality: The Benefits and Challenges of Facial Recognition of the NYPD." Master's thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/60374.

Center for Strategic and International Studies. "About Us." Center for Strategic and International Studies. Accessed August 27, 2022. https://www.csis.org/programs/about-us.

Chameau, Jean-Lou, William F. Ballhaus, and Herbert S. Lin, eds. *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal and Societal Issues*. *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal and Societal Issues*. Washington, DC: National Academies Press, 2014. https://pubmed.ncbi.nlm.nih.gov/25032403/.

Chamoli, Deepti. "Deep Learning-Based Live-Streaming Face Recognition." *Analytics Vidhya* (blog), November 14, 2019. https://medium.com/analytics-vidhya/deep-learning-based-live-streaming-face-recognition-31e9b005ffb.

Crumpler, William. "How Accurate Are Facial Recognition Systems and Why Does It Matter?" *Strategic Technology* (blog). Accessed September 2, 2022. https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.

Crumpler, William, and James Andrew Lewis. *How Does Facial Recognition Work?* Washington, DC: Center for Strategic and International Studies, 2021. https://www.csis.org/analysis/how-does-facial-recognition-work.

Customs and Border Protection. "About CBP." Customs and Border Protection, February 24, 2022. https://www.cbp.gov/about.

———. "Biometric Exit Frequently Asked Questions." Customs and Border Protection. Accessed December 30, 2021. https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

———. “Biometrics Privacy.” Accessed September 20, 2022. https://biometrics.cbp.gov/privacy.

———. “CBP Announces Facial Biometric Pilot for Inbound Vehicle Travelers at Anzalduas International Bridge | U.S. Customs and Border Protection.” National Media Release, September 20, 2021. https://www.cbp.gov/newsroom/national-media-release/cbp-announces-facial-biometric-pilot-inbound-vehicle-travelers.

———. “CBP Biometrics.” CBP Biometrics. Accessed December 27, 2021. https://biometrics.cbp.gov.

———. “Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States.” *Federal Register Notice* 85, no. 224 (November 19, 2020): 74162–93. https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states.

———. “Statement for the Record on Assessing CBP’s Use of Facial Recognition Technology.” Congressional Testimony. Accessed October 29, 2022. https://www.cbp.gov/about/congressional-resources/testimony/statement-record-assessing-cbps-use-facial-recognition-technology.

———. “Test to Collect Facial Images from Occupants in Moving Vehicles at the Anzalduas Port of Entry (Anzalduas Biometric Test).” *Federal Register Notice* 83, no. 220 (November 14, 2018): 56862–64. https://www.govinfo.gov/content/pkg/FR-2018-11-14/pdf/2018-24850.pdf.

Data Privacy and Integrity Advisory Committee. *Privacy Recommendations in Connection with the Use of Facial Recognition Technology*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/publication/dpiac-recommendations-report-2019-01.

Department of Homeland Security. “Biometrics.” Department of Homeland Security, October 24, 2016. https://www.dhs.gov/biometrics.

———. “DHS/CBP/PIA-056 Traveler Verification Service.” Department of Homeland Security, November 15, 2018. https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

———. “The Fair Information Practice Principles.” Department of Homeland Security, May 26, 2022. https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

———. *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies*. Washington, DC: Department of Homeland Security, 2019. https://www.tsa.gov/sites/default/files/biometricsreport.pdf.

———. “Traveler Redress Inquiry Program.” Traveler Redress Inquiry Program. Accessed October 30, 2022. https://www.dhs.gov/dhs-trip.

DHS Privacy Office. *Privacy Incident Handling Guidance*. Washington, DC: Department of Homeland Security, 2017. https://www.dhs.gov/publication/privacy-incident-handling-guidance-0.

Doubleday, Justin. “CBP, TSA Expanding Facial Recognition for Traveler Identity Verification.” *Federal News Network*, October 11, 2022. https://federalnewsnetwork.com/technology-main/2022/10/cbp-tsa-expanding-facial-recognition-for-traveler-identity-verification/.

Dunlap, David. “Securing Our Hospitals and Protecting Your Privacy.” *Campus Security and Life Safety*, March 2019. https://campuslifesecurity.com/digital-edition/2019/04/digital-edition_march_april/asset.aspx.

Electronic Privacy Information Center. “EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures).” EPIC. Accessed December 28, 2021. https://www2.epic.org/foia/dhs/cbp/alt-screening-procedures/#background.

Finklea, Kristin, Laurie Harris, Abigail Folker, and John Sargent. *Federal Law Enforcement Use of Facial Recognition Technology*. CRS Report No. R46586. Washington, DC: Congressional Research Service, 2020.

Future of Privacy Forum. “About.” Future of Privacy Forum. Accessed August 27, 2022. https://fpf.org/about/.

———. *Summary of Privacy Principles*. Washington, DC: Future Privacy Forum, 2018. https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf.

Gambler, Rebecca. *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*. GAO-20-568. Washington, DC: Government Accountability Office, 2020.

———. *Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues*. GAO22106154. Washington, DC: Government Accountability Office, 2022. https://www.gao.gov/assets/gao-22-106154.pdf.

Garvie, Clare, and Laura Moy. *America under Watch: Face Surveillance in the United States*. Washington, DC: Georgetown Law Center on Privacy and Technology, 2019. https://www.americaunderwatch.com/.

Gates, Kelly. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press, 2016. https://doi.org/10.18574/nyu/9780814732090.001.0001.

Gershgorn, Dave. "Retail Stores Are Packed with Unchecked Facial Recognition." The Verge, July 14, 2021. https://www.theverge.com/2021/7/14/22576236/retail-stores-facial-recognition-civil-rights-organizations-ban.

Gill, Pat. "Technostalgia: Making the Future Past Perfect." *Camera Obscura: Feminism, Culture, and Media Studies* 14, no. 1–2 (1997): 161–79. https://doi.org/10.1215/02705346-14-1-2_40-41-161.

Goodwin, Gretta L., and Candice Wright. *Facial Recognition Technologies: Current and Planned Uses by Federal Agencies*. GAO-21-526. Washington, DC: Government Accountability Office, 2021. https://www.gao.gov/products/gao-21-526.

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

———. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NIST IR 8280. Gaithersburg, MD: National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.IR.8280.

———. *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*. NIST IR 8238. Gaithersburg, MD: National Institute of Standards and Technology, 2018. https://doi.org/10.6028/NIST.IR.8238.

Harwell, Drew. "Detroit Police Face Suit over Facial Recognition Software." *Washington Post*, April 14, 2021. https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/.

Herman, Susan N. *Taking Liberties: The War on Terror and the Erosion of American Democracy*. *Taking Liberties*. Cary, UK: Oxford University Press, 2011.

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

Hodge Jr., Samuel D. "The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector Technology in the Business Sector." *DePaul Law Review* 71, no. 3 (2022): 731–63. https://via.library.depaul.edu/law-review/vol71/iss3/2.

International Biometrics and Identification Society. *Identification Technology & Privacy Policy Principles*. Washington, DC: International Biometrics and Identification Society, 2021. https://www.ibia.org/resources/white-papers.

Katsanis, Sara H., Peter Claes, Megan Doerr, Robert Cook-Deegan, Jessica D. Tenenbaum, Barbara J. Evans, Myoung Keun Lee, Joel Anderton, Seth M. Weinberg, and Jennifer K. Wagner. "A Survey of U.S. Public Perspectives on Facial Recognition Technology and Facial Imaging Data Practices in Health and Research Contexts." Edited by Renuka Sane. *PLOS ONE* 16, no. 10 (October 14, 2021): 1–16. https://doi.org/10.1371/journal.pone.0257923.

Kizza, Joseph Migga. *Ethical and Social Issues in the Information Age*. Texts in Computer Science. Cham, Switzerland: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-70712-9.

Klosowski, Thorin. "Facial Recognition Is Everywhere. Here's What We Can Do About It." *Wirecutter* (blog), July 15, 2020. https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

Lewis, James Andrew, and William Crumpler. *Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape*. Washington, DC: Center for Strategic and International Studies, 2021. https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

Lovegrove, Matt. "Why We Need to Talk about Ethics in Technology." Hello World, 2020. https://helloworld.raspberrypi.org/articles/HW06-why-we-need-to-talk-about-ethics-in-technology.

Lynch, Jennifer. *Face Off: Law Enforcement Use of Face Recognition Technology*. San Francisco: Electronic Frontier Foundation, 2018. https://www.eff.org/wp/law-enforcement-use-face-recognition.

Mason, Marcy. "Biometric Breakthrough: How CBP Is Meeting Its Mandate and Keeping America Safe." *Frontline*, December 8, 2018. https://www.cbp.gov/frontline/cbp-biometric-testing.

McCarthy, Craig. "Facial Recognition Leads Cops to Alleged Rapist in Under 24 Hours." *New York Post*, August 5, 2019. https://nypost.com/2019/08/05/facial-recognition-leads-cops-to-alleged-rapist-in-under-24-hours/.

McClellan, Elizabeth. "Facial Recognition Technology: Balancing the Benefits and Concerns." *Journal of Business & Technology Law* 15, no. 2 (2020): 363–80. Ebscohost.

McLaughlin, Michael, and Daniel Castro. *The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist*. Washington, DC: Information Technology and Innovation Foundation, 2020. https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

Meden, Blaz, Peter Rot, Philipp Terhorst, Naser Damer, Arjan Kuijper, Walter J Scheirer, Arun Ross, Peter Peer, and Vitomir Struc. "Privacy-Enhancing Face Biometrics: A Comprehensive Survey." *IEEE Transactions on Information Forensics and Security* 16 (2021): 4147–83. https://doi.org/10.1109/TIFS.2021.3096024.

Naker, Sharon, and Dov Greenbaum. "Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy." *Boston University Journal of Science and Technology* 23 (2017): 88–123. https://www.bu.edu/jostl/files/2017/04/Greenbaum-Online.pdf.

Nelson, Aaron. "Ethical Decision Making for Homeland Security." Master's thesis, Naval Postgraduate School, 2013. https://calhoun.nps.edu/handle/10945/37684.

Nieto, Andres Crucetta. "Is Facial Recognition Inhibiting Our Freedom of Speech?" *Chicago Policy Review*, October 12, 2020. https://chicagopolicyreview.org/2020/10/12/is-facial-recognition-inhibiting-our-freedom-of-speech/.

North-Samardzic, Andrea. "Biometric Technology and Ethics: Beyond Security Applications." *Journal of Business Ethics* 167, no. 3 (2019): 433–50. https://doi.org/10.1007/s10551-019-04143-6.

O'Connor, Sean. "Biometrics and Identification after 9/11." *Bender's Immigration Bulletin* 7 (February 2002): 150–73. https://doi.org/10.2139/ssrn.299950.

Office of Inspector General. *CBP Complied with Facial Recognition Policies to Identify International Travelers at Airports*. OIG-22-48. Washington, DC: Department of Homeland Security, 2022.

———. *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot*. OIG-20-71. Washington, DC: Department of Homeland Security, 2020. https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

Ong, Desmond C. "An Ethical Framework for Guiding the Development of Affectively-Aware Artificial Intelligence." In *2021 9th International Conference on Affective Computing and Intelligent Interaction (ACII)*, 1–8. IEEE, 2021.

Pande, Suchi, and Naomi Hossain. *Grievance Redress Mechanisms in the Public Sector a Literature Review*. Washington, DC: Open Government Partnership, 2022.

Panetta, Larry. "Simplified Arrival: A Stakeholder Overview." Presentation, Port of Seattle, 2020. https://www.portseattle.org/sites/default/files/2020-08/Simplified_Arrival_Overview_CBP_Field_Ops_presentation.pdf.

Parker, Jake. "Facial Recognition Success Stories Showcase Positive Use Cases of the Technology." Security Industry Association, July 16, 2020. https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/.

Privacy and Diversity Office. "CBP Privacy Evaluation of the Traveler Verification Service in Support of the CBP Biometric Entry-Exit Program." Customs and Border Protection, August 15, 2022. https://biometrics.cbp.gov/privacy.

Rose, Nikolas S. *Powers of Freedom: Reframing Political Thought*. *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press, 1999.

Santa Clara University. "A Framework for Ethical Decision Making." Markkula Center for Applied Ethics: Ethics Resources, November 8, 2021. https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/.

Schaffer, Aaron. "The Cybersecurity 2022: Activists and Lawmakers Increase Calls for Ban on Federal Use of Facial Recognition Technology." *Washington Post*, July 2, 2021. https://www.washingtonpost.com/politics/2021/07/02/cybersecurity-202-some-activists-lawmakers-want-ban-federal-government-using-facial-recognition-technology/.

Security Industry Association. "About SIA." Security Industry Association. Accessed August 27, 2022. https://www.securityindustry.org/about-sia/.

———. *Sia Principles for the Responsible and Effective Use of Facial Recognition Technology*. Silver Springs, MD: Security Industry Association, 2020. https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/.

Smith, Aaron. *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*. Washington, DC: Pew Research Center, 2019. https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

Snow, Jacob. "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots." *ACLU NorCal* (blog), July 26, 2018. https://www.aclunc.org/blog/amazon-s-face-recognition-falsely-matched-28-members-congress-mugshots.

Sobol, Richard. "The Right to Travel and Privacy: Intersecting Fundamental Freedoms." *John Marshall Journal of Information Technology & Privacy Law* 30, no. 4 (2014): 639–68. https://repository.law.uic.edu/jitpl/vol30/iss4/1.

U.S. Congress. House. *Examining the Department of Homeland Security's Use of Facial Recognition and Other Technologies, Part II*, House, 116th Cong., 2nd sess., February 6, 2020.

U.S. Congress. House. *Facial Recognition Technology: Part I Its Impact on Our Civil Rights and Liberties*, House, 119th Cong., 1st session, May 22, 2019.

U.S. Congress. Senate. *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism*, Senate, 117th Cong., 1st sess., November 14, 2001. https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/html/CHRG-107shrg81678.htm.

U.S. House. *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technology Part II*, House, 116th Cong., 2nd sess., February 6, 2020.

Washington Post. "Forcing Facial Recognition Is a Mistake." *Washington Post*, February 7, 2022. ProQuest.

Wood, J. Luke, and Adriel A. Hilton. "Five Ethical Paradigms for Community College Leaders: Toward Constructing and Considering Alternative Courses of Action in Ethical Decision Making." *Community College Review* 40, no. 3 (July 2012): 196–214. https://doi.org/10.1177/0091552112448818.

Woodward, John D. *Biometrics: Facing up to Terrorism*. Santa Monica, CA: RAND Corporation, 2001. https://www.rand.org/pubs/issue_papers/IP218.html.

World Economic Forum. *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*. Geneva, Switzerland: World Economic Forum, 2021. https://www.weforum.org/whitepapers/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations.

Wynn, Eric Z. "Privacy in the Face of Surveillance: Fourth Amendment Considerations for Facial Recognition Technology." Master's thesis, Naval Postgraduate School, 2015. http://hdl.handle.net/10945/45279.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California