PRE-DECISIONAL/DELIBERATIVE

Discussing a Framework for the Responsible Use of Facial Recognition Technology in Law Enforcement

The National Artificial Intelligence Advisory Committee (NAIAC)
Law Enforcement Subcommittee (NAIAC-LE Subcommittee)

July 2024

NAIAC-LE SUBCOMMITTEE MEMBERS

The NAIAC-LE Subcommittee prepared this document for review by the full NAIAC.

Armando Aguilar
Assistant Chief of Police, Miami Police Department

Anthony Bak
Head of AI, Palantir

Amanda Ballantyne
Director of the AFL-CIO Technology Institute

Jane Bambauer
Director - Marion B. Brechner First Amendment Project, Brechner Eminent Scholar at the College of Journalism and Communications and at Levin College of Law, University of Florida

Esha Bhandari
Deputy Director of the American Civil Liberties Union's Speech, Privacy, and Technology Project

Jennifer Eberhardt
Professor of Organizational Behavior and Psychology, Stanford University

Farhang Heydari
Assistant Professor of Law, Vanderbilt Law School

Benji Hutchinson
Chief Revenue Officer of Rank One Computing

Rashawn Ray
Vice-President and Executive Director of the AIR Equity Initiative

Cynthia Rudin
Professor of Computer Science, Electrical and Computer Engineering, Statistical Science, Mathematics, Biostatistics & Bioinformatics at Duke University

BACKGROUND

Law enforcement agencies (LEAs) have a legitimate public safety interest in identifying individuals for numerous reasons. Video and photographic evidence obtained from surveillance footage, bystanders, social media, and other sources may provide crucial evidence about who may be a suspect, victim, witness, or community member in distress. Facial recognition technologies (FRTs) can allow LEAs to identify these individuals with greater frequency, speed, and accuracy. Therein lies both the potential and the risk of facial recognition technology.[1]

While some communities and civil rights organizations oppose all use of FRTs by law enforcement, public opinion is mixed, with 46% believing that "widespread use of facial recognition technology by police would be a good idea" (compared to 27% who say it would be a "bad idea"[2]).

The framework provided below creates the structure for legal requirements and best practices that should steer the responsible use of FRTs. Four basic findings provide the backdrop for the framework:

- **FRT, when used appropriately, has the potential to improve the quality of law enforcement's efforts, including both its criminal investigations and its community caretaking functions.**

- **At the same time, unconstrained use of FRT poses a serious risk to civil rights and civil liberties, including but not limited to accuracy and bias concerns, risks to free expression, and privacy invasions.**

- **Current law does not adequately direct or constrain law enforcement FRT use to ensure that law enforcement is capturing the benefits of the technology while also guarding against its risks.**

- **Accordingly, if policing agencies are going to continue to use — or start using — FRT technology, they should do so subject to carefully-considered guardrails.**

[1] National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*, 2024.
[2] Lee Rainie et al., "AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns," Pew Research, 2022, https://www.pewresearch.org/science/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/.

The framework below provides some preliminary recommendations for future recommendations. In some cases, we provide alternative recommendations. Because of the unprecedented nature of FRT, and the fact that reasonable and knowledgeable individuals will have differing opinions about how to plan for uncertainty and how to manage conflicts between competing values, we have not, and could not, reach consensus on each and every major issue relating to FRTs. For this reason, we have noted which issues caused significant fractures among our members so that NAIAC may have a well-informed discussion about the competing interests involved.

We have identified a set of FRT uses that are primarily "surveillance" uses (as opposed to standard uses) for which we do not yet have a framework and set of preliminary recommendations. Discussion of these uses should be reserved for another time.

A FRAMEWORK FOR FRT USE

The heads of federal LEAs should review their use of FRT and ensure that it comports with the following principles. In addition, the executive branch should use all appropriate mechanisms to ensure that state and local LEAs[3] adhere to the following principles, including supporting legislation introduced in Congress consistent with these principles.

DEMOCRATIC ACCOUNTABILITY

Basic democratic values demand that policing tactics receive democratic approval.[4] The form of that approval, however, is up for discussion. The Subcommittee has considered three possibilities:

1-A. Local Government Involvement

LEAs should inform their local government authority prior to acquiring or implementing an FRT system, providing details about the system and soliciting feedback.

[3] According to the U.S. Department of Justice, there are 17,541 state and local agencies that perform law enforcement functions in the United States. *See,* Andrea M. Gardner and Kevin M. Scott, "Census of State and Local Law Enforcement Agencies, 2018 – Statistical Tables," U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2022, https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/cslle18st.pdf.

[4] *See, e.g.*, Barry Friedman and Maria Ponomarenko, "Democratic Policing", 90 *N.Y.U. L. REV.* (2015): 1827; Barry Friedman, *Unwarranted: Policing Without Permission* (2017).

Some members believe the appropriate level of democratic accountability is at the state level and would require authorizing legislation to ensure full political attention and representation.

1-B. State Authorizing Legislation

LEAs should not acquire or implement an FRT system, or should stop usage if already acquired, unless their jurisdiction's state legislature has enacted a law specifically authorizing the use of FRT for law enforcement purposes.

A middle ground is to require pre-authorization from the relevant local government body.

1-C. Local Government Pre-Approval Involvement

LEAs should receive prior approval from their local government authority prior to acquiring or implementing an FRT system.

TECHNICAL GUARDRAILS

Given the stakes in law enforcement investigations, accuracy is essential. To avoid costly errors, FRTs should meet a minimum level of performance and transparency before use in the field.[5]

2. Technical Requirements[6]

LEAs should not purchase FRT software from a vendor, use the results of FRT software from a vendor, or produce their own FRT systems, unless the vendor or producer:

- Can demonstrate, using results from NIST testing, high accuracy across the demographic groups present in real-world use;

[5] Patrick J. Grother, Mei L. Ngan, and Kayee K. Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) Part II: Identification," National Institute of Standards and Technology, 2019, https://www.nist.gov/publications/face-recognition-vendor-test-frvt-part-2-identification ("Recognition accuracy is very strongly dependent on the algorithm and, more generally, on the developer of the algorithm.").

[6] *See, e.g.,* "Facial Recognition Systems Use - Guidelines - Methods & Techniques," Facial Identification Scientific Working Group, 2013-2024, https://fiswg.org/documents.html.

- Discloses information about their FRT systems sufficient to enable independent, expert assessment of their FRT systems' performance for intended law enforcement use cases;

- Provides instruction and documentation on image quality and other relevant technical specifications required to maintain low error rates across demographic groups for the particular system(s) sold to law enforcement;

- Provides LEA users with ongoing training, technical support, and software updates needed to ensure their FRT systems can maintain high accuracy across demographic groups in real-world deployment contexts;[7]

- Builds their FRT technology to facilitate auditing regarding who is using the technology and for what purpose; and

- Can demonstrate compliance with data security best practices.[8]

Comment: Some members of NAIAC-LE would encourage the federal government to develop a certification or licensing procedure that would govern entities holding large biometric datasets, including curated collections of photos of individuals with identifiers, or FRT face maps.

CREATION OF, AND COMPLIANCE WITH, ACCEPTABLE USE POLICIES

3. Acceptable Use Policies[9]

Consistent with NAIAC-LE recommendations for all high-risk AI applications ("Require Public Use Policies for High-Risk AI"), LEAs should maintain and publish a comprehensive FRT acceptable use policy. The policy should, at a minimum, specify:

- **FRT uses that are authorized or prohibited**
- **Protocols and procedures that will ensure consistent and lawful use**
- **Authorized users of FRT**
- **Rules for data collection and retention**
- **Restrictions on data access, analysis, or release**

[7] *See, e.g.,* "Training," Facial Identification Scientific Working Group, 2019-2024, https://fiswg.org/documents.html.

[8] Such as CISA and NSA, *Recommended Best Practices for Administrators: Identity and Access Management* (2023).

[9] *See, e.g.,* "Practitioner Code of Ethics" and "Analysis - Comparison - Evaluation," published documents, Facial Identification Scientific Working Group, 2018-2024, https://fiswg.org/documents.html.

- **Required documentation and supervision of FRT use**

LEAs should have a mechanism for receiving and responding to community input while developing and reviewing these acceptable use policies. Particular emphasis should be placed on engagement with the communities most impacted by crime and policing.

Comment: The recommendations below will set minimum standards for many of these required components of the acceptable use policy.

4. Designated Acceptable Use Officer

LEAs should route requests for facial comparisons to a designated sworn or civilian agency employee(s) well versed in agency facial recognition policy. The designee should ensure that all fulfilled requests fall within agency policy and reject any requests that do not comply with said policy.

5. Public Logs

Consistent with previous recommendations from the NAIAC, LEAs using FRT should collect and publish information about how they use the technology. ("Recommendation: Require Public Summary Reporting on Use of High-Risk AI" (May 2024)).

6. Internal Logs

LEAs should maintain internal logs documenting the reason for each FRT search (consistent with agency policy), the agency case number associated with the search, the name of the employee conducting the search, and the name of the employee requesting the search (if different from the employee conducting the search).

TRAINING REQUIREMENTS

7. Training Requirements

All individuals who review, analyze, use, and interact with the FRT system(s) should first receive specialized training on the capabilities and limitations of this technology generally and the particular system(s) in use. Access to FRTs should be limited to trained agents who have earned a professional credential or certification for FRTs (when such certifications become available). FRT results must be subject to review by a trained human-in-the-loop before any action is taken on the information.

TAXONOMY OF USES

For our recommendations, it is useful to categorize the use of FRTs along two dimensions: (1) law enforcement versus non-law enforcement use and (2) standard versus surveillance use.

Law Enforcement versus Non-Law Enforcement

FRT use for criminal investigations includes the archetype case in which a law enforcement agency applies FRT to identify a suspect from an image captured at the scene of a crime. By contrast, when FRT is used to identify an incapacitated person, or to limit access to a high-security building or area, such use is non-criminal. There are, however, no bright lines that can cleanly separate criminal from non-criminal use. The most difficult examples involve the use of FRT to identify crime victims or witnesses to a crime, who may become reluctant participants in a criminal investigation or prosecution, and who may become criminal defendants in *other* criminal investigations. Thus, we recommend considering FRT use along the law enforcement-to-non-law enforcement range through three crude categories: **suspects**, **victims or witnesses**, and **non-law enforcement use**.

Standard Use versus Surveillance

Throughout this set of recommendations, we will distinguish standard usage of FRT from surveillance. "Surveillance," much like "non-criminal," is another term that evades clean definition.[10] We will use the term to denote using FRT *en masse* (that is, over a large group of people), at scale (that is, distributed across a large number of places) or for the purposes of tracking across time (that is, using FRT to track a target longitudinally, across multiple places and times). The use of FRT for surveillance heightens the concern for misuse, abuse, and public distrust — particularly when used for the purpose of criminal investigations.

Table One: Use Case Illustrations

Putting these two dimensions together, we can consider the following FRT use case illustrations:

[10] Marx, Gary T. "Surveillance Studies." *International Encyclopedia of the Social & Behavioral Sciences*, Second Edition (2015): 733–741. https://web.mit.edu/gtmarx/www/surv_studies.pdf.

	Suspects	**Victims and Witnesses**	**Non-Law Enforcement Uses**
Standard Use	Using FRT based on image/footage from a crime scene to identify a suspect Using FRT to confirm identity of somebody in custody, or lawfully stopped based on reasonable suspicion or probable cause Using FRT after probable cause is established for exculpatory purposes (to find alternative suspects)	Using FRT to identify a crime victim Using FRT to identify a crime witness Using FRT to identify a potential future victim	Using FRT to identify a juvenile, an incapacitated person, or a corpse Using FRT to identify an officer for Internal Affairs / internal administration purposes Using FRT to manage access to police/school/government buildings, devices, and computer systems
Surveillance	Using FRT on images from multiple locations to find a suspect and execute an arrest Using FRT to monitor for safety or execute arrest warrants at large gatherings and events	Using FRT on images from multiple locations to find an abducted child	

Table Two: Recommendation Mapping

The recommendations that appear below can be mapped as follows:

	Suspects	**Victims and Witnesses**	**Non-Law EnforcementUses**
Standard Use	8, 9, 10	8, 9, 11	No special restrictions at this time
Surveillance	OUT OF SCOPE AT THIS TIME	OUT OF SCOPE AT THIS TIME	OUT OF SCOPE AT THIS TIME

Comment on real-time applications: At least one NAIAC-LE member has expressed particular concern for real-time, or near-real-time, use of FRT for finding leads in serious (i.e., arrestable) criminal cases. While the concerns are particularly pronounced for real-time surveillance, even the standard usage of FRT in real-time raises concerns because the sense of time-based urgency is more likely to lead to misjudgment or escalation. However, based in part on briefings from Miami's and New York City's police departments, the majority of NAIAC-LE members concluded that the marginal risks posed by real-time standard use of FRT are outweighed by the benefits from generating actionable leads quickly.

Comment on use to locate victims: NAIAC-LE has reserved for future treatment the use of FRT for law enforcement surveillance (as defined above.) Surveillance use of FRT on potential witnesses and victims has also been reserved, as it, too, runs significant risks of privacy and civil liberties abuse. However, the surveillance-style of use for the purpose of locating crime victims deserves special attention for its public safety benefits. Use of FRT en masse *or at scale may be particularly valuable, even with the limited surveillance infrastructure we have in place today, in order to locate missing children or the victims of human trafficking. Some NAIAC-LE members expressed a hope to encourage the adoption of FRT for these purposes as a top example of beneficial use. Others are concerned that any use of FRT at scale provides a precedent, and possibly incentives, for creating additional physical infrastructure, or for carrying out other forms of mass surveillance.*

USE LIMITED TO CERTAIN CRIMES

These alternative recommendations each seek to create a minimum floor on the types of crimes for which law enforcement investigators may use FRT.

8-A. Limitation to Arrestable Criminal Offenses

With respect to law enforcement investigations, the use of FRT searches should be limited to the identification of individuals or production of leads connected with the investigation of arrestable criminal offenses.

8-B. Limitation to Serious Criminal Offenses

With respect to law enforcement investigations, the use of FRT searches should be limited to the identification of individuals or production of leads connected with the investigation of serious criminal offenses.[11]

OTHER RESTRICTIONS AND LIMITATIONS ON USE

9. Manipulation Prohibited[12]

LEAs should not substantively manipulate probe images or generate probe images through composite sketches, AI, or other methods unless the methods have been scientifically validated through NIST testing.

10-A. No Probative Value for Suspicion

FRT search results should be used only as investigatory leads. Under this standard, LEAs would be prohibited from using FRT search results to establish probable cause for an enforcement action, or to accord any probative weight to them in a suspicion analysis. Reasonable suspicion and probable cause must be established without reliance on FRT search results using physical, electronic, testimonial, or other circumstantial evidence.

Comment: Nothing in this recommendation is meant to suggest that LEAs should obscure the use of FRT from judges and magistrates who are considering warrant applications. To the contrary, as we discuss below, disclosure in the criminal process is essential. Rather, this recommendation concerns the weight that should be attached to FRT search results.

[11] One definition of "serious criminal offense," coming from the U.S. laws that apply to foreign diplomats, defines a serious criminal offense as "(A) any felony under Federal, State, or local law; (B) any Federal, State, or local offense punishable by a term of imprisonment of more than 1 year; (C) any crime of violence as defined for purposes of section 16 of title 18 ; or (D) (i) driving under the influence of alcohol or drugs; (ii) reckless driving; or (iii) driving while intoxicated." 22 USC § 4304b(a)(3).

[12] *See, e.g.,*: "Standard Practice/Guide for Image Processing to Improve Automated Facial Recognition Search Performance," Facial Identification Scientific Working Group, 2020, https://fiswg.org/fiswg_image_proc_to_improve_fr_search_v2.0_2020.07.17.pdf.

Some members of NAIAC-LE would prefer to allow LEAs to afford some probative weight to the results of FRT searches, equivalent to the weight afforded an anonymous tip.

10-B. Probative Value Equivalent to an Anonymous Tip

FRT search results should be used only as investigatory leads equivalent to anonymous tips. Under this standard, LEAs would be prohibited from using FRT search results alone to establish probable cause for an enforcement action, but they may use FRT search results alongside physical, electronic, testimonial, or other circumstantial evidence to establish probable cause or reasonable suspicion.

Other members prefer to have the weight vary in proportion to the FRT's demonstrated performance in the field under similar circumstances and with its confidence levels for the search at hand, if there were no other way to obtain additional evidence.

10-C. Probative Value Dependent on Testing

Unless independent field testing has demonstrated consistent performance under conditions similar to the investigation, FRT search results should be used only as investigatory leads and should be afforded no probative weight in a suspicion analysis.

11. Use to Identify Victims and Witnesses

With respect to law enforcement investigations, the use limitation policy required under Recommendation 3 should specify whether FRT may be used to identify potential witnesses or crime victims, and should describe any further restrictions or policies on such use.

12. Use for Lineups

The Subcommittee has begun, but not yet concluded, a discussion of how the results of FRT searches should be used, if at all, to construct eye-witness lineups. Two possible guardrails include:

12-A. Restriction on Lineups

LEAs should be prohibited from conducting a lineup based solely on a facial recognition investigative lead without independent and reliable evidence linking a suspect to a crime.

12-B. Restriction on Lineups

If LEAs conduct a lineup based solely on a facial recognition investigative lead, a positive identification from the lineup should not be used alone to meet the probable cause standard. Some independent and reliable evidence apart from the FRT search results or the lineup identification must link the suspect to the crime to establish probable cause.

Enrollment Databases

13. Enrollment Databases

The databases that agencies may search or access for FRT ("enrollment databases") should be subject to the following requirements:

- For law-enforcement databases — for example, booking photos — the LEA must ensure that, at least annually, the database is purged of images of individuals who have been released after criminal charges were dropped or dismissed, or who were acquitted of a charged offense

- For government, non-law enforcement databases — for example, department of motor vehicle image databases — the government agency sourcing the images must ensure that the public is provided explicit notice (such as conspicuous disclosures posted at public-facing agency offices and on agency websites) that law enforcement may use face recognition to search these databases for criminal investigations

14-A. Privately-Collected Enrollment Databases Permitted

Law enforcement agencies may use privately-collected and -managed enrollment databases.

Several members stated strong objections to the use of mug shot databases because of the biasing and self-fulfilling prophecy nature of their use. For this reason, a slight majority of NAIAC-LE members prefer privately collected enrollment databases because today, at least, they cast a wider net and are not limited to any particular population based on geography or prior interaction with law enforcement.

14-B. Privately-Collected Enrollment Databases Prohibited

LEAs may not use privately-collected and -managed enrollment databases, including those that contain images scraped from the public internet.

14-C. Privately-Collected Enrollment Databases Restricted
LEAs may use privately-collected and -managed enrollment databases, but the companies collecting and maintaining the enrollment database must meet specially designated data security standards.

Other Issues

15. Internal Affairs Investigations
LEAs may use FRT to conduct Internal Affairs investigations.

Comment: LEAs have a similar public safety interest in upholding strict ethical and professional standards, justifying a need to use video and photographic evidence when investigating complaints against their officers and civilian employees. FRT, therefore, should be used when needed to assist in identifying principal officers, witnesses, or other persons involved in internal affairs/professional compliance investigations, regardless of whether the agency investigation is of a criminal or administrative nature.

16. Community Caretaking
LEAs may use FRT to identify an individual who is incapacitated, cognitively impaired, or deceased for purposes related to community caretaking and unrelated to the criminal investigation of that individual.

17. Self-Study
LEAs may use FRT to conduct self-audits and counterfactual self-studies, i.e. to retrospectively study whether the use of FRT in a closed case could have led to a more fair or efficient investigation.

18. Testing
For all databases, including privately-owned or privately-compiled image databases, LEAs must ensure that the FRT continues to perform with high accuracy across the demographic groups present in real-world use.

19. Defense Access
For any case in which an FRT search was performed and a criminal proceeding commenced — whether or not the defendant was identified using FRT— LEAs

should disclose to the accused complete information about their use of FRT, including a copy of the FRT search results.

20. Data Retention

In any case in which FRT is used to identify an individual who is not thereafter the subject of a criminal investigation or a witness or victim in such an investigation (such as with the identification of unrelated bystanders), data or information regarding such an identification will be expunged to the extent practicable.

Several NAIAC-LE members support such a limitation to minimize the privacy invasions that use of FRT can engender, such as when the record of an individual's placement at a certain location or event (such as a protest) might constitute sensitive information.

ACKNOWLEDGEMENTS

We want to express our gratitude to the individuals and organizations who generously shared their time and expertise with the NAIAC and NAIAC-LE Subcommittee:

American Association for People with Disabilities
Maria Town

American Civil Liberties Union
Olga Akselrod

American Federation of Labor and Congress of Industrial Organizations
Brett Gibson and Eric Gottwald

American Federation of Teachers
Rob Weil

Asian Americans Advancing Justice
Emily Chi

Black in AI
Gelyn Watkins

Business Disability International
Susan Scott Parker

Center for Democracy and Technology
Alexandra Givens

Communications Workers of America
Dan Mauer

Creative Commons
Anna Tumadóttir

D.C. Police Department
Commander Matthew Fitzgerald

Department of Homeland Security
Jon McEntee

Department of Justice
Kathryn McKenzie

Department of Professional Employees
Michael Wasser

Federal Bureau of Investigation
Richard Vorder Bruegge

Greenlining Institute
Vinhcent Le

Hispanic Technology and Telecommunications Partnership
JudeAnne Heath

IndigiGenius
Mason Grimshaw

International Brotherhood of Electrical Workers
Erica Fein

International Federation of Professional and Technical Engineers
Faraz Khan

LatinX in AI
Laura Montoya

Lawyers Committee for Civil Rights under Law
Quinn Anex-Rios

Leadership Conference on Civil and Human Rights
Frank Torres

Los Angeles Police Department
Captain Anthony Espinoza

Montgomery County Police Department
Chief Marcus Jones and Lt. Sunyoung Kim

National Association for the Advancement of Colored People (NAACP)
Derrick Johnson, Patrice Willoughby, and Amalea Smirniotopoulos **(NAACP LDF)**

National Center for Missing & Exploited Children
Fallon McNulty

National Fair Housing Alliance
Lisa Rice and Nikitra Bailey

National Institute of Standards and Technology
Patrick J. Grother

New York Police Department
Chief Ruben Beltran

Peoples Tech Project
Hannah Sassaman

Prince George's Police Department
Chief Malik Aziz

Queer in AI
Carter Buckner and Arjun Subramonian

U.S. Black Chambers
Talisha Bekavac

UNIDOSUS
Laura MacCleery

Women in AI
Yang Cheung and Bhuva Shakti

ABOUT NAIAC-LE SUBCOMMITTEE

The Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee (NAIAC-LE) has the responsibility to make recommendations and provide advice on matters relating to the development, adoption, or use of AI in the context of law enforcement.

The Subcommittee was established in Section 5104 (e) of the National Artificial Intelligence Initiative Act of 2020. It is charged with providing advice to the President, through recommendations that will be considered by the full NAIAC, on a range of legal and ethical issues that will arise as law enforcement increases its use of AI tools. These issues include AI bias, data security, adoption protocols, and legal standards. (Section 5104 (e) (2).)

The Law Enforcement Subcommittee was established in the summer of 2023 and began its work in August 2023.

ABOUT NAIAC

The National Artificial Intelligence Advisory Committee (NAIAC) advises the President and the White House National AI Initiative Office (NAIIO) on the intersection of AI and innovation, competition, societal issues, the economy, law, international relations, and other areas that can and will be impacted by AI in the near and long term. Their work guides the U.S. government in leveraging AI in a uniquely American way — one that prioritizes democratic values and civil liberties, while also increasing opportunity.

NAIAC was established in April 2022 by the William M. (Mac) Thornberry National Defense Authorization Act. It first convened in May 2022. It consists of leading experts in AI across a wide range of domains, from industry to academia to civil society.

https://www.ai.gov/naiac/

###