To: Members and Staff, House Energy and Commerce Committee and Senate Judiciary Committee; DOJ Office of Justice Programs (OJP) and Civil Rights Division
From: Joel Sinchi
Date: 19 March 2025
Subject: Establishing Federal Guardrails for Facial Recognition Used in Suspect Identification

Decision Requested

Adopt a federal framework that conditions key DOJ law enforcement grants on agency compliance with three baseline requirements for facial recognition used in suspect identification: disclosure, accountability, and independent auditing, supported by standardized reporting to a federal public database.

Executive Summary

- Facial recognition is increasingly used to generate investigative leads and identify suspects, but its performance and downstream use can vary by demographic group and by operational settings, creating predictable civil rights and reliability risks.

- Federal oversight remains uneven. Major federal reviews document inconsistent agency policies and limited tracking of use, especially when officers access non-federal facial recognition services.

- Wrongful arrests linked to facial recognition illustrate a recurring failure mode: a low-quality match becomes a primary evidentiary basis without adequate corroboration, disclosure, or meaningful opportunity to challenge.

- Municipal bans and voluntary corporate policies create a patchwork that does not set a uniform floor for safeguards or accountability.

- This memo proposes a mechanism-grounded federal framework built on three pillars: (1) **disclosure** of facial recognition use and key limitations in investigative and court contexts, (2) **human accountability** with clear decision rights and supervisory sign-off rules, and (3) **independent auditing** tied to standardized performance metrics and documented workflows.

- Implementation should rely on DOJ grant conditions, a national reporting template, and an audit protocol aligned with NIST testing concepts and GAO findings about policy gaps and weak use-tracking.

Introduction

Facial recognition has moved from an experimental tool to a routine component of suspect identification in many law enforcement settings. Agencies use it to compare still images from surveillance footage against driver's license databases, mugshot repositories, or third-party face search systems. While proponents emphasize speed and investigative efficiency, federal reviews and empirical testing show that accuracy and error profiles are not uniform, and risks increase when systems are deployed on low-quality images, when thresholds are set aggressively, or when operators treat matches as determinate rather than probabilistic leads.

A small number of high-profile cases reveal a core governance problem: even if facial recognition is intended to generate leads, weak procedural controls can allow a match to drive arrest decisions without adequate corroboration, disclosure, and accountability. Investigative reporting and litigation around Detroit's use of facial recognition illustrates this failure mode and the downstream harm when safeguards are not in place.

Despite these risks, the United States has no uniform federal baseline for how agencies must document, disclose, audit, and supervise facial recognition when used for suspect identification. The result is fragmented governance: some cities ban use, some agencies self-regulate, and many jurisdictions operate without consistent transparency or auditable controls.

Scope of the Problem

1) Reliability and demographic performance variation

NIST testing has documented demographic effects in face recognition evaluations and provides a credible basis for requiring agencies to track thresholds, error rates, and operational settings. Separately, NIST's ongoing demographic effects resources underscore that false positive rates can differ across groups depending on algorithm and conditions, which matters when a false match can become a suspect lead.

2) Weak tracking and inconsistent policies across agencies

GAO reviews of federal law enforcement use of facial recognition document that agencies vary in how they use the technology and, critically, in whether they track employee use of non-federal face recognition systems. GAO has repeatedly recommended stronger tracking mechanisms and clearer policies and training.

3) Civil rights, transparency, and access-to-justice concerns

The U.S. Commission on Civil Rights has highlighted concerns about oversight, transparency, discrimination risk, and access to justice in federal use of facial recognition. These concerns support federal guardrails that treat facial recognition as a high-impact investigative tool requiring documentation and meaningful challenge procedures.

Current Approaches and Why They Are Not Enough

Municipal bans and local rules

City-level bans can reduce harm locally but cannot create a consistent national floor for safeguards, training, or auditability. Patchwork rules also complicate interagency coordination.

Voluntary corporate restrictions

Corporate pauses and policies are inconsistent and can change over time. They also do not govern how law enforcement uses systems after procurement, including how officers set thresholds, corroborate matches, or disclose use in court.

Stalled federal legislation and partial guidance

CRS analysis indicates active congressional attention to law enforcement uses of AI, including facial recognition, but policy remains incomplete and uneven.
BJA has provided a face recognition policy template, but template guidance is not a binding national baseline and does not ensure independent auditing or standardized public reporting.

Proposed Federal Framework: Three Pillars

Goal: Keep facial recognition available as an investigative lead tool while preventing it from becoming an unaccountable, error-prone pathway to wrongful arrest.

Pillar 1: Disclosure

Mechanism: DOJ conditions Byrne JAG and COPS grant eligibility on adoption of disclosure rules and reporting.

Minimum disclosure requirements:

1. **Case-level disclosure**: When facial recognition is used to generate a suspect lead, agencies must record it in the case file, including the source system, image quality notes, and match confidence score or rank where available.

2. **Court disclosure**: When a facial recognition lead materially contributed to probable cause or charging decisions, agencies must disclose use to defense and courts in a standardized format, including known limitations and steps taken to corroborate the match.

3. **Public transparency**: Agencies must publish an annual summary of facial recognition use for suspect identification, including volume of searches, databases used, and aggregate outcomes.

Why this is publishable: GAO's findings about inconsistent tracking and policy gaps make standardized documentation and disclosure a direct response to known federal weaknesses.

Pillar 2: Accountability

Mechanism: Grant conditions plus a required internal policy that draws clear decision rights and supervisory responsibility.

Minimum accountability requirements:

1. **Lead-only rule**: Facial recognition matches are investigative leads and may not be the sole basis for arrest or warrant application.

2. **Corroboration requirement**: Before a facial recognition lead can support probable cause, agencies must document corroborating evidence independent of the face match.

3. **Supervisory sign-off**: A trained supervisor must sign off on any warrant packet that relies on a facial recognition lead, attesting that corroboration and disclosure requirements were satisfied.

4. **Training and certification**: Personnel who run searches or interpret matches must complete annual training that covers limitations, demographic performance issues, thresholding, and known misuse patterns.

Why this is publishable: This pillar addresses the exact failure mode highlighted in prominent wrongful arrest reporting, where a weak match was treated as strong evidence without sufficient corroboration or procedural safeguards.

Pillar 3: Independent Auditing and Standardized Reporting

Mechanism: A national audit protocol tied to a federal reporting template, with independent audits required for agencies above a specified usage threshold.

Audit protocol minimums:

1. **Performance and threshold testing**: Agencies must test systems at operational thresholds and document false match rates and false non-match rates, with demographic breakdown where feasible and lawful, using NIST-aligned concepts.

2. **Workflow audit**: Auditors must evaluate the end-to-end workflow, including image intake quality controls, operator training, corroboration practices, and disclosure compliance.

3. **Use tracking**: Agencies must track and report officer use of non-federal facial recognition services, aligning with GAO recommendations.

4. **Incident reporting**: Agencies must report known false match incidents and corrective actions.

Public reporting system:

- DOJ OJP, in coordination with relevant civil rights offices, should maintain a National Facial Recognition Use Database containing agency annual reports and audit summaries, with appropriate redactions for ongoing investigations.

Implementation Plan

Year 1: Standards and templates

- DOJ OJP issues the reporting template and minimum policy requirements, drawing on GAO findings and BJA's existing policy template.
- Pilot with volunteer agencies that receive federal funds.

Years 2 to 3: Grant-linked adoption

- Byrne JAG and COPS grant eligibility requires compliance with all three pillars.
- DOJ publishes the first annual national database summary.

Year 4 and beyond: Continuous improvement

- Annual updates to the audit protocol as new testing evidence and incident patterns emerge.

Stakeholders and Anticipated Opposition

Supporters: civil liberties groups, impacted communities, and agencies that want clear operational rules and reduced liability.
Opposition: some agencies and vendors may object to administrative burden and transparency.
Response: the framework is designed to preserve investigative utility while reducing wrongful arrest risk and litigation exposure through standardized documentation and validated workflows.

Tone note: Replace the original "neutralize the opposition" phrasing with "address concerns" and "reduce liability and operational risk."

Conclusion

Facial recognition used for suspect identification is a high-impact investigative capability that requires a federal floor of safeguards. The most defensible federal approach is not a blanket ban, but a mechanism-grounded framework that conditions DOJ grant funding on disclosure, accountability, and independent auditing, supported by standardized reporting and transparent oversight. This approach addresses known performance variation, weak use tracking, and documented wrongful arrest pathways while preserving legitimate investigative uses.

Bibliography

1. National Institute of Standards and Technology (NIST). *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*. NIST Interagency/Internal Report (IR) 8280, 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf
2. National Institute of Standards and Technology (NIST). *Demographic Effects in Face Recognition (FRVT Demographics)*. NIST, updated resource. https://pages.nist.gov/frvt/html/frvt_demographics.html
3. U.S. Government Accountability Office (GAO). *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Track Employee Use of Non-federal Systems* (GAO-21-518), 2021. https://www.gao.gov/products/gao-21-518
4. U.S. Government Accountability Office (GAO). *Facial Recognition Services: Federal Law Enforcement Agencies Should Better Assess and Manage Technology Risk* (GAO-23-105607), 2023. https://www.gao.gov/products/gao-23-105607
5. Congressional Research Service (CRS). *Law Enforcement Use of Artificial Intelligence and Facial Recognition* (CRS Product IN12289), 2023. https://www.congress.gov/crs-product/IN12289
6. U.S. Commission on Civil Rights (USCCR). *Civil Rights Implications of Federal Use of Facial Recognition*. Report release page, 2024. https://www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial
7. Bureau of Justice Assistance (BJA). *Face Recognition Policy Development Template for Use in Criminal Justice Agencies*. U.S. Department of Justice. https://bja.ojp.gov/doc/face-recognition-policy-development-template.pdf
8. Hagerty, Jon, and Drew Harwell. *A Flawed Facial-Recognition System Sent This Man to Jail.* Wired, 5 August 2020. https://www.wired.com/story/flawed-facial-recognition-system-sent-man-jail/
9. Harwell, Drew. *Face Recognition Played a Role in the Robert Williams Arrest. Was It Reliable?* The Washington Post, 13 April 2021. https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/
10. *AP News.* Reporting on Porcha Woodruff wrongful facial recognition accusation and context, 2025. https://apnews.com/article/detroit-facial-recognition-arrest-821d260e932a4582a6a912dd61fde157