REGULATING FACE RECOGNITION TECHNOLOGY

LEGISLATIVE CHECKLIST FOR CONGRESS

Congress is actively considering regulating police use of face recognition technology (FRT). If policing agencies are going to continue to use—or start using—this technology, such use must be subject to carefully-considered regulatory guardrails. This document provides federal lawmakers with an outline of minimum legislative requirements to guide the development of a comprehensive regulatory framework for the most common law enforcement use of FRT: attempting to identify a witness, victim, or person suspected of committing a crime from an image, or "investigative face identification." (This framework does not permit authorizing the use of FRT on live or recorded video footage for surveillance.) Although lawmakers may decide to exceed this checklist, everything in it is essential.

I. DEMOCRATIC AUTHORIZATION

1. Use of FRT by law enforcement should be banned unless authorized by a democratically-accountable body.
2. Legislation should require that states centralize all FRT use in a single state agency.
    a. If individual agencies are permitted to use FRT, such use must be approved specifically by the local democratically-accountable body.
3. Legislation should authorize FRT only for a limited pilot period.
    a. During this time, FRT's impact on public safety—both its advantages as well as its harms and risks—should be evaluated, with opportunities for community feedback, before continued use is authorized.
    b. Absent explicit re-authorization by the original authorizing body, FRT use should not be permitted beyond the pilot period.

II. TRANSPARENCY AND DATABASES

4. Require specific legislative authorization for the databases that agencies may search or access for FRT ("enrollment databases").
    a. If non-law enforcement databases are authorized—for example, department of motor vehicle image databases—the public should be provided explicit notice (such as conspicuous notices posted at public-facing agency offices and on agency web sites) that law enforcement may use face recognition to search these databases for criminal investigations.
5. Require that, at least annually, any law enforcement databases used for FRT searches are purged of images of individuals who have been released after criminal charges were dropped or dismissed, or who were acquitted of a charged offense.
6. Prohibit policing agencies from conducting FRT searches on any enrollment database composed of privately-owned images, including but not limited to any enrollment database that contains images scraped from social media platforms.
7. Require that any policing agency that uses FRT has and makes public a comprehensive use policy, developed with an opportunity for public review and comment.
8. Require that agencies track complete details of FRT use in each individual case and include this information in the case file.
9. Require that agencies publish, at least annually, a report summarizing their FRT use, including aggregated data tracked for individual cases (see #8).
10. Require that agencies conduct and make public annual audits of their use of FRT, including demographic breakdowns by race, ethnicity, gender, and age of searches conducted, to ensure use complies with all applicable laws and policies.

III. TESTING

International standards and best practices recommend three types of testing for FRT systems—each serving a distinct purpose: (1) technology testing to assesses how well the FRT algorithm performs; (2) scenario testing to simulate a real-world use case; and (3) operational testing to assesses an FRT system as it is actually deployed in the real world. To facilitate this:

Congress should direct and empower the National Institute of Standards and Technology (NIST) to:

11. Develop a version of its benchmark tests that implements the following four key changes:
    a. Evaluates FRT algorithms actually sold to law enforcement;
    b. Evaluates surveillance cameras images as well as other images commonly used by law enforcement;

c. Searches demographically-representative, larger enrollment databases; and

d. Reports error rates disaggregated by demographic groups.

12. Develop a scenario testing program that simulates common law enforcement investigative uses in order to provide insight into potential sources of error for these applications and to inform guidelines for real-world use.

13. Develop an operational testing protocol that agencies can use to assess how effective, equitable, and accurate their FRT systems are when actually deployed.

14. Require that agencies only procure FRT from a vendor that the appropriate administrative body determines, using results from NIST's technology testing on low-quality probe images, has demonstrated high accuracy across the demographic groups present in real-world use.

WHAT IS NIST?

The National Institute of Standards and Technology (NIST), housed in the U.S. Department of Commerce, is the nation's leading physical sciences laboratory. Its mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology."

For the past two decades, NIST has led federal government efforts to develop standards for emergent biometrics and artificial intelligence technologies. As part of this work, NIST has created benchmark evaluations of face recognition algorithms. Its expertise and experience with technical assessment of face recognition systems is unrivaled.

15. Require at least annual testing of FRT systems as actually deployed—operational testing—to ensure low real-world error rates.

    a. Results should be made available publicly in concise, clear, and accessible language to enable review by a nontechnical audience and with the context necessary to understand the relevance and any limitations of these assessments.

    b. This testing should be conducted either by independent, expert third-party testers (such as a biometrics testing lab or qualified academic lab) or according to a legislatively-approved testing protocol developed by independent experts.

IV. OFFICER TRAINING

16. Require that all individuals who review, analyze, use, and interact with the FRT system(s) receive specialized training on the capabilities and limitations of this technology generally and the particular system(s) in use.

17. Require that FRT results be subject to review by a trained human-in-the-loop before a possible match can be determined.

18. Develop and incentivize the adoption of national training standards for individuals who review and analyze the results returned by face recognition algorithms, (commonly referred to as the "humans-in-the-loop") before those results are shared with investigators.

V. PROCEDURAL AND CATEGORICAL LIMITS

19. Limit FRT searches to the investigation of serious felony crimes or to identify deceased, incapacitated, or missing persons.

20. Ban FRT:

    a. For use in criminal investigations to identify suspects who are minors;

    b. For surveillance—i.e., using real-time or stored video to track, observe or analyze the movements, behavior, data, or actions of an individual or groups of individuals.

21. Require an "investigative" warrant before an FRT search is initiated for criminal investigations, showing that there is probable cause to believe the unidentified person in the probe photo is involved in one of the uses for which FRT is authorized.

22. Require a court order before an FRT search is initiated to identify deceased, incapacitated, or missing persons.

23. Prohibit FRT search results from being considered positive identification or used to establish probable cause for an enforcement action.

24. Absent exigent circumstances, before arresting an individual identified based on FRT, require that law enforcement obtain an arrest warrant or court order that confirms, in addition to all other existing legal requirements, that all FRT statutory and policy requirements have been followed.

VI. DISCLOSURE TO THE ACCUSED

25. For any case in which an FRT search was utilized and a criminal proceeding commenced—whether or not a suspect was identified using FRT—require agencies to disclose to the accused, including prior to plea negotiations, complete information around their use of FRT. Such a provision should include meaningful remedies for failure to comply.

VII. VENDOR REQUIREMENTS

Authorizing legislation should require that vendors:

26. Disclose documentation and information about their FRT systems sufficient to enable independent, expert assessment of their FRT systems' performance for intended law enforcement use cases.

27. Ensure their FRT products are self-auditing, i.e., are built with sufficient capabilities such that law enforcement can fulfill all tracking and reporting requirements.

28. Provide 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.

29. Provide law enforcement agency 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.

VIII. ENFORCEMENT

30. Legislation should include meaningful enforcement mechanisms for statutory violations, such as:

    a. **Civil actions** for damages for any person injured as a result of an individual or agency's violation.

    b. **Injunctive relief:** The Attorney General should be empowered to prohibit an agency from using or acquiring any FRT systems, or FRT data where necessary to stop ongoing violations or to prevent future violations.

    c. **Administrative remedies:** Violation by an employee of a law enforcement agency should be grounds for termination, demotion, or any other appropriate consequences.

    d. **Exclusion:** Results from unauthorized use and evidence derived therefrom should be excluded as evidence in any trial, hearing, or other judicial or administrative proceeding.