BIOMETRIC TECHNOLOGY REPORT

Submitted in fulfillment of Section 13(e) of Executive Order on *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* (EO 14074)

U.S. Department of Homeland Security

U.S. Department of Justice

White House Office of Science and Technology Policy

December 2024

Executive Summary

Biometrics—automated recognition of individuals based on their biological and behavioral characteristics—are an important, and often critical, tool for the Nation's law enforcement (LE) community. Biometrics afford law enforcement officers a powerful means to help find missing children, fight human trafficking, and conduct investigations involving criminals and terrorists. Whether to support field, investigative, or custodial LE activities – on the web or in person – biometrics, and the systems that support them, provide tangible benefits to the public. However, LE use of biometric systems also has raised concerns about the impact on equity, privacy, civil rights, and civil liberties.

Like any technology, biometric systems must be continually informed by the latest and best science to optimize benefits, accuracy, and efficiency for the public's rights and privacy. Adjudication of biometric results must not discriminate based on actual or perceived race, ethnicity, national origin, religion, sex (including sexual orientation and gender identity), or disability. Accordingly, guardrails to protect civil rights, civil liberties, and privacy are vital.

So too is accuracy and impact testing which evolves amongst international standards-making bodies and the organizations leading those efforts within the U.S. Government. For years, the Departments of Homeland Security (DHS) and Justice (DOJ) have worked with these standards-making bodies, to modernize and improve image and testing standards, for example. On the policy side, significant effort has been made to put proper guardrails in place such as using only algorithms that meet high accuracy in testing, applying finely tuned due diligence processes and procedures, and protecting biometric information both prior to and during system implementation.

This report provides a major public review of biometric technologies employed by the DHS and DOJ. Produced in collaboration with the White House Office of Science and Technology Policy, this document explains the historical context and authorities under which biometrics are deployed; provides a description of four major biometric modalities, including their accuracy and prevailing standards; offers an overview of LE biometric programs at DHS and DOJ, including use cases, identity management systems, and implementation processes; conducts an analysis of stakeholder views on federal biometrics; and finally, defines a set of clear best practices and guidelines for biometrics use by Federal, State, Local, Tribal and Territorial (FSLTT) LE partners. The best practices focus on the use of facial recognition technology (FRT); other biometric technologies, like DNA, iris, and fingerprint already have a substantial body of detailed guidelines on use which are outlined in Section V.

Required by Executive Order (EO) 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*, this report's information and recommendations advance the EO's goals of increasing transparency and trust between LE entities and the communities they serve, while making policing safer and more effective.

Best Practices

In fulfilling a mandate of EO 14074, this report enumerates best practices for biometric technology use, offered as recommended guidance to our FSLTT partners. Guidelines for each best practice are found in Section IV Chapter 7.

In addition to the best practices specific to FRT, DOJ and DHS refer FSLTT law enforcement agencies (LEAs) to the widely accepted standards and best practices for use of DNA, iris, and fingerprint systems, available in Section V of this report.

For FRT, the best practices for FSLTT LEAs include:

- **In LE investigations, FSLTT LEAs should use FRT identification candidate results only as an investigative lead and not as the sole basis for identification or probable cause.**
- **Where multiple FRT candidate results are returned, FSLTT LEAs should manually review top candidate results from a candidate list before focusing on one candidate result for further investigation.**
- **FSLTT LEAs should prohibit the use of FRT probe photos or other biometric data captured in violation of existing laws and policies, as well as Artificial Intelligence (AI) models known by the agency to be trained on photos or biometric data captured in violation of existing laws, Federal government guidance, or agency policy.**
- **FSLTT LEAs should retain detailed internal logs of FRT system use for auditing and compliance with existing requirements.**
- **FSLTT LEAs should specifically articulate the authority that permits the capture of FRT biometric data or associated personally identifiable information, which should be reflected in public documentation whenever possible.**
- **FSLTT LEAs should have minimum quality criteria for input biometric data used for FRT systems, which should align with existing standards set by independent testing and standard-setting bodies.**
- **FSLTT LEAs should have strict criteria to govern the acceptable use of FRT systems in investigations—considering factors such as the nature of the investigation, the likelihood of generating a true match, and the testing and evaluation performance of the particular FRT system and relevant data—and should document these in public policies and procedures whenever possible.**
- **FSLTT LEAs should require documented technical and policy training for agency personnel who will use FRT systems. For FRT systems, that should include training on interpreting similarity scores displayed by a system and the adjudication of results.**
- **FSLTT LEAs should have policies and procedures in place to address the improper use of a FRT biometric system. Agencies should have consequences for improper**

uses of a biometric system, such as terminating system access in cases of intentional misuse.

- **When employing FRT systems that use AI, SLTT LEAs are strongly encouraged to follow applicable Federal guidance and prevailing scientific standards for appropriate, equitable, and fair use of FRT.**
- **FSLTT LEAs should minimize the risks of automation and confirmation bias for users through the configuration of systems and policies and procedures governing use, such as by carefully considering the benefits and risks of FRT systems that present similarity scores on candidate results for identification searches.**
- **FSLTT LEAs should ensure FRT systems have a minimum similarity threshold for candidate results, which may vary depending on a variety of criteria and should only be overridden in exigent circumstances.**
- **FSLTT LEAs should have policies in place to prohibit the use of commercially available FRT biometric systems that have not been approved by the agency for use.**
- **FSLTT LEAs should specify—and disclose in public documentation whenever possible—any independent assessments and benchmarks of FRT systems, which should be measured using standardized methodologies in as close to an operational context as possible.**
- **FSLTT LEAs should implement existing accredited and International Organization for Standardization-recognized standards for FRT biometric systems and data.**
- **FSLTT LEAs should disclose information about their use of FRT systems in publicly available documentation, including the type of FRT system and general purpose of use, whenever possible.**
- **FSLTT LEAs should retain system performance documentation and testing results about the FRT systems sufficient to allow for independent evaluation and/or auditing and should require technology vendors to provide the testing and evaluation results for the system version that is procured by agencies, not results for a previous or adjusted versions of the system.**
- **Federal agencies should have testing and evaluation requirements for SLTT grantees for grants that fund the procurement or development of FRT and other biometric systems and should require that SLTT grantees follow applicable Office Management and Budget M-24-10 requirements, as appropriate.**

Preface

The Department of Homeland Security (DHS), the Department of Justice (DOJ), the White House Office of Science and Technology Policy (OSTP), with support from the Executive Office of the President, publish this report in response to **Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, Section 13(e), Ensuring Appropriate Use of Body-Worn Cameras and Advanced Law Enforcement Technologies** (EO 14074). Pursuant to the requirements set forth in the EO, this report satisfies the EO's mandate that "the Attorney General, the Secretary of Homeland Security, and the Director of OSTP…jointly lead an interagency process regarding the use by Law Enforcement Agencies of facial recognition technology, other technologies using biometric information… as well as data storage and access regarding such technologies."[1] The interagency process considered the impact facial recognition technology (FRT) and other biometric technologies have on privacy, civil rights and liberties, and disparate treatment of individuals in federal law enforcement (LE) contexts. This report provides guidance to federal, state, local, tribal, and territorial (FSLTT) law enforcement agencies (LEAs) who use, or seek to use, biometric technologies and articulates this guidance as a set of best practices and guidelines.

In response to the EO's mandate, senior officials from DHS, DOJ, and OSTP worked together to provide guidance in line with EO 14074's goal that "our criminal justice system … respect(s) the dignity and rights of all persons and adhere(s) to our fundamental obligation to ensure fair and impartial justice for all." This interagency group focused on the EO's direction to ensure that "law enforcement technologies do not exacerbate disparities based on … actual or perceived race, ethnicity, national origin, religion, sex (including sexual orientation and gender identity), or disability" by assessing how federal law enforcement implements, tests, reviews, and uses designated biometric technologies in line with privacy, civil rights, and civil liberties. Protecting Americans' privacy, civil rights, and civil liberties is critical to the effective administration of justice in the United States and equitable LE activity more broadly. Therefore, law enforcement's use of technology—including FRT and other Artificial Intelligence (AI)-enabled biometric tools—must always respect these values and adhere to the highest ethical standards and constitutional principles.

As public servants, law enforcement officers (LEOs) should employ FRT and other biometric tools responsibly, respect the public's rights, inspire public trust, and ensure public safety. This report's working group contained representatives from DHS and DOJ, and included experts from each Department's LE components, policy, privacy, civil rights/civil liberties, and science and technology offices. DHS and DOJ align our technology use cases with authoritative sources and related privacy and transparency activities to ensure that we not only seek the highest quality of accuracy in our deployments but that they are properly prescriptive to minimize unnecessary and unintended consequences on the communities served by federal LEOs. The report relates due diligence efforts as well as the continuum of testing improvements to minimize potential issues of demographic differentials, including efforts to develop algorithms that directly address Executive Order 14074 concerns pertaining to demographic differentials (referred in the order as "disparate impact.")

The working group consulted with biometric subject matter experts on the science of biometrics; authorities on privacy, civil rights, and civil liberties; and the DHS and DOJ LE components that use these technologies to advance their missions. The working group also met with relevant technical providers, academic thought leaders, and advocacy voices to assure their concerns were understood and given serious consideration. This process included coordination and consultation with the Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee (NAIAC) within the National Institute of Standards and Technology (NIST). The working group also engaged relevant civil society organizations: DOJ issued a solicitation for public input specific to this report and a listening session was held with interested civil society groups. This report summarizes these multiple stakeholder inputs.

Contents

Figures

SECTION I: FUNDAMENTALS

1. Scope and Issue Statement

Assuring identity across the federal LE community is critical to denying fraud and anonymity to criminals, terrorists, and organizations that are a threat to public safety and national security. Biometrics are a vital tool to help make better identity decisions by determining if people are, or are not, who they say they are.[2] To prevent, uncover, and prosecute crime, LEOs have successfully used biometrics to identify missing children, fight human trafficking, identify victims and witnesses as well as missing and deceased persons, and locate criminals and terrorists. Beyond its applications for combatting crime and terrorism, biometrics also provide important benefits to the public by, for example, facilitating and expediting lawful travel and securing access to sensitive locations through identity verification.

At the same time, LEs use of biometric systems also has raised concerns about the impact on equity, privacy, civil rights, and civil liberties. The U.S. has various federal and state laws focused on issues related to privacy, as well as constitutional protections for freedom of speech and association; protection against unreasonable search and seizure; and due process rights protecting privacy, family, and intimate associations. FRT and other biometric technologies, if used irresponsibly or unjustly, may be inconsistent with the expression of these rights. Thus, it is imperative to ensure that any use of FRT and other biometric technologies is done in a way that respects peoples' rights, does not result in discriminatory outcomes, avoids re-enforcing historical injustice, and increases public trust in law enforcement.

DHS, DOJ, and other LEAs are entrusted to limit and guard the biometric information they capture, operate identity verification systems with high standards of accuracy, and protect civil rights, civil liberties, and privacy. Civil rights, civil liberties, and privacy are not only important, but essential to the integrity of any LEA biometrics use case. This responsibility is directly connected to the EO's important charge for LEAs to do more to strengthen trust with the communities they serve through transparent engagement that makes policing safer and more effective.

Thus, it is critical that LEAs use technologies that do not discriminate based on actual or perceived race, ethnicity, national origin, religion, sex (including sexual orientation and gender identity), or disability. Similarly, it is critical that LEAs have effective guardrails in place to plan, procure, implement, and maintain their biometric systems, including a strong framework of authorities, policies, privacy, civil rights, and civil liberties protections.

This report: (1) provides the origin story for the rapidly expanded use of biometrics based on 9/11 Commission facts and recommendations that were, at the time, specific to immigration but quickly permeated all LE activities; (2) reviews critical executive orders, key statutory authorities, and guardrails that currently are in place for biometric use by DHS and DOJ; (3) provides an overview of biometric technologies in use today by DHS and DOJ; (4) discusses DHS and DOJ operational use cases and identity management systems currently deployed, as well as the implementation process frameworks within which they are situated; (5) summarizes public comments received; (6) provides best practices and guidance for FSLTT LE partners; and (7) offers key information on additional technical specifications and standards for reference.

2. Historical Context of Biometrics in Federal Law Enforcement

9/11 Final Report Findings and Recommendations

The 9/11 Commission, formed in 2002 in response to public outcry over the U.S. government's failure to prevent the 9/11 attacks, focused on how the hijackers infiltrated the U.S. The Commission meticulously detailed how the hijackers exploited identity loopholes to repeatedly enter the U.S., stay undetected, and ultimately board the planes used in the attack. Had their identities been properly verified, the attacks might have been thwarted and thousands of lives could have been saved. The Commission highlighted the hijackers' efforts to conceal their intentions, prompting recommendations for enhanced identity practices, including biometrics, in DHS and DOJ activities.

The Commission concluded that better identity verification, particularly through biometrics, was crucial for public safety:[3]

> Since September 11, the United States has built the first phase of a biometric screening program, called US VISIT (the United States Visitor and Immigrant Status Technology program). It takes two biometric identifiers-digital photographs and prints of two index fingers-from travelers. False identities are used by terrorists to avoid being detected on a watchlist. These biometric identifiers make such evasions far more difficult.[4]

And lastly, recognizing that "no agency can do it alone," the 9/11 Commission insisted upon "unity of effort in sharing information." Executive Orders were written to create better information sharing that included direct reference to improved identity capabilities using biometrics, and Congress passed numerous statutes calling for biometric programs, especially at the border. Backend identity systems were funded by appropriations. The shift away from biographic-only identity information enabled DOJ to address terrorism and crime head-on and in more real time, and DHS to close the gap on the major border security gaps that the 9/11 Commission found during its immigration investigation of the 9/11 hijackers.

To be clear, the federal government has used fingerprinting systems since the start of the 20th century. For example, in 1999 the Federal Bureau of Investigation (FBI) implemented the Integrated Automated Fingerprint Identification System, or IAFIS, the first automated fingerprint system used for criminal justice purposes, replacing a fingerprint card system that had been used by policing for nearly the prior century. The first automated fingerprint system used for homeland security purposes was implemented in the 1990s to help support identification of persons repeatedly illegally crossing U.S. borders by the legacy Immigration and Naturalization Service (INS), at the time housed at DOJ. But it was the horrific events of 9/11 that set the course for the passage of the *Homeland Security Act of 2002* that created DHS with its critical mission of establishing an organized, national effort to protect and safeguard the homeland from threats to national security. This included moving the legacy INS into DHS with its various missions divided into DHS components. The establishment of DHS, alongside the findings and codification of the 9/11 Commission's *Final Report* recommendations, and implementation of the *Enhanced Border Security and Visa Entry Reform Act* of 2003, led to biometrics becoming a mainstay tool used by the entire U.S. government, including its LE functions, and eventually, in some American policing communities.

2.1 Key Authorities for DHS and DOJ Biometric Activities

In response to the 9/11 Commission recommendations, the federal government improved information-sharing through direct interoperability of national and homeland security information, including those pertaining to terrorists. This came in the form of implementing real time, automated identity management systems and attending watch lists, both of which were heavily based in biometric technology. To assure there was proper authority in place for such systems, and that bureaucratic processes were in place to check and balance these systems for issues pertaining to accuracy and privacy, for example, statutory authority was initiated specific to the biometric enterprise. This authority resides in the form of both EOs and statutory law, including direct appropriations in some cases, and supporting regulatory authority.

National Security Presidential Directive (NSPD)-59 is the backbone of these authorities, along with Homeland Security Presidential Directive (HSPD)-24. HSPD-24 gives DHS and DOJ the authority to capture, use, and manage biometric information to accomplish their respective missions. HSPD-24 delineates that the U.S. government shall build upon its success to identify, and screen, known and suspected terrorists and "other persons who may pose a threat to national security." While understood that biometric and biographic information may be captured for national and homeland security purposes, the purpose of this directive was to enhance capabilities to "use, in a more coordinated and efficient manner, all biometric information associated with persons who may pose a threat to national security, consistent with applicable law, including those laws related to privacy and the confidentiality of personal data."[5]

In 2017, National Security Presidential Memorandum (NSPM)-7, "Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans" sought to expand information sharing pertaining to identified threat actors with international, State, Local, Tribal, and Territorial (SLTT), and private sector partners "where support activities benefit national security." Building on other authorities, HSPD-24, coupled with NSPM-7 give executive authorities for the interoperability of the two primary LE-based identity management systems in the U.S. government, the FBI's Next Generation Information System (FBI NGI) and the DHS Automated Biometric Identification System (IDENT).[6]

The Privacy Act of 1974 pertains to all biometric activities and broadly applies to federal agencies that hold an individual's information in a record. A record means "any item of information about an individual that includes an individual identifier."[7] A system of records exists if "1) there is an indexing of retrieval capability using identifying particulars built into the system; and 2) the agency does, in fact, retrieve records about individuals by reference to some personal identifier." In fact, the *Privacy Act* drives much of the current implementation process for biometric programs throughout the U.S. government today.

Statutory Authorities for DHS Office of Biometric Identity Management (OBIM). Key authorities underpin DHS's interoperable biometric system, the Automated Biometric Identification System (IDENT), the Department's central, enterprise-wide biometric repository that compares, stores, and shares biometric and associated biographic information. The legacy INS created IDENT in the mid-1990s for the U.S. Border Patrol. After DHS was established in 2003, US-VISIT operated IDENT until 2013, when US-VISIT transitioned to become OBIM. Today, OBIM operates IDENT in support of about 45 stakeholders with LE and non-LE missions.[8] Section 205 of the *Visa Waiver Permanent Program Act of 2000* requires a biometric technology standard for the interoperable exchange of identity data.[9] The same standard-making entry-exit system requirement was repeated again in 2001 in Section 403(c) and 414 of the *U.S.A. PATRIOT Act* and included enabling the use of FBI fingerprint data to screen travelers seeking visas at U.S. consular posts overseas and at U.S. ports of entry.[10]

In 2002, Congress passed measures to assure "interoperable LE and intelligence data system with name-matching capacity" and emphasize the use of biometrics for traveler screening in the *Enhanced Border Security and Visa Entry Reform Act of 2002*.[11] Congress passed Section 7208 of the *Intelligence Reform and Terrorism Prevention Act of 2004*,[12] amending *The National Security Act of 1947*, again requiring a biometric entry and exit data system and repeating many of the requirements for an integrated entry and exit system amongst the U.S. government enterprise. In 2007, biometrics were to be compared against "relevant watch lists" in certain instances per Section 711(d) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, again reinforcing the requirements of interoperability and reliable underlying identity data.[13]

Within DHS, the policies addressing biometrics, identity, or personal identifying information provide guidance on its capture, use, storage, and management. Also addressed are consequences for inappropriate handling or disclosure of the information, or misuse or misapplication of procedures that result in a data breach. The consequences are based on the penalties found in the *Privacy Act of 1974*, as amended.

Statutory Authority for DOJ Federal Bureau of Investigation. The FBI use of fingerprints as an identification is compliant with the Attorney General's Guidelines for Domestic FBI Operations, [14] the Code of Federal Regulations (CFR), and additional federal laws, policies, and guidelines. FSLTT agencies that have connectivity to the NGI System are in compliance with the Electronic Biometric Transmission Specification[15] and the Criminal Justice Information Services (*CJIS) Security Policy,*[16] and have been issued an Originating Agency Identifier may utilize fingerprint-based identification through the NGI System, where authorized by federal and state law.

2.2 Privacy, Civil Rights, Civil Liberties, and Equity Context

Some stakeholders and advocacy groups have raised concerns about the impacts FRT and other biometric technologies may have on equity and privacy, civil rights, and civil liberties. The U.S. has various federal and state laws focused on issues related to privacy, as well as constitutional protections for freedom of speech and association; protection against unreasonable search and seizure; and due process rights protecting privacy, family, and intimate associations. FRTs and other biometric technologies, if used irresponsibly or unjustly, may be inconsistent with the expression of these rights. Thus, it is imperative to ensure that any use of FRT and other biometric technologies is done in a way that respects peoples' rights, does not result in discriminatory outcomes, avoids re-enforcing historical injustice, and increases public trust in LE.

Historically, with respect to some FRT systems, academic and federal government research documented some disparities in FRT performance across certain demographics, including race, gender, and disability. Evaluation of more recent FRT systems demonstrates that many have significantly curtailed demographic-based disparities. As biometric technology continues to develop and become more common, certain applications and use cases may raise different privacy and equity concerns depending on the context. Consequently, a set of standardized best practices assists in minimizing inaccuracies based on erroneous interpretation of results, lack of training, or other factors. Public access to information about FRT systems is integral to public trust in the responsible LE use of FRT.

2.2.1 Protections for Civil Rights and Civil Liberties at DHS

The DHS Office for Civil Rights and Civil Liberties (CRCL) supports the Department's missions while preserving individual liberty, fairness, and equality. Pursuant to statutory authorities, DHS CRCL is responsible for assisting the Department in developing, implementing, and periodically reviewing policies and procedures to ensure the protection of civil rights and civil liberties and that those

protections are appropriately considered in all aspects of operations, including in programs using biometric technologies.

In so doing, DHS CRCL influences DHS policies and programs throughout their lifecycle. For example, when deploying biometric systems, civil rights, civil liberties, and privacy must be integrated into their foundations and designing such systems with civil rights considerations from the beginning avoids the difficult task of retrofitting complex systems. Early engagement in the process gives everyone the maximum time possible to identify the issues and develop appropriate mitigation strategies.

Successful and appropriate use of biometric technology requires ongoing oversight and quality assurance, initial validation, and regular re-validation, and a close relationship between the users and oversight offices. DHS CRCL has been, and continues to be, engaged with DHS Components and Offices to ensure that DHS use of biometric technologies, including face recognition, is consistent with civil rights and civil liberties law and policy. For example, CRCL participates in DHS enterprise-level groups working on biometric and face recognition issues, such as the DHS Biometric Capabilities Executive Steering Committee which provides coordination and guidance to all DHS and Component-level programs that are developing or providing biometric capabilities in support of DHS mission objectives and serves as a forum for cross-Department collaboration. DHS CRCL provides advice and oversight to the Department's efforts to ensure these technologies work to reduce the potential for racial, ethnic, or gender bias, and other types of discrimination. DHS's commitment to nondiscrimination in LE and screening activities remains an important cornerstone of the Department's daily work to secure the homeland and informs its adoption and use of these technologies.

DHS CRCL also monitors operational execution and engages with stakeholders to provide feedback to Department and Component leadership regarding the impacts or consequences of policies and programs, including but not limited to, minimizing bias in operational use, and safeguarding individuals against impacts based on protected characteristics.

Finally, DHS CRCL investigates complaints and makes recommendations to DHS Components, often related to the creation or modification of policies, or changes to implementation, training, supervision, or oversight. Such complaints include allegations of racial profiling or other impermissible bias.

3. Biometric Technologies

This chapter provides an overview of the four biometric modalities within scope for this report: face recognition, fingerprint, iris, and DNA. This information was developed in consultation with the top scientists in the U.S. government who lead international standards making, including at National Institute of Standards and Technology (NIST); research, test and evaluation specialists at DHS's Maryland Test Facility (MdTF); and lead biometric engineers at DHS and DOJ. These technologies are first described, followed by information on how they are used by DHS and DOJ, including how biometric data is tested, evaluated, and maintained to fulfill statutory requirements for assuring the identity of those that pose a criminal or terrorist threat to the U.S., seek immigration or other federal benefits, or enjoy improved or expedited trade and travel programs. The chapter also describes how multi-modal biometric technologies improve identification and verification and therefore increase overall system performance, useability, and accessibility.

3.1 Biometric Technologies Overview

A biometric characteristic is a biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition. There is not one biometric mode that is best for all use cases, nor necessarily available or appropriate. Societal and human factors, in addition to technical capability and business justification, require consideration when undertaking the inclusion of a new biometric algorithm into an existing identity management system, or setting up an identity management system. An Automated Biometric Identification System (ABIS) may house one or more biometric modes, or algorithms. An ABIS requires an initial enrollment, the extraction of features, and creation and storage of a template that is then used for comparison and potential match. ABIS include data quality procedures and access criteria to assure that only appropriate information is shared with appropriate stakeholders, security and interoperability standards are in place, thresholds are set for accuracy when appropriate, accuracy is routinely tested, and algorithms upgraded as budgets and innovation allow.

It is important to understand the differences between verification and identification terms used in this report, and as understood by the International Organization for Standardization (ISO).[17] *Verification* is a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. In LE functions, *Verification* is less used than *Identification,* the task where the biometric system provides a candidate list to human reviewers and then examiners, to determine the identity of an individual as an investigatory lead. It is *Identification* that federal LE uses most often.[18]

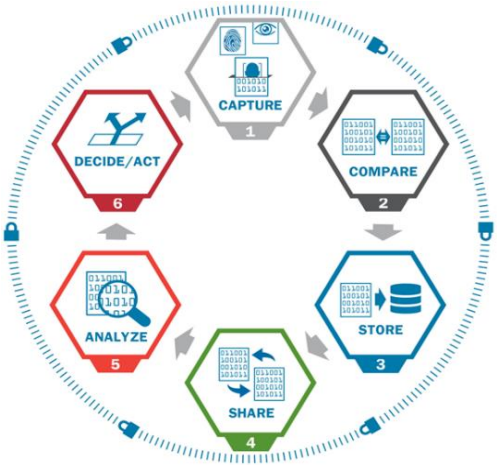

Figure 1 - Biometrics Continuum

Biometrics technology is a support capability used to assist LE in meeting its mission goals and objectives. The capture or use of biometric technology is not an

end in of itself, nor does it replace the underlying missions of LEOs. Whether biometrics are used or not, the missions—and the need to identify individuals—do not change. The use of biometric technology can complement associated capabilities, such as biographic, contextual, and forensic data, as an important element of a broader suite of identity-related capabilities. In LEOs that use biometrics such as DOJ and DHS, the intended purpose is to establish or verify an individual's identity through biometrics to enable faster and more accurate operational front-line decisions – identifying missing and deceased persons or witnesses and perpetrators of a crime, for example. As shown in Figure 1, the overall biometric process can be represented as a continuum biometrics concept of operation: the capture, comparing, storing, and sharing of those biometrics; analysis to confirm biometric comparison results or review additional associated information; and ultimately, a decision or action taken by a LE decision maker about an individual.

3.2 Facial Recognition Technology

3.2.1 Basics

FRT replicates the process of human face recognition through the development and use of an algorithm that models an image of a face as a set of stored biometric features. This set of biometric features is usually referred to as a "template." Automated FRT compares the mathematical similarity of two of these templates and returns a "match score" that reflects the degree of similarity between the two. It may be used in (1) one-to-one (1:1) *Verification* scenarios or in (2) *Identification* one-to-many "identification" and "investigation" scenarios. Millions of people around the world use 1:1 FRT every day for access control, such as to unlock their mobile phones or transit border crossings. In these scenarios, the user's live face image is converted to a template which is then compared to a stored template and a similarity score is generated.

In the other LE settings, the stored template comes from the photo taken upon booking, or in some federal LE border functions, from the passport or identity document used. In both cases, if the similarity score exceeds a threshold set by the system operator, a match occurs, and access is granted – by either unlocking the phone or allowing the traveler to pass. As a best practice, 1:1 FRT is not used by federal LE except for the limited purpose of identity verification during access control-oriented border entry and exit scenarios, or when moving individuals already in custody from one location to another either on intake or prior to release.

The primary difference between *Identification* and *Investigation* in the context of one-to-many search FRT is as follows:

> In the *Identification* scenario a threshold score is used in support of an automated system decision regarding whether the probe is verified/identified as a member of the gallery. In other words, if the comparison of the probe to any member of the gallery generates a similarity score above a given threshold, then a "match" is declared in human review.
>
> In contrast, as described below, in the *Investigative* scenario a threshold is not required, because the purpose of this search is to allow a human operator to review and compare candidates from the gallery to the probe image and determine to the extent possible whether any

candidate matches to the probe image for lead purposes. The candidates are organized for display to the operator in order based on the similarity score, regardless of whether those scores exceed a threshold or not. Some investigative systems will use a threshold score to restrict the number of gallery subjects returned to the user/operator, but this threshold has no impact on whether a specific gallery member is subsequently labeled as a lead.[19]

3.3 Fingerprint Recognition Technology

The fingerprint modality is one of the most long-established biometrics modalities. The basic structures or patterns that are used within fingerprint biometrics are arches, loops, and whorls. The permanent and distinctive arrangement of the features of this skin allows for the initial identification of an individual.

Prints are captured, stored, retrieved, and shared using a variety of devices and systems. Databases can store millions of prints and provide either one-to-one (verify), or one-to-many (identify) comparisons. Comparison response times vary relative to gallery size and system capabilities with some organizational requirements in the sub-15 second range. Watchlist comparison in the field using handheld devices or laptops is sub-5 minutes.

3.3.1 Basics

A contact print is one that has been proactively taken with a biometric device with the fingerprint touching the device to control light, friction, and finger curvature. Some devices take all ten fingerprints, and others rely on two, depending on the use case. Most criminal justice use cases take ten contact prints at booking stations, and latent prints for forensic instances, while in the field handheld devices are generally used. Each digit is designated by the software as a different number. A latent print is the chance impression of the friction ridge skin of the fingers and/or palms of the hand on a surface. A latent impression is generally not visible to the naked eye and requires enhancement processing at a forensic lab.

Contactless biometric devices take an image of a fingerprint without touching a screen and are useful especially in cases of high volume or hygienic concerns. However, without standards in place that enable contactless fingerprints to be compared to contact finger enrollments, contactless fingerprints technologies are not yet widely used.

3.4 Iris Recognition Technology

3.4.1 Basics

Iris recognition uses mathematical pattern-recognition techniques on images of the iris to map intricate structures of the iris that are unique to the individual for identification purposes. It is only in recent years that advances in imaging capture technologies and processing power have enabled accuracy rates sufficient for wider use. The FBI has an iris system (see Section V),[20] but DHS has only partially operationalized iris recognition (see Section 5.1.1).

3.5 DNA Technology

3.5.1 Basics

DNA is distinct from biometric modalities in that it is not just an image, but actual physical matter. It thus requires a different type of architecture than traditional biometric identity management systems that contain face, finger, and iris, such as DHS OBIM IDENT and FBI NGI. As a result, DNA data is only stored by the FBI in its Combined DNA Index System (CODIS) system for criminal justice purposes as it requires a different type of architecture than traditional biometric identity management systems. Notably, DHS does not have a DNA repository. For LE investigations, DHS relies on external federal partners to test DNA and search CODIS. While DHS does not employ the Rapid DNA tool developed through a small business research collaboration, it supports states who seek to utilize this technology suite to identify deceased persons following disasters. This section describes the science of DNA technologies from the viewpoint of the top FBI DNA physical scientists and operators, and DHS S&T research scientists.

DNA is the genetic material contained in most of the cells in our bodies. The use of DNA for human identification rests on the premise that—apart from identical twins—all individuals have unique DNA sequences. Forensic DNA testing extracts and characterizes DNA from biological material captured from evidence and compares the resulting DNA profile to known individuals, such as suspects or victims of crime. Forensic DNA profiles can also be compared against databases containing the DNA profiles of known individuals.

While the majority (over 99.7%) of DNA is the same for all people, a small fraction of the total (0.3% or approximately 10 million base pairs) is different. Areas within this small subset of the genome, known to be highly variable among individuals, are examined during forensic DNA analysis. These locations (loci) are known as non-coding regions and do not code for any externally visible traits (e.g., hair color, skin color, eye color) and are not known to be associated with any medical conditions, traits, or predispositions for disease.[21] To promote consistency and facilitate comparisons between laboratories, a standard set of core loci (or markers) have been established.

A DNA profile (also referred to as a genetic profile) is simply a string of numbers collectively representing an individual's genotypes (complete set of genetic material) for all tested loci.

3.5.2 DNA Probabilistic Genotyping

The goal of DNA mixture interpretation is to determine the possible genotype combinations of contributors to a forensic sample. Binary (or manual) DNA interpretation methods applied data thresholds to determine possible genotype combinations. The simplicity of this approach allowed analysts to interpret DNA typing results without computer assistance. However, the binary approach had significant limitations because it could not account for the possibility of missing data (allelic dropout). Additionally, the amount of data available for statistical calculations was often limited, frequently resulting in inconclusive results.[22] Most notably, binary interpretation methods had limited utility when applied to low-level and complex mixtures obtained from trace DNA samples.

Probabilistic genotyping software (PGS) is a tool that assists DNA analysts in interpreting forensic DNA typing results. PGS applies the same principles used in manual interpretation of DNA evidence; however, as an automated computer-based approach it exceeds human capabilities. These programs, introduced into forensic practice over the past decade, combine biological modeling, statistical theory, and probability distributions to infer genotypes and/or calculate likelihood ratios (LRs) for forensic samples.[23] The resulting genotypes can then be compared to the profiles of known persons or searched in the (CODIS). PGS systems offer an advantage over binary interpretation methods since they can model various aspects of DNA behavior such as degradation, locus specific amplification efficiency, and DNA template amounts while also factoring in the probability of allelic dropout and/or drop-in. These capabilities address the inherent limitations of binary methods and make PGS ideal for the interpretation of complex DNA mixtures.

PGS is a significant advancement over the binary mixture interpretation as it produces much more informative results. Whereas the binary method considered all interpreted genotype combinations equally probable, probabilistic approaches provide a statistical weighting to the different genotype combinations.[24] Generally, this strengthens exclusionary support for non-contributors and inclusionary support for contributors. Moreover, probabilistic genotyping methods reduce subjective decision making by analysts, moving the discipline towards greater standardization.[25]

The scientific foundation of PGS is well-established and based on longstanding and widely accepted principles supported by a large body of peer-reviewed scientific literature.[26] PGS is well regulated, highly characterized, and extensively validated.[27] These factors establish the scientific basis and reliable application of PGS to aid DNA analysts in their interpretation of single-source and mixed forensic DNA samples. In the legal domain, PGS has been extensively evaluated and admitted into evidence by numerous federal and state courts across the nation.[28]

3.6 Multi-modal Biometric Systems

Automated outputs of biometric algorithms are improved when two or more biometric modalities are used together, increasing overall accuracy that a biometric is attributable to a correct identity. *Multi-modal biometric systems* use two or more biometrics results (fingerprint, face, iris, etc.) collectively to increase the overall comparison performance of authentication systems and reduce false acceptance rates.[29] Leveraging these traits for an authentication system enhances its robustness to intraclass variation and useability. To be clear, DNA is not used today in concert with other modalities, as it is a physical attribute in and of itself that requires different comparison and retention requirements than the imagery biometrics of face, finger, and iris. Thus, this multi-modal discussion does not include DNA.

Fundamentally, use of multi-modal biometrics provides significant benefits for larger scale identity management systems such as DHS IDENT and FBI NGI, providing both higher confidence verification and identification rates. With limited resources and long procurement cycles, it is difficult for the United States Government (USG) to reduce dependency on single modality biometrics and single vendors for each modality. However, it is well recognized by the federal LE community that multiple vendors for a single modality, and multiple modalities fused together for a single result, are

highly valuable in increasing accuracy.[30] One 2019 DHS study found an 80% improvement in match scores when combining match scores of multiple vendors across different vendors on public datasets, with a significant impact on reducing false positives. Fusing face and finger match scores reduce the number of unimodal "undetermined" transactions by as much as 98%, saving a significant amount of time and cost from manual review.[31]

Usability and Accessibility. Multi-modal systems also have important usability benefits. Unimodal systems may limit participation for users who are unable to properly or consistently present samples for the specific modality. For example, a fingerprint only system may exclude certain users who have damaged their fingerprints, typical for manual laborers or hobbyists working with their hands. A multi-modal system provides one or more alternative biometric capture opportunities for a user to participate in the authentication system.

However, whether one or more modalities are available, biometric providers are required, as any technology provider, to comply with Section 508 of the *Rehabilitation Act of 1974* which requires that all electronic and information technology (IT) be accessible to people with disabilities. In the biometrics context, this means that hardware that enrolls a biometric through imagery, an issue most common with fingerprint devices, takes into account the loss of a friction ridge required for a quality image, loss of one or more fingers, or issues with capture such as fingers that are too wet or dry. Current software automatically notes if a particular sets of prints, or portions of prints, are unusable. The hardware itself must comply with standards that enable people at different heights to still retain access by moving the device up and down for individual comfort.

SECTION II: BIOMETRICS PROGRAMS AT DHS AND DOJ

4. DHS's Process for Implementing Biometric Activities

The figure below shows the DHS biometric capability implementation policy process that has existed for the past two decades and is currently in process of modification by the DHS Face Recognition Directive issued on September 11, 2023. (*See section 4.2.1*).

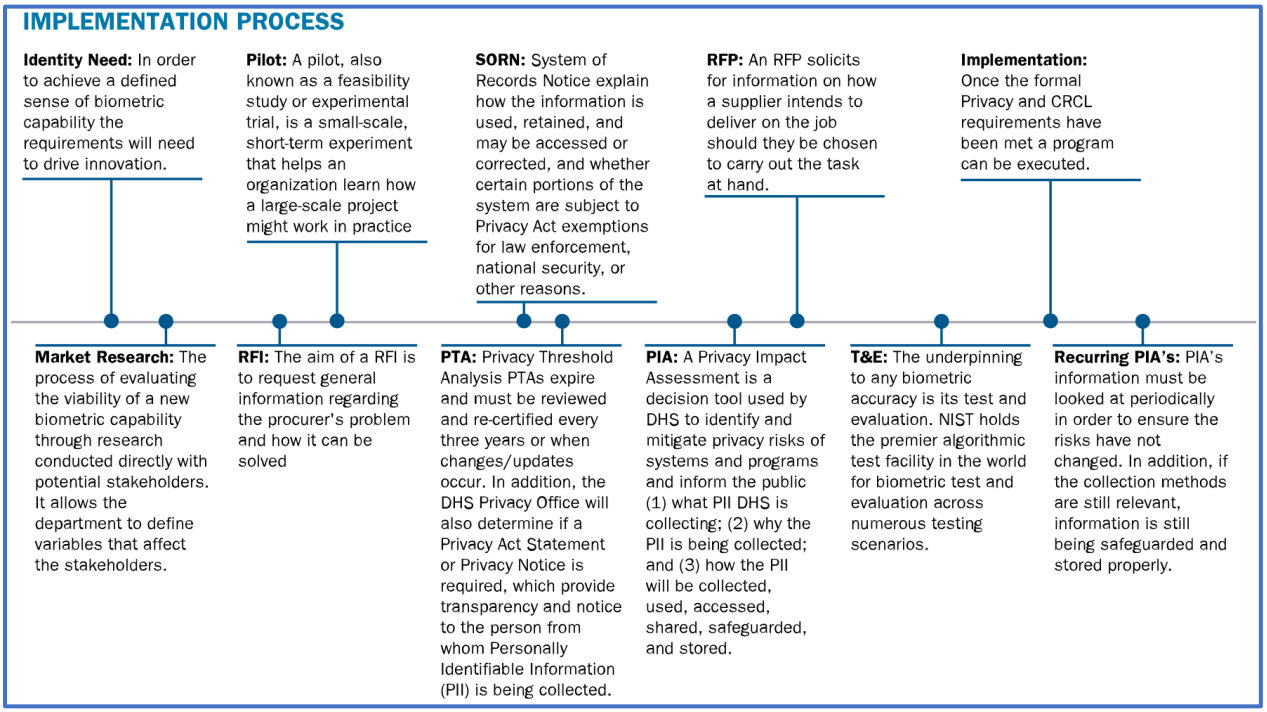

Figure 2 - DHS Biometric Capability Implementation Process

The process involves the following steps:

- An identity need is articulated and justified.
- Market research is conducted.
- Request for Information published.
- A feasibility study, or pilot, is conducted to determine how a large-scale project may operate.
- If pilot deemed feasible, a System of Records Notice (SORN) is published, including how data will be used and whether the Privacy Act applies.
- A Privacy Threshold Analysis (PTA) is submitted by operational components to the Privacy Office, to determine if a Privacy Impact Assessment (PIA) must be completed, with detailed information including identity information captured and biometric modalities used on what use case.

- A PIA helps determine if mitigation processes must be put in place by component and provides notice to the public of the biometric activity.
- Once the PIA is complete, the component may solicit with a Request for Proposal. DHS and DOJ both make clear that vendors must adhere to all privacy, security, and accuracy requirements in their solicitations.
- Once a vendor(s) is chosen and development has occurred to specified requirements, test and evaluation takes place.
- Upon implementation, Privacy and CRCL requirements are re-evaluated.
- PIAs are ongoing during the life of the program and must occur with any change in the use or expansion of a biometric capability.

4.1 DHS Biometric Activities

Since its founding, DHS operational components have implemented biometrics to support federal LE missions as well as FSLTT and international partners. Assuring who someone is, or determining who someone is, are core functions that only biometrics in tandem with other key data can reasonably assure. Backed by statutory authority and implemented policy and procedure focused on privacy and civil liberties, and in consultation with NIST and DHS Science and Technology Directorate (S&T), DHS components use biometrics both in singularity, such as face recognition in cybercrimes or in missing and exploited children's investigations, or multi-modal applications, such as face and finger in criminal investigations.

4.2 Overview of Recent DHS and DOJ Face Recognition Policies

Both DHS and DOJ have worked to address concerns with face recognition implementations by their LE (and other) components. This section reviews those activities.

4.2.1 DHS Face Recognition Directive

On September 11, 2023, DHS issued its *Use of Face Recognition and Face Capture Technologies* Directive and an attending Instruction to clarify implementation processes.[32] The Directive was nearly two years in deliberation and emphasizes DHS's careful implementation of face recognition and other biometric technologies. Its stated purpose is to establish a DHS-wide policy that covers all identification and verification face recognition use cases at DHS, including those where the face image is derived from another image or video, and in all face analysis cases where a human examiner is used.

Its scope is broad, covering all use cases for any purpose (not just LE); and includes technologies used by FSLTT government, non-U.S. government, and international entities operated by or on behalf of the Department. The Directive does include reference to NIST's responsibility to support biometric standard production, with a heavy emphasis throughout the Directive on performance testing.

The Directive also uses as an authoritative reference EO 14074, the same EO to which this report responds. It makes clear that the only permitted use cases at DHS are those enumerated by existing

law or policy. Future biometric activities require DHS Chief Information Officer (CIO) approvals, articulated policy support from the DHS Office of Strategy, Policy, and Plans, DHS Privacy, CRCL and DHS S&T testing before and every three years after deployment of identity management systems that use FRT. FRT used for identification may not be used as the sole basis for law or civil enforcement actions, or investigative leads, and all matches must be reviewed manually by human examiners prior to any actions taken, civil or LE.

Whereas previously a DHS LE component could engage independently with the Privacy Office and CRCL when procuring a biometric technology, as shown in Figure 2, the Directive now requires the additional DHS entities involvement or approvals prior to an implementation:

- Undersecretary for Strategy, Policy, and Plans: Establishes FRT policy and plans, leads development, acquisition, and implementation of FRT that is "operationally required and technically feasible;"
- CIO: Responsible for overseeing FRT and related infrastructure; oversees acquisition, management and implementation of FRT technologies;
- Science and Technology Directorate: Develops accuracy and performance metrics as well as procedures for testing FRT;
- Chief Privacy Officer: Responsible for all privacy and information disclosure in assuring "DHS sustains, and does not erode, privacy protections for the capture, use, retention, dissemination, or disclosure of personally identifiable information; and conducts all privacy assessments and privacy oversight of FRT;
- Office for Civil Rights and Civil Liberties: Conducts impact assessments and "ensures use… minimizes bias during operational use and safeguards individuals against disparate impacts based on protected characteristics;"
- Office of General Counsel: Makes sure authority exists for each use case;
- Component Head: (1) coordinates all FRT activities with the (CIO), in accordance with the Policy Office; (2) are fully authorized to proceed with FRT; (3) do not commit any privacy or civil rights and civil liberties violations; (3) are tested and evaluated prior to, and every three years thereafter, by S&T; and
- Chief Information Security Officer (CISO): Publishes and maintains security standards in accordance with law.

4.2.2 DOJ's Facial Recognition Technology Working Group and Interim Policy

In February 2022, in order to foster Department-wide consistency in the use of FRT and ensure effective internal controls, the Department of Justice launched the FRT Working Group, co-chaired by the Department's Office of Legal Policy (OLP) and the Office of Privacy and Civil Liberties (OPCL). The FRT Working Group, comprised of legal and operational subject matter experts from across the Department, met regularly throughout 2022 and 2023 to develop a policy to govern the use of FRT by Department components.

The FRT Working Group was tasked with developing an interim FRT policy with a framework centered on oversight, accountability, equity, and transparency. Announced by the Deputy Attorney General in December 2023, this interim FRT policy is consistent with recommendations from a September 2023 Government Accountability Office Report on Facial Recognition Services, as well as a mandate in the House Subcommittee for Commerce, Justice, Science and Related Agencies Appropriations Bill of 2022. The FRT Working Group continues to meet monthly to discuss next steps to promote successful implementation of the policy, including helping components develop their own policies and implement training.

The Interim Policy and Safeguards for FRT Acquisition and Use. The Interim FRT Policy prohibits unlawful use of FRT, provides guardrails to ensure effective and compliant use, and addresses the Department's FRT governance structure, including scope of FRT use, implementation, procurement, training, protection of privacy and civil rights, accuracy, the approval process for FRT use, accounting and reporting, and data retention.

The Interim FRT Policy requires that Department FRT systems be assessed for risk to accuracy across demographic groups, bias, and unlawful discrimination; that personnel using or approving FRT systems must receive required training on relevant legal and policy requirements; and that mandated training must include at a minimum, the terms of the Interim FRT Policy, the mandates of relevant privacy, civil rights, and civil liberties laws, and discussion of discovery obligations related to FRT use.

Notably, the Interim FRT Policy mandates that activity protected by the First Amendment may not be the sole basis for the use of FRT. This would include peaceful protests and lawful assemblies, or the lawful exercise of other rights secured by the Constitution and laws of the United States. Additionally, under this policy pursuant to the Department's anti-discrimination policies and other anti-discrimination laws, Department personnel "shall never use FRT to engage in or facilitate unlawful discriminatory conduct." Further, FRT systems must comply with the Department's policies on AI.[33] And "FRT results alone may not be relied upon as the sole proof of identity. An individual's identity must be confirmed through other analysis and/or investigation."

The Interim FRT Policy also requires any component that deploys FRT systems to develop a process to account for and track system use and provide an annual report to the Emerging Technology Board (ETB) and the Department's Data Governance Board. Without compromising law-enforcement sensitive or national security information, each of these annual reports will be consolidated into a publicly released summary on the Department's FRT use. OPCL will report to the FRT Working

Group, the ETB, and the Office of the Deputy Attorney General any complaints received through the existing privacy complaint process about use of FRT. These complaints will also be reported in the publicly released annual report summary.

In addition to the Interim FRT Policy, the Department has numerous policies that apply generally to the use of technology by the Department's components, including DOJ Order 0903, Information Technology Management, DOJ Order 0601, Privacy and Civil Liberties, and the Department's AI Strategy. Some components, like the Bureau of Justice Assistance (BJA) in the Office of Justice Programs, have developed guidance documents with participation and support from stakeholders, including privacy advocates. As just one example, the 2017 Face Recognition Policy Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities, which provides LE, fusion centers, and other public safety agencies a framework for developing face recognition policies that comply with applicable laws, reduce privacy risks, implement minimum required training for authorized users and examiners, and establish entity accountability and oversight. Also, specific to BJA's Edward Byrne Memorial Justice Assistance Grant (JAG) Program, the largest grant-making activity in the Department, BJA employs a special condition in its awards to states, tribes, and local government for funding FRT projects.[34]

Furthermore, in deploying new technology, all Department components–-including those involved in LE—must comply with all applicable constitutional provisions, laws, regulations, and established policies. For example, the use of FRT is subject to Section 208 of the *E-Government Act*, and certain information acquired or generated attendant to use of FRT is governed by the *Privacy Act*.

4.3 Privacy Compliance and Oversight at DHS and DOJ

4.3.1 DHS Privacy Compliance and Oversight

Since the inception of biometric activities, DHS Privacy Office compliance and oversight has been the key linchpin for the initiation and continued approval of biometric activities that assure that scope is defined and limited, and ongoing activities receive continuous oversight. Even with the FRT Directive at DHS, for example, the Privacy Office retains this pivotal role. This section reviews in detail what privacy activities take place at DHS and DOJ, as both are similar in that they fall under the *Privacy Act*, a statutory authority which, along with others previously described, conditions how the U.S. government operates its biometric programs.

Among the responsibilities of the DHS Chief Privacy Officer are that they assume primary responsibility for privacy policy, including: (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, capture, and disclosure of personal information; (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the *Privacy Act* [5 U.S.C. 552a]; (3) evaluating legislative and regulatory proposals involving capture, use, and disclosure of personal information by the Federal Government; and (4) conducting a PIA of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information captured and the number of people affected.

These responsibilities are detailed further in DHS Delegation 13001, Rev. 01, which includes in subsection (h): Coordinating with the CIO and CISO to provide guidance regarding information, information management (IM), (IT), and technology-related programs, and to develop and implement policies and procedures to personally identifiable information (PII) used or maintained by the DHS in accordance with federal law and policy, including responding to privacy incidents and breaches of PII (per Office of Management and Budget (OMB) M17-12).

DHS Privacy Office Proactive in Biometric Activities

Privacy Office subject matter experts participate—alongside counterparts from OCIO, OBIM, PLCY, and operational Components— in numerous Interagency Policy Committees (IPCs), sub-IPCs, task forces, working groups, interagency committees, tiger teams, and other bodies addressing the use of biometric information and artificial intelligence. Participation in such groups allows Privacy Office staff the opportunity to engage in policy development and become aware of potential use cases for which privacy compliance documentation may be lacking.

Figure 3 - Privacy Snapshot

All of the Chief Privacy Officer's authorities and responsibilities are agnostic to the nature of the technology, including how it is deployed, where it is deployed, and who within DHS employs the technology for the capture, use, maintenance, or dissemination of PII. As such, all biometric modalities—and the use of AI related to PII—are subject to DHS Privacy compliance and oversight processes.

Overview of the DHS Privacy Compliance Process. The Privacy Office assesses the privacy risk of DHS IT systems, technologies, rulemakings, programs, pilot projects, information capture, or forms, and develops mitigation strategies by reviewing and approving all DHS privacy compliance documentation. The privacy compliance process is an ongoing cycle with four key parts to ensure appropriate oversight: PTA, PIA, SORN, and periodic review.

1. **PTA**. The DHS Privacy Office reviews the PTA to determine if the system or program is privacy-sensitive and requires additional privacy compliance documentation such as a PIA or SORN. PTAs expire and must be reviewed and re-certified every three years or when changes/updates occur. In addition, the DHS Privacy Office will also determine if a Privacy Act Statement or Privacy Notice is required, which provide transparency and notice to the person from whom PII is being captured.
2. **PIA**. Required by the *E-Government Act of 2002*, the *Homeland Security Act of 2002,* or DHS Privacy policy, the PIA is a decision tool used by DHS to identify and mitigate privacy risks of systems and programs, and inform the public (1) what PII DHS is capturing; (2) why the PII is being captured; and (3) how the PII will be captured, used, accessed, shared, safeguarded, and stored. PIAs assess risk by applying the universally recognized Fair Information Practice Principles (FIPPs) to Department systems and programs. If a PIA is required, the program

manager will work with the Component Privacy Office to write the PIA for submission to the DHS Privacy Office for review and approval by the Chief Privacy Officer.

3. **SORN**. *The Privacy Act* requires that federal agencies issue a SORN to provide the public notice regarding PII captured in a system of records. SORNs explain how the information is used, retained, and may be accessed or corrected, and whether certain portions of the system are subject to Privacy Act exemptions for LE, national security, or other reasons. If a SORN is required, the program manager will work with the Component Privacy Office and Component counsel to write the SORN for submission to the DHS Privacy Office for review and approval by the Chief Privacy Officer.

4. **Periodic Review**. DHS practices a privacy continuous monitoring strategy in accordance with OMB Circular A-130, "Managing Information as a Strategic Resource," dated July 28, 2016. Specifically, DHS practices comport with guidance that—as part of an agency's risk management process, the appropriate privacy official should develop and maintain a privacy continuous monitoring strategy that should catalog the available privacy controls implemented at the agency across the agency risk management tiers. Further, DHS ensures that the privacy controls are effectively monitored on an ongoing basis, at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. DHS accomplishes these functions through implementation of DHS Directive 047-01, "Privacy Policy and Compliance," (July 7, 2011) and DHS Instruction 047-01-001, "Privacy Policy and Compliance," (July 25, 2011). To execute this requirement, the DHS Privacy Office uses the Privacy Compliance Artifacts Tracking System to ensure all outstanding privacy requirements and privacy documentation are completed, as appropriate. In addition, the Privacy Compliance Review (PCR) is both the process followed and the final document designed to provide a constructive mechanism to improve a program's ability to comply with existing privacy policy and compliance documentation, including PIAs, SORNs, formal agreements, such as Memoranda of Understanding or Memoranda of Agreement, or at the discretion of the Chief Privacy Officer. The objective of the PCR is to assess ongoing compliance with existing privacy compliance documentation and to make sure the privacy protections in the PIA are followed. The DHS Privacy Office Oversight Team can assess these protections and publish recommendations and commentary which are also made public for purposes of accountability. In the interest of transparency, unclassified PIA and all SORN documents are published online. Existing documents can be edited and reviewed to incorporate new technologies, new use cases, or revised understandings of a system's functions if appropriate, or new PIA/SORN documents can be written. Associated links between PIAs and SORNs are listed following a system's abstract to better facilitate public understanding of the interconnected nature of many systems. Abstracts are typically updated to reflect essential changes in a document's revision history.

Process For New Use Cases. All new technology use case or pilot proposals undergo the same process outlined above regardless of their content. A team of analysts is tasked with comparing the relative privacy risks of any new use case in the context of existing systems and applying the foundational concerns of the Fair Information Practice Principles. Through probing questions and multiple levels of peer review from stakeholders associated with the system, all risks to privacy are considered, assessed, and appropriately mitigated.

Targeted archival tagging of documents related to high-risk categories of PII—such as those related to biometrics and predictive algorithms—is consistently implemented to both provide:

- An accountability process for the historic tracking of grouped items of interest; and
- The ability to provide statistical summaries of work products related to those topics.

Additional oversight via legal review may be conducted to ensure that programs are not operating outside of the confines of existing law, and that plans for the storage, retention, or deletion of any personally identifiable data have been articulated and are in alignment with applicable retention and disposition schedules.

Examples of significant published PIAs related to biometric recognition considerations[35] within the LE scope of this report:

a. DHS/ALL/PIA-077 Biometric Interoperability Between DHS and DOJ - PIA allows an approved user to submit a single query and receive results from the US-VISIT Automated Biometric Identification System (IDENT) and the DOJ Integrated Automated Fingerprint Identification System (IAFIS).

b. DHS/ALL/PIA-095 International Biometric Information Sharing Program (IBIS) - PIA supports DHS Components and foreign partners in assessing the eligibility or public security risk of individuals seeking an immigration benefit in the context of a border encounter or LE investigation related to immigration or border security issues.

c. DHS/ICE/PIA-050 Rapid DNA Operational Use - PIA describes deploying Rapid DNA technology as a factor to determine if removable noncitizens who represent themselves as a noncitizen in a family unit (NFM), or noncitizen encountered as part of a family unit when apprehended by DHS do, in fact, have a bona fide parent-child relationship (pilot no longer in operation).

d. DHS/OBIM/PIA-001 Automated Biometric Identification System - PIA details the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; LE; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses.

e. DHS/S&T/PIA-024 Rapid DNA System - PIA describes how S&T developed the Rapid DNA System to meet a need to verify family relationships (kinship) in refugee immigration processes. (Not in operation within DHS.)

4.3.2 DOJ Privacy Compliance and Oversight

Pursuant to statute, DOJ's Chief Privacy and Civil Liberties Officer (CPCLO) is the principal advisor to Department leadership and components on privacy and civil liberties matters affecting the Department's missions and operations, and fulfills the statutory duties set forth in Section 1174 of the Violence Against Women and *DOJ Reauthorization Act of 2005*, and Section 803 of the 9/11 Commission Act. The CPCLO has primary responsibility for the Department's privacy policy and is to consider the privacy and civil liberties implications of proposed or existing laws, regulations, procedures, and guidelines. The CPCLO also has primary responsibility for the Department's compliance with the *Privacy Act*; the *E-Government Act of 2002*; *Federal Information Security Modernization Act*; and all other privacy laws, regulations, policies, and directives protecting the personal information of individuals. CPCLO's privacy compliance process involves the following:

Overview of the DOJ Privacy Compliance Process. Under the CPCLO's leadership, the OPCL is responsible for helping to ensure the compliance of the Department's components with existing laws, regulations and policies protecting privacy. The privacy compliance process consists of three primary parts which ensure the Department's compliance with applicable law and policy: the Initial Privacy Assessment (IPA), (PIA), and (SORN).

1. **IPA.** The privacy compliance process begins when the Department first determines it needs to capture, maintain, disseminate, or otherwise use PII. The Department has established the IPA template, which consolidates various privacy compliance requirements in to a single, unified, and comprehensive process. The IPA template consists of questions designed to help components and OPCL determine whether a particular information system contains and maintains PII; requires further privacy risk assessments and documentation (e.g., a PIA or a SORN); or raises other privacy issues or concerns.

   In particular, the IPA bridges (IT) security and privacy assessment processes and assists in identifying information assets requiring appropriate privacy security controls. An IPA must be completed prior to the development of an information system, including before the initiation of any testing or piloting of an information system. This enables components to identify steps to mitigate any potential adverse impact on privacy at the outset of the information captured or program. For example, an IPA may help a component determine that the capture and use of Social Security Numbers (SSNs) or other sensitive PII within a system is not necessary and decide to forego the capture of such PII.

2. **PIA.** OPCL may determine, based on an IPA, that a component must conduct further privacy assessments and documentation, including a PIA. PIAs analyze how electronic capture of information and information in systems or technologies are handled by components to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy.

Through the PIA process, the Department outlines the risks and effects of capturing, maintaining, and disseminating information in an IT. Additionally, the Department examines and evaluates protections and alternatives processes for handling information to mitigate potential privacy risks. A PIA must be completed either before developing or procuring IT systems or projects that capture, maintain, or disseminate IIF about members of the public, or before initiating a new electronic capture of IIF for 10 or more persons. By conducting a PIA at this time, components should consider the privacy impact from the beginning of a system's development through the system's lifecycle to ensure that system developers and owners have made technology choices that incorporate privacy protections into the underlying architecture of the system.

3. **SORN.** The Privacy Act requires agencies to provide notice to the public by, among other requirements, publishing a SORN if a component maintains, captures, uses, or disseminates records about an individual and retrieves them by a personal identifier. A SORN provides the public with details about a system of records, including its purpose for capture and maintenance, the categories of individuals serving as the subject of such records, the categories of information to be used and captured by the agency, the location where the agency maintains the information, the means of access and correction available to the individual, the safeguards that will protect the information, and the parties with whom and under what conditions the agency will share the information in the system. A system of records must be covered by a SORN published in the Federal Register before the system of records may be used. Thus, the Department must determine whether records are covered by an already existing SORN or require the publication of a new SORN. OPCL advises the Department's components on whether a particular information system qualifies as a system of records, and whether it is necessary to draft a new SORN, or to modify an existing SORN and any accompanying exemption regulation.

DOJ's published PIAs and SORNs are available on OPCL's website.[36]

Component Privacy Governance. DOJ components also have Privacy Programs that are led by senior component officials for privacy (SCOPs). For example, the FBI's SCOP is currently a Deputy General Counsel within FBI Office of the General Counsel (OGC) and also serves as the FBI's Privacy and Civil Liberties Officer (PCLO). The FBI's PCLO, who reports directly to the FBI Director and works closely with DOJ's CPCLO, is responsible for FBI-wide compliance with laws, regulations, and policies concerning privacy and civil liberties, pursuant to the responsibilities codified under 42 U.S.C. § 2000ee-1 and other related authorities. The FBI's Privacy and Civil Liberties Unit (PCLU), within FBI OGC, directly supports the FBI's PCLO. Generally, the FBI's PCLU is responsible for providing legal advice and counsel on compliance with federal law protecting individual privacy, such as *Privacy Act of 1974*, Section 208 of the *E-Government Act of 2002*, and the *Federal Information Security Modernization Act (FISMA)*, and best practices to achieve an appropriate balance between protecting civil liberties and facilitating investigative and intelligence collection activities.

Like DHS and DOJ, FBI's Privacy Program reviews and advises on all biometric modalities and the use of AI related to PII, which are subject to FBI's privacy compliance and oversight processes. For example, the FBI PCLU reviews privacy documentation (i.e., PTAs and PIAs, as described above) for biometric technology submitted by FBI headquarters divisions and field offices, consults with the program managers, as necessary, and forward the privacy documentation for review and approval by the FBI PCLO.

Also, like DHS and DOJ, the FBI PCLU subject matter experts and FBI's PCLO participate—alongside counterparts from DOJ, FBI Office of the (CIO), FBI Science and Technology Branch, operational divisions, and field offices— in numerous working groups, interagency committees, and other bodies addressing the use of biometric information and AI. This participation helps the FBI's Privacy Program to ensure privacy compliance and oversight are appropriately accounted for in FBI biometrics and AI programs and policies.

4.4 Civil Rights and Civil Liberties Protections at DHS

DHS utilizes biometrics to help enable operational missions, both to support national security and public safety, and deliver benefits and services with greater efficiency and accuracy. Biometric technologies can serve as an important tool to increase the efficiency and effectiveness of the Department of Homeland Security's broad and diverse missions, but it is vital that programs utilize these technologies responsibly and in a way that safeguards our Constitutional rights and values. The policies and procedures DHS follows ensures that the Department's use of this technology protects civil rights and civil liberties and in full compliance with the law.

Operators, researchers, civil rights advocates/stakeholders, and policymakers must work together to prevent algorithms from leading to racial, gender, or other impermissible biases in the use of biometric technologies. DHS's commitment to nondiscrimination in LE and screening activities remains an important cornerstone of its daily work to secure the homeland and informs its adoption and use of this technology.

In addition to the strong civil rights and civil liberties interest in ensuring equality of treatment, DHS has a compelling interest in ensuring the accuracy of biometric technologies or any tool that assists in performing the mission. Improved accuracy and efficiency in the DHS's data systems results in better performance of all the DHS missions they support.

The successful and appropriate use of biometric technologies requires ongoing oversight and quality assurance, initial validation and regular re-validation, and a close relationship between the users and oversight offices. In this way, it can be developed to work properly and without impermissible bias when it achieves initial operating capability, and then continually through its entire project lifecycle.

No single list can address all the issues in the permutations of biometrics technology and data use, but there are broad themes that the DHS Office for Civil Rights and Civil Liberties (CRCL) considers when supporting programs utilizing biometric technologies:

1. Legal Authority and Compliance*. Prior to establishing a biometric program, work closely with your legal counsel to confirm there is legal authority to capture and utilize biometrics for the intended purpose. Involve legal, privacy, civil rights, and civil liberties experts at every stage of formulation, operation, and review of a biometric program to ensure compliance with applicable laws and policies.*

2. Clear Purpose. *Clearly articulate the primary purpose for establishing a program utilizing biometric technologies.*

Considerations:

- The public may better understand and appreciate an agency's reasons for establishing a biometric program with a clearly stated and plainly worded purpose.
- Identify the challenge that prompted your agency to create a biometric program and how biometrics will assist in addressing that challenge.
- Describe the primary purpose(s) of your biometric program online and/or make this information publicly accessible, while not revealing information that could reasonably be expected to compromise LE or national security.

3. Respect Constitutionally Protected Activities. *It is essential that biometric technologies be employed in a manner that includes safeguards for privacy, civil rights, and civil liberties. The development of new biometric technologies, significant improvement of a current technology, or the new application of an existing technology often results in concerns about the impact on individual privacy, civil rights, and civil liberties. It is important that agencies work closely with legal, privacy, civil rights, and civil liberties experts to ensure compliance with applicable laws and regulations when developing a biometric technology program.*

Considerations:

- Biometric recorded data should not be captured, disseminated, or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations).
- Capture, use, dissemination, or retention of biometric data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, gender, or disability).
- Biometric technologies used for identification should not be used as the sole basis for law or civil enforcement related actions, especially when used as investigative leads. Any potential matches or results from the use of a biometric technology for identification should be manually reviewed and adjudicated prior to any law or civil enforcement action.

4. Discrimination. Biometric technologies, in either their design or use, can result in an impermissible discriminatory impact, some more so than others. This is seen in private sector analysis of certain facial recognition software platforms for example—these issues are likely due to the algorithms used and not being able to control certain variables. The presence of algorithmic bias has been highlighted in U.S. government analysis as well, perhaps the most widely known being the December 2019 NIST

report which noted substantial bias or substantial demographic effects in many algorithms, often due to the quality of the image, but sometimes due to an algorithm.[37] Nonetheless, it is imperative that all demographics be treated equally – an ongoing challenge which industry and the academic community, including DHS's MdTF, continue to work to mitigate.

However, the NIST report also highlights how the demographic differentials are smaller or undetectable with more accurate, high-performing algorithms in certain applications. *It is imperative that NIST testing, high quality algorithms from trusted sources continue to be required for any type of biometric algorithm or system*. Even when using such high-performing algorithms, as DHS does, *testing and validation must be a constant in the operational life cycle.* DHS policy requires that all uses of face recognition and face capture technologies will be thoroughly tested to ensure there is no unintended bias or disparate impact in accordance with national standards.

Considerations:

- What algorithm is being used and has it been tested by NIST or another independent assessment? What were the results of that assessment? Has the algorithm also been tested in the operational environment in which it will be used?
- What variables are present that may negatively impact an individual's interactions with the system? Examples could be environmental, such as lighting, the type and quality of photographs being captured, or the ability of an individual to use the system.
- How can we mitigate the impact of these variables in our operations?

5. *Accuracy.* *The CRCL interest in accuracy tracks closely with the Department's strong operational interest in a high degree of accuracy in systems relied on to identify individuals in support of screening, vetting, security, and other activities. In all-systems, but biometric systems in particular, the importance of accuracy is paramount.* Identity systems need to operate at a high-level of accuracy to minimize unintended negative impacts on individuals and vulnerable populations—and almost as importantly, the perception of discriminatory impacts of accuracy in systems relied on to identify individuals or verify an individual's identity in support of screening, vetting, security, and other activities.

Considerations:

- What can we do to ensure that we're identifying any potential accuracy issues as early in the process as possible?
- What is the process for potential matches to be reviewed? Is there a human review in the process?
- Is there a review process for instances where the biometric system fails to provide a positive match for an individual?
- Is there a tracking process to identify potential disparate impacts in the comparison results?
- What training do human examiners receive?

- Are users aware of potential inaccuracies or disparities, and how to identify and remedy errors?

6. *Scale and Flexibility.* *Biometric systems and processes and procedures must be implemented with appropriate flexibilities to allow for reasonable accommodations*. With certain biometric modalities, a non-trivial percentage of the population cannot present suitable features to participate in certain biometric systems. For example, many people have fingers that simply do not "print well" or have a disability which would limit their participation. Even if people unable to be fingerprinted represent 1% of the population, this may translate into massive inconvenience and suspicion for that minority.

Considerations:

- What processes and procedures are in place to provide appropriate accommodations for individuals that comply with Section 508 of the Rehabilitation Act of 1974?
- Are there alternate procedures in place to accommodate individuals with disabilities or individuals that may require alternate procedures for religious reasons?

7. Use. *Information gathered for one purpose should not, as a general rule, be used for completely unrelated, unconsented-to purposes. Recognizing that the purpose and utility of a biometric program may evolve over time, certain changes to the biometric program's stated purpose that may impact individual rights should be reviewed by an agency's legal, privacy, civil rights, and civil liberties experts.*

Considerations:

- Changes to the biometric program's primary purposes should be reflected in documents readily available to the public prior to implementing those changes.
- Establish a routine program review process to assess whether the program's purpose is being met and whether modifications are required.

8. Perception. Public support is essential for a biometric program's success. A program that is not transparent according to applicable laws, agency policies, and best practices may quickly lose support and create misperceptions about the program's intended mission(s). *While we need to guard against actual and perceived bias in biometric systems, we similarly need to address misperceptions that the biometrics the federal government captures for legitimate missions are being used to conduct unlawful surveillance or tracking of individuals.* With the potential for some biometrics, such as face or voice, to be easily captured without consent or without a custodial interaction (as opposed to giving a fingerprint to receive a benefit, or have DNA captured due to an arrest), DHS has a *responsibility to actively promote a common understanding of the technology and the federal government's use and non-use of it. DHS CRCL engages with stakeholders in order to provide feedback to federal government and Component leadership regarding the impacts or consequences of policies, programs, activities and initiatives.*

Considerations:

- What transparency measures can we adopt so that requirements and system performance are communicated clearly and understood? Are there language access considerations when communicating about biometric technologies?

- What public notifications are required prior to use?
- Are individuals provided notice that they can opt-out of a system?
- Establish and make publicly available clear policies and procedures to ensure respect for privacy, civil rights, and civil liberties.

9. Redress. *Individuals must have an opportunity to correct both their biographic and biometric information so that incorrect biometric comparisons or other adverse consequences can be effectively and timely challenged, and databases corrected.* If a database contains incorrect information about a suspect or a defendant, incorrect information should be corrected, removed, and/or appropriate mitigating information be included to ensure the data is properly contextualized. DHS CRCL has an established complaint process to investigate allegations of violations of civil rights and civil liberties related to the DHS's use of biometrics and provide recommendations for the development and implementation of applicable additional safeguards.

Considerations:

- What redress processes are in place to correct biometric records, if necessary?
- Information on how an individual requests redress should be succinct, straightforward, and readily available to the public.
- Ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

10. Unintended Consequences. *Consequences of a false match and the impact of a false match should be considered to ensure this "do no harm" approach is appropriately implemented in all biometric-related programs.*

Considerations:

- What happens in the event of a non-match? What is the impact on the individual?
- What processes or procedures can be implemented to minimize any negative impact on an individual?
- What are the secondary procedures for individual with disabilities or a religious exemption that would preclude their participation in the program?
- What are the potential access concerns?
- How will reliance on the system change agency operations? And how will the agency react in case of degradation or unavailability of the system?

11. Validation. Equally important is ensuring that systems undergo independent reviews and audits. Face recognition, for example, can be highly accurate. But accuracy rates depend on multiple factors, including the camera, quality of the face photo, and the algorithm used to compare face photos in an automated fashion. *Analysis of accuracy and error rates need to account for the various factors potentially presented in an operational setting. Objective, independent analysis of software and algorithms can ensure that the system is*

operating as we believe it is, and to verify that the Department's biometric data remains secure and that technical protections are effective and implemented properly.

Considerations:

- What internal reviews will be conducted to identify potential issues? How can organizations determine whether matches may be having negative demographic impacts?
- Are there internal oversight procedures in place (including audits or assessments) to ensure that biometric-related queries are being conducted consistent with policy?
- Is there adequate supervision of personnel and a process for personnel to report suspected cases of misuse or abuse.
- What business requirements may be needed to ensure biometric data remains secure?
- Do the risks associated with the biometric system merit lifecycle testing/oversight/validation efforts?

These best practices are not prescriptive, but rather are provided to share DHS's considerable experience operating biometric technologies, and to provide biometric system operators with privacy, civil rights, and civil liberties practices to consider before initiating a biometric technology program. The applicability or advisability of implementing each recommended practice to a particular biometric program will vary based upon each individual agency's legal authorities, purpose of the mission, mission of the agency, and type of biometric modality. Therefore, each LEA is encouraged to consult with its legal counsel to ensure compliance with its agency's own particular legal requirements.

5. DHS & DOJ Centralized Identity Management Systems

The federal government continuously operates, maintains, and seeks to improve its centralized identity management services in order to provide critical information to its stakeholders, including those in law enforcement tasked with supporting public safety and national security. The goal of these identity management systems is to support highly assured decision-making and actions in the field in a timely manner with technical proficiency in the match score, share and analyses of its stakeholder biometric and biographic captures, both with automated algorithmic functions of biometric modalities, as well as support centers and human examiners. This section provides an overview of these systems at DHS and DOJ.

5.1 DHS OBIM IDENT and FBI NGI: Identity Management Systems Overview

The two key identity management systems at DHS and DOJ are DHS's Automated Biometric Identification System (IDENT), housed in DHS OBIM, and the FBI's Next Generation Identification (NGI) System, housed within its CJIS Division. Law enforcement decision making is significantly enhanced with the interoperability between IDENT and NGI. Together and apart, IDENT and NGI support their respective DHS and DOJ components as well the U.S. Departments of State, Defense; SLTT entities; the Intelligence Community; and international partners.

For both systems, how a *match* is adjudicated depends on the biometric modality captured or queried, but for all modalities, fast responses help identify criminals, fugitives, and known or suspected terrorists rapidly to federal government, international and SLTT stakeholders. Business rules support both data *sharing* and privacy rules in regard to what information is shared with whom. *Storage* is based upon standard protocols in the areas of compliance, data protection, systems protection and continuous monitoring that assure confidentiality, availability, and integrity of data 24x7, at rest or in transit. *Analyses* enables bulk data to be refined for integrity and surety, with examiners trained in each modality to help assure valuable adjudication of modality images.

Super Bowl Case Study

At Super Bowl XLIX in 2015, a threatening letter was left at the University of Phoenix Stadium in Glendale, Arizona. A fingerprint was recovered by university officials and turned over to the Glendale Police Department.

Due to the interoperability of IDENT and NGI, this fingerprint matched to a known identity. OBIM advised that the individual be flagged in IDENT in the event of any future border or LE encounter.

Figure 4 - Case Study

Interoperability. The sound work of criminal justice, immigration, border enforcement, national security, intelligence, background investigations for national security positions and certain positions of public trust, and other authorized function is grounded in the interoperability that HSPD-24 and NSPM-7 emphasized. A manhunt in the late 1990s provided the catalyst for today's IDENT-NGI interoperability. A serial killer who traveled by freight train and committed murders near railroad lines became known as the "Railway Killer." The man, a Mexican national, had crossed into the United States illegally several times. Because IDENT contained information only about U.S. Border Patrol apprehensions and was not linked to other biometric databases in the criminal justice community, the man was returned to Mexico several times, even though there was a warrant out for his arrest. The case provided the impetus to link IDENT and FBI's fingerprint database at the time, IAFIS, in order to identify those people with criminal records or active warrants moving across the border.

In the months that followed, the FBI began to provide IDENT with higher-value sets of data such as those concerning wanted persons--individuals for whom Federal warrants are outstanding; warrants--precept or writs issued by a magistrate authorizing an officer to make an arrest, seizure, or search; sex offenders, and known or suspected terrorists, which provided the framework for today's interoperability.[38]

The seamless interoperability between IDENT and NGI provides accurate and timely information to each organization's numerous stakeholders, multiplying the effect of providing accurate and timely information that support both national security and law enforcement throughout the United States.

5.1.1 DHS OBIM IDENT

IDENT was developed in 1994 by legacy INS as a generic Automated Biometric Identification System for the U.S. Border Patrol as a LE tool for capturing and processing biometric data on recidivist border crossers. IDENT moved from pilot to program in 1998. Upon the creation of DHS in March 2003, and the absorption of IDENT, the system has grown exponentially over the years due to statutory requirements and innovations around use cases across numerous components. IDENT today is the DHS-wide system for the storage and processing of biometric and associated biographic information, servicing 40-plus customers across FSLTT and international organizations.

More specifically, IDENT has grown from its initial few thousand transactions in 1998 for just fingerprint, to approximately 400,000 transactions per day in 2023 that also includes face and, to a limited extent, iris. Initially, IDENT fell under the responsibility of US-VISIT, a program designed to improve the nation's capability to capture information about foreign nationals who travel to and from the United States. Under US-VISIT, IDENT grew to become the main biometric database for DHS. In 2013, US-VISIT transitioned to become OBIM.

OBIM is the Congressionally designated lead entity within DHS responsible for rapid identification and verification biometric identity services. OBIM's mission is to provide enduring identity services to DHS and its mission partners, enabling national security and public safety decision making by producing accurate, timely, and high assurance biometric identity information and analysis. OBIM provides biometric identity services through the operation, maintenance, and improvement of IDENT, the central, DHS-wide repository that compares, stores, and shares biometric and associated biographic information, its Biometric Support Center (BSC) human examiners, and additional biometric expertise.

Overview. As of 2023, top IDENT federal customers include, but not limited to, Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services, the Transportation Security Administration, U.S. Department of State, Federal Emergency Management Agency, U.S. Secret Service (USSS), and Immigration and Customs Enforcement (ICE), Department of Defense, and the U.S. Coast Guard. IDENT as a system stores more than:

DHS OBIM IDENT PROCESSING

More than 40-plus stakeholders query IDENT's 300 million unique identities, the largest identity repository in the U.S. government.

Annually, more than 114 million biometric transactions are processed.

Every day, 105,000 biometric exchanges are made with FBI NGI, enhancing the effectiveness of both IDENT and NGI.

Every hour there are 14,603 biometric transactions, 69 enforcement actions, 2,324 new enrollments, 7 enforcement hits, and 5 suspected or known terrorist hits.

Figure 5 - IDENT at a glance

- 1.3 billion encounters for more than 300 million unique identities, the largest fingerprint repository in the United States;
- Approximately 1 billion face images; and
- Approximately 10 million pairs of irises.

IDENT can search an entire gallery of unique identities in less than two minutes for priority requests. The system receives 1.29 million wants and warrants from the FBI annually. Its watchlist is at 19 million unique identities; everyday IDENT capabilities help OBIM customers identify dozens of fugitives, criminals, or known or suspected terrorists.

It is important to IDENT's scalability robustness, and confidence in comparison results that it only use biometric algorithms that rank in the top of NIST accuracy in both 1:1 and one-to-many searches across currently employed biometric modes. In addition, OBIM's Biometric Support Center Services (BSC) provides 24/7 biometric identification and verification for 10-print comparisons and verifications, unknown deceased identifications, latent fingerprint comparisons, face and iris comparisons, and enrolls captures from its LE stakeholders. On an average day, for example, the BSC conducts 1,987 10 print comparisons in support of IDENT and corrects 65 biometric captures.

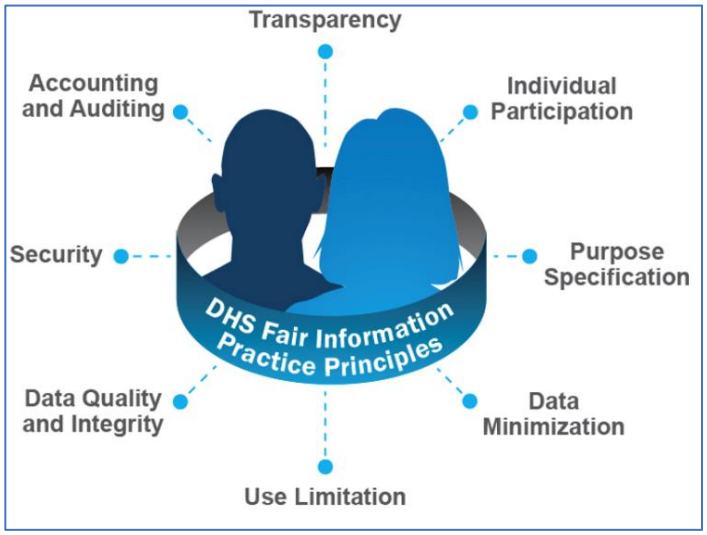

Figure 6 - DHS OBIM Privacy Matrix

Fingerprint Services. 1:1, one-to-many comparison, and latent to known searches are returned in 10 seconds of the 19 million watch listed identities, and can perform 2-print, 10-print and latent comparisons. OBIM has identified more than 12,600 latent fingerprints.

Face Recognition Services. 1:1, one-to-many search, and face comparison (2 photo submission) to its DHS components. OBIM is also partnering with NIST to develop a face image quality standard to measure the quality of a face image for future comparisons in a vendor-agnostic face recognition application.

Iris Services. 1:1, one-to-many search, using two different vendors. Iris comparisons initiate review of fingerprint decisions when results differ.

OBIM Notification Services. Users can subscribe to two different types of alerts: (1) encounter notification service, when a match has occurred on an identity; and (2) derogatory update notification service when derogatory information changes or is added to an enrolled identity. When an IDENT customer subscribes to receive IDENT Notification Services, they will receive activity alerts about an individual whom they have previously enrolled in IDENT. For example, if an individual is arrested by

Federal, State, or local LE, their fingerprints are sent to the FBI CJIS NGI system, which subsequently sends the biometric record to IDENT for search. If there is a match to an independent DHS or Department of State encounter, a new encounter containing derogatory information is created in IDENT. IDENT subsequently notifies the subscribing agency of the new encounter, as well as the existence of new derogatory information based on the watchlist status change.

Privacy Protections. OBIM protects the privacy of persons whose PII is within its holdings by adhering to U.S. privacy law, complying with Fair Information Practice Principles, and establishing business rules that protect personally identifiable information and assure that information is only shared with those specifically granted access to particular data.

OBIM embeds privacy protections into its biometric identification and analysis services that help assess whether an individual poses a risk to the United States.

5.1.2 FBI NGI

System Background. Fingerprint transaction processing became automated in 1999 with the establishment of the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS provided automated ten print and latent fingerprint searches, electronic image storage, electronic exchanges of fingerprints and responses, as well as text-based searches based on descriptive information. Because of growing threats, new identification capabilities were necessary. Advancements in technology allowed further development of biometric identification services. The CJIS Division, with guidance from the user community, developed the NGI System to meet the evolving business needs of its IAFIS customers.

The NGI System is interoperable with DHS's IDENT,[39] and the Department of Defense (DoD) Automated Biometric Identification System, known as ABIS.

NGI System Overview. Fully deployed in 2014, the NGI System is the FBI's national repository that provides biometric identifications, biometric investigative support, and identity history services for authorized FSLTT and international criminal and noncriminal justice agencies. This is primarily completed by providing identification services for fingerprints and irises; and providing investigative services for latent fingerprints; palm prints; face images; and scars, marks, and tattoo images; as well as identity history services through checks and challenges.

The categories of fingerprints currently maintained in the NGI System include: persons fingerprinted as a result of arrest, incarceration, or other authorized criminal justice purpose; persons fingerprinted for employment, licensing, or other authorized noncriminal justice purpose, such as federal background checks and military service; persons fingerprinted for alien registration, immigration, naturalization, or related purposes; and individuals fingerprinted for authorized national security purposes (including known or suspected terrorists and military detainees). FBI Universal Control Number (UCN) is a unique identity number in the NGI System, which links the photos with biographic and other biometric information in the NGI System.

As of year's end of 2023, the NGI System contained 158,067,671 unique identities, supported by fingerprints. In fiscal year 2023, the NGI System processed an average of 202,303 fingerprints per

day. On February 12, 2024, the NGI System processed its 1 billionth fingerprint transaction. The FBI's CJIS Division, through NGI, offers a fingerprint-based identification service to authorized local, state, tribal, and federal partners for criminal and noncriminal justice purposes. The FBI serves as the nation's central repository for identification and criminal history record information and maintains criminal, civil, and national security fingerprint records in its NGI System.

The purpose of the NGI system is to provide its authorized users with information relevant to their missions and authorities. The NGI system maintains criminal history record information (CHRI) associated with criminal ten-print fingerprints. CHRI is defined as information captured by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The CHRI is submitted voluntarily by federal, state, local, tribal, and foreign criminal justice agencies. The ten-print fingerprint remains the primary biometric in NGI and is the only biometric used to establish an NGI record.

Authorized partners may submit an electronic criminal or civil fingerprint image for comparison against the NGI System. Fingerprint comparisons provide a positive identification or nonidentification to an individual for criminal or noncriminal justice purposes. The fingerprints must be captured, stored, and disseminated pursuant to applicable legal authorities and for the intended purpose defined within the CFR.[40]

Enrolled Fingerprints. Fingerprints have been used for identification for over 100 years. The NGI System classifies and searches fingerprints by pattern classification type and has a comparison accuracy of 99.6 percent. The NGI System serves as the FBI's biometric identity and criminal history records system and maintains the fingerprints and associated identity information of individuals submitted to the FBI for authorized criminal justice, national security, and civil purposes.

Latent Fingerprints. The NGI System's latent services provide LE and national security partners with the ability to identify latent prints obtained from evidence within criminal and terrorism investigations. A latent print is a transferred impression of friction ridge detail (i.e., the raised portion of the epidermis of the palm and fingers) that is not readily visible. The identification of latent prints provides new investigative leads to assist with solving crimes and/or intercepting terror plots against our nation, as well as protecting military personnel and coalition forces operating worldwide. These services also provide the ability to identify unknown deceased persons and eliminate individuals as persons of interest within active LE investigations, clearing the innocent of suspicion, while helping to insure the guilty are held accountable. Latent prints are searched against known biometric identities retained within the NGI System and those remaining unidentified can be retained within the NGI System's Unsolved Latent File (ULF). The ULF allows for the vetting of new biometrics received by the FBI after initial search of the NGI System. Latent print identifications resulting from candidates produced by the NGI System are considered investigative leads; therefore, candidates require subsequent review by latent print examiners within the receiving LE or national security agency to determine a positive identification.

The governing policies and applicable laws, regulations, and Executive Orders for the FBI's latent services are referenced within the FBI's PIA for the *Next Generation Identification Latent Services.*[41]

5.1.3 Case Study: Interoperability from NGI System to IDENT[42]

Criminal justice fingerprints searched or maintained in the NGI System include fingerprints of individuals encountered by LE as a result of a criminal inquiry, a lawful detention, arrest, or incarceration. These criminal justice fingerprints are submitted to the NGI System by FSLTT agencies.[43] After the NGI System has been successfully queried for these fingerprints, the IDENT system is also automatically queried for them as well. Criminal justice fingerprints account for the majority of the fingerprint transactions shared with IDENT for a biometric search. In addition to the fingerprints, the name, date of birth, and gender of the subject are sent to IDENT, as well as the Originating Agency Identifier (ORI)[44], and the Universal Control Number (UCN).[45] Unless there is a match, the NGI System data is not retained by the IDENT system.

If there is an identity match in IDENT, it will return a response to the NGI System that contains name, date of birth, place of birth, gender, record identifier, and photo. This information is not retained in the NGI System, but the DHS Fingerprint Identification Number (FIN) is maintained on the NGI System record to establish a pointer between the two systems for record linking purposes. In the event a "match" response is received from IDENT, the NGI System generates a separate query to a separate ICE System regarding the immigration status of the individual. After receiving both the IDENT match response and the ICE response, the NGI System generates a response to the original submitting criminal justice agency, if the state agency has installed a program to electronically receive this additional DHS information. In addition, if a fingerprint match is not generated in IDENT, but the subject appears to be a non-U.S. person based on the NGI System record, the NGI System sends a query to ICE. These queries are only generated for criminal arrests that have not matched in IDENT. ICE uses this process to identify subjects in LE custody who may be appropriate for removal but who lack previous encounter information in IDENT.

If an NGI System search results in a match in IDENT and that system already maintains a separate, independent encounter with the individual, then a new encounter will be created in IDENT. The new encounter in IDENT includes a pointer within the record to alert IDENT users of another information source regarding that identity. The IDENT record does not maintain the criminal history information but retains the UCN and is updated with the subject's name, date of birth, gender, and fingerprint images. If there is not a match, no NGI System information is retained in IDENT.

In addition, certain non-criminal justice fingerprint transactions are sent from the NGI System to IDENT for a secondary biometric search. These transactions include individuals fingerprinted for federal employment background investigations and security clearances. Participating agencies include the Defense Counterintelligence and Security Agency (DCSA), the DOS Diplomatic Security (DS) Office of Personnel Security and Suitability (OPSS), and the International Criminal Police Organization. If there is an identity match in IDENT, it will return a response to the NGI System that contains name, date of birth, place of birth, gender, record identifier, and photo. This information is not retained in the NGI System. As with the criminal fingerprint submissions, after receiving the match response from IDENT, the NGI System generates a query to ICE to obtain the immigration status of the individual. After receiving both the IDENT match response and the ICE response, the NGI System combines the responses to send to the original agency, if the agency is programmed to receive the response.

DCSA transactions are only queries, and no information is retained in IDENT, even when there is a match. DOS DS OPSS transactions are retained in IDENT regardless of an independent encounter and the IDENT record is updated with the subject's name, date of birth, gender, and fingerprint images. The UCN is not provided to IDENT for non-criminal justice fingerprint transactions. Finally, for humanitarian purposes, the fingerprints of unknown deceased persons are forwarded from the NGI System for a search of IDENT to assist in identifying human remains, victims of crimes such as homicide, or even persons who have been missing. The NGI System sends the combined IDENT and ICE response to the originating agency. The ability to search IDENT with unknown deceased fingerprints has aided in the successful identification of deceased victims in several cold cases.

The FBI shares certain data sets in bulk with DHS rather than sending transactions automatically via the NGI System to IDENT. These data sets include the wanted individuals/warrants and sex offender records from the National Crime Information Center (NCIC)[46] system and certain national security and foreign fingerprints maintained in the NGI System. Because the NCIC system is name-based, to avoid the risk of misidentification, only those identities that have associated fingerprints in the NGI System are shared with IDENT. The wants/warrants and national security/foreign records shared in bulk with DHS are retained in IDENT regardless of whether IDENT has an independent encounter; currently DHS retains the sex offender records only if IDENT has an independent encounter.[47]

The NCIC wants/warrants are shared with IDENT every four hours, and the national security/foreign fingerprints and NCIC sex offender records are shared with IDENT once per day. In all instances, the fingerprints and basic identity elements (i.e., name, date of birth, place of birth) associated with the UCN are sent to IDENT. Consistent with NCIC policy, in order to reduce the risk of misidentification, DHS must independently confirm with the record owning LEA if a wanted individual or warrant has generated a match to an identity in IDENT. When appropriate, record deletions are provided via an NGI System delete message to IDENT. An automated synchronization process between IDENT and the NGI System occurs the first of every month for the wants/warrants and the national security/foreign records, and a manual synchronization process occurs annually for the sex offender records.

DHS sends several types of fingerprint inquiries via IDENT to the NGI System, including DOS, USCIS, CBP, and ICE transactions. DHS components that use IDENT must affirmatively choose to search the NGI System. IDENT will not automatically send the transaction to the NGI System unless the user requests a separate search. As an agency with LE components, DHS submits criminal justice fingerprints taken pursuant to arrest or other criminal justice purpose via IDENT to the NGI System for search or retention. If a match occurs in the NGI System, the criminal history information and associated biographic information will be returned to DHS. Only the UCN is retained in IDENT to serve as a pointer to criminal history in the NGI System. IDENT is not programmed to retain the criminal history; however, IDENT returns the NGI System response and criminal history to the originating DHS component which may retain the information in its case management system. For those searches retained in the NGI System, identity information such as name, date of birth, gender, as well as fingerprint, photos, and iris images from IDENT are maintained.

DHS sends fingerprints to the NGI System captured by CBP at the nation's land, sea, and air borders to assist with admissibility determinations. The NGI System responses provide criminal history that may be relevant to admissibility or LE actions. In a program instituted at major airports, CBP sends fingerprints for a rapid search of the NGI System. These fingerprint searches are not retained in the NGI System. In these rapid search situations, the NGI System returns a candidate list to CBP, rather than a positive identification. If a returned candidate appears to be a match, CBP may subsequently send criminal inquiry fingerprints to the NGI System to obtain the subject's criminal history. If CBP arrests the subject, CBP would submit criminal retain fingerprints to the NGI System at that time.

The NGI System also searches and retains the DHS-captured fingerprints of subjects of interest in foreign countries, including those captured pursuant to ICE's Biometrics Identification Transnational Migration Alert Program (BITMAP). The BITMAP fingerprints, captured in partnership with foreign LE, are of subjects who may pose a criminal or national security threat to the U.S. The BITMAP fingerprints may be submitted as retain or non-retain to the NGI System, depending upon the category assigned by ICE. For example, gang members and special interest aliens are submitted as retain but many other fingerprints are submitted as non-retain.

DHS also sends non-criminal justice fingerprint inquiries via IDENT to the NGI System, including fingerprint searches for the purpose of visa issuance. The DHS performs this service on behalf of the DOS's Consular Offices. The NGI System is capable of processing tens of thousands of visa fingerprint submissions per day with an expedited response time within 15 minutes. These DOS transactions are sent as search only in the NGI System. In addition, USCIS submits fingerprints of applicants for immigration benefits to the NGI System for criminal history background checks. These USCIS transactions are retained in the NGI System. As with the criminal justice submissions, if a match occurs in the NGI System, the criminal history information and associated biographic information will be returned to DHS but IDENT retains only the UCN. The originating DHS component may retain additional information.

5.1.4 NGI Interstate Photo System (IPS)

The NGI System serves as the FBI's biometric identity and criminal history records system and maintains the fingerprints and associated identity information of individuals submitted to the FBI for authorized criminal justice, national security, and civil purposes. The NGI IPS[48] contains the photos captured by federal, state, local, tribal, territorial, and select foreign and international agencies submitted with ten print fingerprints and offers a facial recognition search capability to LE users.

NGI IPS Use and Information Technology. The NGI IPS currently contains face photos as well as photos of scars, marks, and tattoos. Photos submitted to the NGI IPS are received voluntarily with ten print fingerprint transactions from authorized federal, state, local, tribal, territorial, and select foreign and international agencies. The NGI IPS photos are associated with the submitted images are housed together in a common repository, separated into criminal, civil,[49] and national security[50] identity groups. This logical separation provides system flexibility to maintain handling and dissemination of information. For purposes of NGI IPS searching, the automated NGI IPS FR algorithm is applied to each submitted image to determine if the image is of sufficient quality for search; and, if so, the algorithm creates a face template. Although a template may be created for images in any of the three identity groups, FR searches (FRSs) of the NGI IPS are not conducted against face images associated with a civil-only identity in the NGI System.

The NGI IPS also provides an investigative FRS capability limited to LEAs. LEAs are permitted to search photos obtained related to criminal investigations, known as "probe" photos, against the photos maintained in the NGI IPS. Authorized users conducting FRSs against the NGI IPS must comply with FBI *NGI Policy and Reference Guide* regarding use of the system. FBI policy defines probe photos as facial photos lawfully obtained pursuant to an authorized criminal investigation. FBI policy prohibits the submission of photos of individuals exercising rights guaranteed by the First Amendment (e.g., lawful assembly) unless pertinent to and within the scope of an authorized LE activity. The policy also prohibits submission of photos captured as a result of a search in violation of the Fourth Amendment. After the FRS is performed, the probe photo is not retained in the NGI IPS.

The automated FR algorithm[51] in the NGI IPS compares the probe photo against the photos in the NGI IPS to locate potential candidate photos. The FR algorithm uses pattern-comparison approaches developed within the field of computer vision to identify people in photos from their facial appearance. Patterns are groups of numbers that summarize the image of a face, or a part of a face, in a way that is preserved as identity information. The distance between two patterns[52] should be low for two images of the same person and high for images of different people. The software that computes the pattern is written to take advantage of the anatomy of the face but also uses inputs such as lighting, facial surface changes like facial hair or cosmetics, and facial modifications due to changed expressions, such as closed eyes, wrinkled brow, etc. The FR algorithm uses these features to create a template from the face, which is then compared against other face templates.

Since the NGI IPS is designed to provide investigatory leads, rather than an identification, a gallery of potential candidate photos will always be returned to the LEA. The candidate gallery returned to the LEA will generally consist of photos associated to a criminal identity. A gallery of two to 50 photos

will be returned, with the LEA choosing the size of the gallery. If no choice is made, a default of twenty photos is returned.

Candidate photos returned to the LEA are provided as investigative leads only and are not positive identification. Although FR technology has become increasingly accurate, authorized users of the NGI IPS are prohibited from relying solely on the candidate photos as the basis of any LE action. The candidate photos must be considered as investigative leads only, in conjunction with other relevant information and evidence related to the criminal investigation.

FBI policy requires that LEA users complete FR training in compliance with national scientific guidelines prior to conducting FRSs of the NGI IPS. States and LEA with the capability to conduct FRSs of the NGI IPS have been notified of the training requirement, noted in the FBI *NGI IPS Policy and Reference Guide*, which may be met either through vendor or FBI provided training. Training must meet the Facial Identification Scientific Working Group (FISWG) guidelines.[53]

With this training, the LEA user learns how to conduct an effective manual review of the candidate photos to determine whether the gallery contains a likely candidate to the probe photo. If the LEA user determines a likely candidate, the LEA user will then proceed with additional evaluation and investigation to determine if the probe photo and the candidate photo are, in fact, the same individual.

To conduct FRSs of the NGI IPS, the LEA's information system must be programmed to submit and receive FR transactions electronically and must successfully complete testing with the FBI. The probe photos received for LE purposes from these agencies are processed by the FBI under rules detailed in the *NGI IPS Policy and Reference Guide*[54] with candidate photos returned as investigative leads.

NGI IPS Authorities, Data Security, and Standards. The FBI's NGI IPS operates under the following authorities, orders, and regulations that authorize the capture of the information.

Authority	Citation/Reference
Statutes	28 United States Code (U.S.C.) §§ 533, 534 34 U.S.C. §10211 44 U.S. C. §3301 6 U.S. C. § 211(g)(4)(C) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist (USA PATRIOT) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001)
Executive Orders	8781, 8914, and 13764
Federal regulations	28 C.F.R. 0.85, 20.31, 20.33

Figure 7 – Authorities for NGI IPS

Privacy Act notices are not provided to individuals regarding the capture, use, and sharing of their photos in the criminal or national security identity groups of the NGI IPS, with the FBI exempting

itself out of the *Privacy Act* systems of records notice requirement to disclose the purpose for which the NGI identity records are maintained under its Section 552a(e)(3). However, the photos are captured in conjunction with ten print fingerprints, which means the subject should be aware of the e capture. Only individuals in the NGI IPS Civil Identity Group of the NGI IPS will receive a Privacy Act notice concerning the capture of their fingerprints, photos, and other personally identifiable information when applying for employment and licensing. The NGI (SORN)[55] provides general notice of the capture and use of the photos.

Electronically, biometrics are supported through the Electronic Biometric Transmission Specification (EBTS), which currently supports fingerprint, palm print, latent print submissions, face and scar, mark, and tattoo photos. The EBTS provides proper methods for external user systems to communicate with the FBI NGI System for the transmission of biographic and biometric information for purposes of criminal or civil identification and investigative types of transactions. The FBI developed the EBTS standard for electronically encoding and transmitting biometric image, identification, and arrest data that extends the American National Standards Institute/NIST–Information Technology Laboratory (ANSI/NIST-ITL) standard. ANSI/NIST-ITL is developed and maintained in conjunction with NIST and the biometric community. While the ANSI/NIST-ITL standard provides the guidelines for the exchange of information between various federal, state, local, tribal, territorial, and international biometric systems, the FBI's EBTS defines requirements to which federal, state, local, territorial and partner agencies must adhere when electronically communicating with the NGI System.

Additional privacy protections are provided by 28 U.S.C. §534, which state that the dissemination of information under its authority is subject to cancellation if shared information is disclosed outside the receiving agency or related agencies. Although this is a separate statute from the *Privacy Act*, it provides specific controls on the dissemination of criminal history record information, including, identification of authorized recipients and potential sanctions for unauthorized disclosures. These restrictions are, in turn, reflected in long-standing and extensive system security standards and operating policies applicable to all system users. In addition, authorized users must comply with applicable security and privacy protocols addressed in the FBI CJIS Security Policy.

NGI IPS Auditing. The FBI CJIS Division performs triennial audits of all CJIS system agencies (CSA), the state agencies that are responsible for their states' connections to the NGI IPS and whose CJIS Systems Officer (CSOs) are responsible for implementing compliance by their states. The state CSOs, in turn, conduct audits of their local agencies on a triennial basis. The state CSO is responsible for implementing and ensuring compliance with the FBI CJIS Security Policy. Likewise, federal agencies with a connection to the NGI IPS have federal CSOs with a similar responsibility at the federal level. The FBI CJIS Division provides training assistance and up to date materials to each CSO and periodically issues information letters to notify authorized users of administrative changes affecting the system. CSOs at the state and federal level are responsible for the role-based training, testing, and proficiency affirmation of authorized users within their respective state or federal agencies. The FBI CJIS Division and CSA audits confirm that only authorized agency personnel are accessing the NGI IPS for authorized purposes.

The audits assess and evaluate users' compliance with the FBI CJIS Division's technical security policies, regulations, and laws. Audit reports are typically prepared within a few months and deficiencies identified during audits are reported to the CJIS Division Advisory Policy Board (APB). The APB operates pursuant to the Federal Advisory Committees Act and is comprised of representatives from federal, tribal, state, and local criminal justice agencies who advise the FBI Director regarding CJIS Systems, such as the NGI System. System access may be terminated for improper access, use, or dissemination of system records.

The NGI System is not available to users unless there has been an application for, and assignment of an Originating Agency Identifier (ORI). Each using entity may only access the types of information for the purposes that have been authorized for its ORI. Such access is strictly controlled and audited by the FBI CJIS Division. Federal and state CSOs must apply to the FBI CJIS Division for the assignment of ORIs and FBI CJIS Division staff evaluates these requests to ensure the agency or entity meets the criteria for the specific type of ORI requested. The FBI CJIS Division maintains an index of ORIs and logs each dissemination of identification records to the applicable ORI.

In addition, the NGI System's Information System Security Officer is responsible for ensuring that operational security is maintained on a day-to-day basis. Adherence to roles and rules is tested as part of the security certification and accreditation process. All FBI employee and contractor personnel must complete privacy training and annual information security training. The training addresses the roles and responsibilities of the users of FBI Systems and raises awareness of the sensitivity of the information contained therein and how it must be handled to protect privacy and civil liberties.

The NGI System data, including the photos in the NGI IPS, are retained in accordance with the applicable retention schedule approved by the National Archives and Records Administration (NARA). NARA has approved the destruction of fingerprints and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age. NARA has determined automated FBI criminal history information and NGI System transaction logs are to be permanently retained. Biometrics such as photos may be removed from the NGI System earlier than the standard NARA retention period pursuant to a request by the submitting agency or the order of a court of competent jurisdiction.

NGI IPS Privacy, Risks, and Mitigation. Pursuant to its statutory authorities, the FBI has captured, maintained, and exchanged biographic and biometric information for many decades. Therefore, the photos in the NGI IPS do not constitute a new capture type or capture purpose. Instead, the NGI IPS provides the significant enhancement of FR technology for these photos.

The FBI recognizes that any biometric capability must be carefully assessed and tested to ensure sufficient reliability and minimum error. The FBI has conducted tests, which verified the NGI IPS is sufficiently accurate for all allowable candidate list sizes according to system requirements. The FBI has also evaluated detection rates for all allowable candidate list sizes ranging from two to fifty. Detection rates were verified to meet system requirements for each list size. Traditionally, NIST benchmark testing was performed approximately every three to four years. However, due to the speed at which technology advances, traditional methods no longer permit the level of technology awareness the FBI desires.

FBI NGI IPS Annual Accuracy Testing by NIST

FBI's ongoing FRT testing partnership with NIST enables the FBI to test its NGI IPS FRT technology annually, as well as permit other vendors to submit FR algorithms to NIST at least once a year.

NIST testing focuses primarily on algorithm accuracy across the following categories:

(1) overall accuracy (all categories combined); (2) across demographics (i.e., sex, race, age, twins, etc.): (3) image quality and properties (i.e., mugshot photos, unconstrained photos, poor quality photos, etc.).

As of January 1, 2024, the FBI successfully installed a new FR algorithm in the NGI System that is achieving accuracy rates of over 99 percent in current NIST testing for all candidate list sizes.

Figure 8 - NGI IPS Testing Snapshot

Internally, the FBI monitors the candidate photos returned to requesters in response to FRSs and works with those requesters in refining thresholds to improve the success of investigative FRSs performed in the NGI IPS. In addition, the FBI performs regression and baseline tests on the FBI test environments, which have been established with data and environments that are scaled representatives of the NGI IPS operational environment. The FBI continuously tests and evaluates the NGI IPS with each system changes, new algorithm installation, etc. to ensure that accuracy and system performance is not negatively affected. The FBI CJIS Division designed a FR operational evaluation tool in order to perform an annual FR analysis of the NGI IPS operational environment to ensure performance, system integrity, and assure that data does not change as the repository/NGI System changes over time due to architectural design (e.g., infrastructure or code), new or removed gallery enrollments, and vendor algorithm enhancements. The FBI CJIS Division began using this operational evaluation tool during the first quarter of calendar year 2020. Specifically, this operational tool's purpose is to evaluate the operational integrity of the FRS solution as change is introduced to the NGI IPS over time.

Although FR technology continues to improve, the FBI only permits the NGI IPS to be used as an investigative lead. The FBI has promulgated policies and procedures to emphasize that photos returned from the NGI IPS are not to be considered "positive" identifications, and searches of the NGI IPS will merely result in a ranked listing of candidate photos from the NGI IPS; the search result will include a specific caveat advising that the photos are to be used for investigative lead purposes only and that further investigation is required to determine the subject's identity. Other indicators and

factors must be required to take FR training prior to accessing the NGI IPS, in order to conduct an effective manual review of the returned candidate photos.

Photos submitted to the NGI IPS for retention by authorized users must meet the requirements as described above. In addition, it is the responsibility of the participating LEAs to develop appropriate use policies for NGI IPS FRS, in accordance with the applicable laws and policies of their relevant governmental jurisdictions. All appropriate use policies must protect the Constitutional rights of all persons. The LEA users must also ensure compliance with the FBI's *CJIS Security Policy*, CJIS User Agreement, and the *NGI IPS Policy and Reference Guide*. The *NGI IPS Policy and Reference Guide* expressly prohibits capture of probe photos in violation of an individual's First and/or Fourth Amendment rights.

The FBI made several decisions to protect privacy and civil liberties when it developed the FR capability within the NGI IPS. The FBI does not permit the searching or dissemination of civil photos in its repository. These photos were submitted for authorized noncriminal justice purposes, such as employment, licensing, and security clearances. By limiting the searchable photo repository, the FBI ensured that only those photos captured pursuant to a lawful LE purpose and positively associated with ten print fingerprints would be available for searching. Further, to maintain the integrity of the NGI IPS, the FBI stores information regarding the dissemination of photos and related information in audit logs but does not retain the actual probe photos. Although the probe photos must be obtained in furtherance of a LE investigation and must be captured in compliance with law and policy, such photos are not retained in the NGI IPS.

The increased retention of photos presents a correspondingly increased risk that the information may potentially be subject to loss or unauthorized use. The strong security features and robust audit processes already present in the NGI System mitigate this risk. The FBI CJIS Division's Audit Unit continues to conduct audits of FSLTT agencies enrolling and/or searching photos in the NGI IPS. The NGI IPS audits continue to be conducted in conjunction with pre-established National Identity Services triennial audits. In addition, the system stores information regarding the dissemination of photos and related data for audit logs. Dissemination of information is linked to the authorized NGI IPS user or the agency that requested the photo. This information is incorporated into the audit process and provides an enhanced capability for ensuring the information is being appropriately used and disseminated. Agencies requesting and receiving photos will be subject to training and audit requirements by the applicable state or federal agency and periodic FBI audit.

The increased retention and searching of photos in the NGI IPS present a privacy risk that the photos will be searched and used for purposes unknown to the individual who provided the photo. It also creates a risk that the photos will be disseminated for unauthorized purpose or to unauthorized recipients. Another privacy risk could be the improper access to the data or misuse of information in the NGI System, such as unauthorized electronic searching of the photos in the NGI IPS. These risks are mitigated through the NGI System's strict system security requirements and user rules regarding access and dissemination, as well as the periodic audits conducted by the FBI to ensure that system searches are relevant and necessary to the person's official duties. Dissemination of information is

linked to the authorized user and the agency that requested the information. The FBI CJIS Division's Audit Unit regularly visits agencies that are authorized to capture and submit photos. Allegations of misuse of FBI CJIS Systems, including the NGI System, are generally referred to the appropriate CSO of the jurisdiction where the misuse occurred, and the FBI responds to all such allegations.

The FBI has a substantial interest in ensuring the accuracy of the information in the system, and in taking action to correct any erroneous information of which it may become aware. The maintenance and dissemination of information must comply with the provisions of any applicable law, regulation, or policy, including the *Privacy Act*. Among other requirements, the *Privacy Act* obligates the FBI to make reasonable efforts to ensure the information that is disseminates to non-federal agencies is accurate, complete, timely, and relevant. This risk is further mitigated to the extent that an agency that contributes information to the NGI System has a process in place for access to or correction of the contributing agency's source records.

5.2 DHS Use Cases

DHS uses biometrics to support multiple aspects of its diverse mission set; facial recognition use cases are comprehensively documented in the Department's *Artificial Intelligence Use Case Inventory*.[56] Here, the report details two DHS LE components who use biometrics for diverse LE purposes, ICE and the USSS. While the two components have distinct mission sets, both rely on biometrics as core toolsets. A decision was made to focus on these lesser-known use cases to provide insight into how biometrics are used in use cases that mirror more directly the activities of SLTT LE.

5.2.1 Immigration and Customs Enforcement (ICE) Use Cases

ICE is responsible for conducting criminal investigations and enforcing immigration and customs law to safeguard our nation, its communities, and assure integrity in U.S. trade, travel, and financial systems. ICE uses the biometric technologies of face recognition and fingerprint as integral tools to support its various national security and LE missions to better assure it appropriately exhausts all opportunities to identify criminals, as well as provide a more efficient and less cumbersome means to track certain noncitizens as required by law. Face recognition technologies are used in counterterrorism and national security, in-person crime investigation, cyber-crime, forensic, and identity verification activities. Fingerprints are used with face recognition for identity verification use cases. ICE has two main operational directorates: Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).

Homeland Security Investigations (HSI) is the DHS principal *investigative* body responsible for "investigating, disrupting and dismantling terrorist, transnational and other criminal organizations that exploit the global infrastructure through which international trade, travel and finance move." Their broad legal authority includes terrorism, narcotics smuggling, gang activity, child exploitation, cybercrime, identity and benefit fraud, human rights, and war crimes. HSI works with state and local communities to investigate its cases, and primarily with the DOJ to execute search and seizures and prosecute criminal activity. ICE has over 6,000 special agents that work with over 2,800 task force officers representing key strategic FSLTT partners.[57]

Enforcement and Removal Operations (ERO) is the primary *immigration enforcement* body within the U.S. interior, arresting and removing foreign nationals "who undermine the safety of our communities and the integrity of our immigration laws."[58] ERO works closely with other immigration agencies as well as state and local communities who receive 287(g) authorities and resources to help secure the integrity of the immigration system.

5.2.1.1 Homeland Security Investigations

HSI biometric activities are closely monitored by the ICE Office of Information Governance and Privacy (OIGP), responsible for drafting its numerous PTAs and/or PIAs related to ICE biometric activities. HSI also has specific a policy on the use of facial biometrics (Memo M-21-0115) detailing HSI's policy for facial biometrics. Case management handbook HB 20-04 and EAGLE directive DIR 14-01 detail HSI's policy for fingerprints. These documents guide all HSI biometric use cases, including those described below.

Use of Images and Face Recognition. During its investigations, HSI routinely encounters digital images of potential victims or individuals suspected of crimes that are unable to be connected to identifiable information through existing investigative means and methods. HSI submits those images to government agencies and commercial vendors to compare against their digital image galleries via facial recognition processes. The agencies and vendors query their databases and return lists of potential candidates that HSI can use to produce investigative leads. Prior to operational use, each face image submitted to FRT is evaluated to assure:

- User-specific identity management and auditing capabilities robust enough to attribute each query to a specific user and time.
- Transmitted data is properly encrypted.
- PII is appropriately safeguarded.
- Probe images are not retained or re-disseminated.
- Query database only contains lawfully obtained images.

HSI uses facial recognition technology results only as investigative leads to further the identification of said unknown individuals and cannot be used as the sole source of identification justification, nor relied upon as the sole justification of identification. Any facial recognition results are used as an investigative lead to further the identification of unknown individuals. HSI uses FRT combined with traditional LE investigative techniques to help verify any potential FRT results that may lead to the true identity of the unknown individual in question. Other data supports identity findings, including biographic, contextual, and metadata.

Technical Capabilities for Face Images. HSI has a suite of face image capabilities it uses for various use cases where other investigative techniques have been found to be less than productive, especially

in cyber-related crimes. **HSI Forensic Lab (HSI-FL)** uses the Repository for Analytics in a Virtualized Environment (RAVEn) Facial Recognition Algorithm for clustering and case linkages. Prior to submitting an image to IDENT/HART's facial image service, HSI-FL will upload probe images into the HSI RAVEn for use with its facial recognition application HORUS, a Graphical User Interface (GUI) that will allow LE users to interact with and use the RAVEn algorithms. There is no PII associated with the images inside HORUS. HSI-FL runs one-to-many search queries to potentially link individuals from new probe photos to cases currently under investigation by HSI. Examiners then compare those cases to understand if evidence found in the probe photo's case or the returned image's case may assist investigators in generating a lead.

HSI Cyber and Operational Technology Unit's **Cyber Crimes Center's Child Exploitation Investigations Unit (CEIU)** uses FRT to investigate crimes against children, specifically the possession, distribution, receipt and production of child sexual abuse material and transnational child sexual offenders. The CEIU uses Clearview AI's external face services to help identify unknown victims of child sexual exploitation and abuse and their unknown offenders.[59] The HSI CEIU also collaborates with DHS S&T on the research and development of tools and technologies which seek to aid investigator and analyst review of child sexual abuse material. Some of these R&D projects use FRT to help quickly identify victims of child sexual abuse and their offenders.

The **HSI Cyber Unit** also employs FRT to help identify and locate suspects, victims, and witnesses for certain other types of criminal investigations that meet specific, defined parameters. Prior to performing a FRT search, licensed users are to first make reasonable efforts to identify, locate, or verify an individual through traditional investigative techniques. FRT results are treated by licensed HSI users as an investigative lead to further the identification of said unknown individuals, and not used for arrest or prosecution. These face image leads are not considered reliable as the sole source of identification.

ICE HSI CYBER INVESTIGATIONS: WAR CRIME HUNTER

Within ICE HSI's Countering Transnational Organized Crime (CTOC) Innovation Lab Human Rights Violator and War Crimes Unit, known as its **War Crimes Hunter**, the RAVEn algorithm works in combination with its HORUS user interface, isolating and clustering facial images. It also links individuals between other media found depicting human rights violations.

A query is then run against HSI-FL current gallery of images derived from fraudulent travel documents (this action is only taken within the War Crime Hunter application.).

It will not run queries against other galleries or

Figure 9 - War Crimes Hunter Snapshot

Certain HSI field offices maintain agreements with state and local LEA FRT services for use in authorized LE purposes. These agreements are reviewed and approved by HSI management prior to operational use and are only authorized for use within the geographic area of responsibility serviced by the local authority granting access to the FRT. Authorized LE purposes require that HSI's use must be either relevant and

necessary to an ongoing investigation relating to HSI's statutory authorities or part of an established HSI program or task force whose use of facial recognition is assessed for its impacts on privacy, civil rights and civil liberties.

Of note, HSI only uses identity verification 1:1 in only one instance: support of investigations where forensic document examination is required to identify identity document fraud. This use of FRT is supplemental to existing forensic examination practices.

5.2.1.2 Enforcement and Removal Operations

Use of Images and Face Recognition. LE coordination and partnership efforts within ERO involve the biometric and biographic identification of priority undocumented individuals who are incarcerated within federal, state, and local prisons and jails. **ICE's LE Support Center** coordinates response and enforcement actions with LE partners using biometrics to identify foreign-born individuals arrested for criminal offenses or wanted for crimes abroad. ERO's Compliance Assistance Reporting Terminal (CART) manages non-citizens on the non-detained docket, minimizing in-person check-ins with remote identity verification.

Technical Capabilities for Biometrics. The ERO's common database repository shared with other DHS immigration LE components is its Enforcement Integrated Database (EID).[60] EID supports the LE activities of certain DHS components. It contains all records created, updated, and accessed by several software applications collectively referred to as the ENFORCE applications. In recent years, EAGLE (booking application), EDDIE (Identification Environment), and DAVID (Digital Application for Victim Witness Identification)[61] have been added to EID to improve the event-based records and enable a person-centric view of records. EID maintains information to support the "identification, apprehension, and removal of individuals unlawfully entering or present in the US in violation of law, including fugitive aliens," and supports "identification and arrest of citizens and non-citizens who commit violations of criminal law enforced by DHS."[62]

The CART is a kiosk-based system designed to manage noncitizens on the non-detained docket within ICE's Alternatives to Detention Program (ATD). ATD is authorized in the 2018/2019 consolidated appropriations bills, and in 2020 its appropriations language was found in Senate Report 116-125, accompanying the *DHS Appropriations Act, S.2582*. The system is housed within ATD's Intensive Appearance Technology Services System (IATSS).[63] CART confirms identity biometrically, queries databases, asks specific questions, and conducts basic analysis (e.g., reviews changes in criminal history, checks for immigration court changes, parses responses provided by noncitizens, etc.) for events that indicate the need for direct communication between a noncitizen and a Deportation Officer.

Currently, CART captures fingerprints and a facial photo. While both fingerprints and photos are stored in OBIM's IDENT system, at present, only the fingerprints are compared to previously captured fingerprints to make an identity verification determination. The facial photo is used for testing the viability of 1:1 facial recognition to support future multi-modal comparisons. More recently, voice and face are also used for ATD IATSS individual verification.

5.2.2 United States Secret Service Use Cases

USSS has a mission that initially was to stop counterfeit currency during the Civil War in 1865. Its protective mission it is best known for was established in 1901 at the Treasury Department. After 9/11, USSS was brought into DHS. Its mission today encompasses both protection of dignitaries and the U.S. monetary system and includes Secret Service agents and its police force equivalent in its Uniformed Division. USSS protects dignitaries, locations, and secures national events, assessing threats, as well as investigations of financial crimes in both the physical and the cyber world. Financial crimes include those of counterfeit currency, credit card fraud, wire and bank fraud, computer network breaches, ransomware, and other cyber-enabled financial crimes.

> The 1994 Omnibus Crime Bill mandated the U.S. Secret Service to support major crime investigations by state and local law enforcement partners, including investigative and forensic biometric support.

Figure 10 - USSS Mandate

As required by the 1994 Omnibus Crime Bill (*Violent Crime Control and Law Enforcement Act),* the Secret Service was mandated to support major crime investigations by state and local LE partners, including investigative and forensic support. In addition, the USSS is a leading LE partner in forensic investigations with the National Center for Missing and Exploited Children, also required by law by the PROTECT Act of 2003.

USSS Forensic Services is responsible for adjudicating a variety of evidence and use biometrics as one of many pieces of evidence to support identification of persons of interest related to criminal investigations as well as to protect dignitaries and provide intelligence.[64] For example, USSS captures latent prints and/or DNA on threat letters, credit card skimming devices, counterfeit currency, firearms, and evidence from missing or exploited children cases for direct comparison to an individual or for biometric database search. USSS biometric activities pertaining to latent prints underwent an initial PTA in 2022.[65] Prior DHS PIAs were conducted in 2017,[66] 2020,[67] and May 2024.[68]

Like its counterparts at CBP and ICE, USSS Forensic Services is a nationally accredited forensics lab. Although Live-Scan fingerprinting is utilized for employment and criminal background checks, no biometric data repositories are held within USSS programs but for a threat letter database for handwriting comparisons, which has its own forensics PIA/PTA. Instead, all biometric queries are outsourced with results returned to USSS for examination. Established through user agreements, fingerprints (latent or contact) are queried through FBI's NGI and OBIM's IDENT finger and palm print repositories, where one-to-many search candidate lists are provided back to USSS Forensic Examiners for comparisons. USSS has policies in place for the submission, recording and searching of latent prints with the FBI and OBIM. OBIM is also used for FRT for investigative purposes, where images are searched by OBIM's IDENT examiners. No data is maintained by USSS,[69] and a PIA was approved on September 12, 2024.[70]

Mugshots and other investigative face images are queried through FBI NGI IPS and/or OBIM's IDENT. If there appears to be a match upon human examination in a criminal investigation, identity

information is provided back to agents in the field, which occasionally includes state and local LE partners. USSS relies on other Federal labs for DNA analysis of evidentiary and person samples and searching in CODIS. The iris modality is not used by USSS.

	Face	Fingerprints	DNA
Screening/Vetting		X	
Investigatory (in person crime)	X	X	X
Investigatory (cybercrime)	X	X	X
Forensic		X	X
Identity Verification	X	X	X

Figure 11 - USSS Forensic Lab Services by Biometric Modality and Use Case

5.3 DOJ Use Cases

For over 100 years DOJ components have utilized biometrics to support federal LE missions as well as federal, state, and local and international partners. The first biometric modality used by DOJ was fingerprints, but over the years the modalities of DNA, palmprints, face and iris have been added. The DOJ uses these biometrics in singularity, such as utilizing technology with facial recognition capabilities in child exploitation investigations, or multi-modal, such as face and finger in criminal investigations.

Biometric data increases the accuracy and reliability of identification systems, thereby reducing the risks to individuals of misidentification when the government accesses personally identifying information for a LE or national security purpose. By contrast, identification systems that rely on less reliable associational information such as names or social security numbers, are subject to much greater risk of inaccuracy, as well as fraud or other forms of manipulation, placing innocent individuals needlessly at risk.

5.3.1 FBI Facial Recognition Technology Use Cases

The FBI's mission is to protect the American people and uphold the U.S. Constitution. In meeting that mission it has 8 priorities: (1) protect the U.S. from terrorist attack; (2) protect the U.S. against foreign intelligence, espionage, and cyber operations; (3) combat significant cyber-criminal activity; (4) combat public corruption at all levels; (5) protect civil rights; (6) combat transnational criminal enterprises; (7) combat significant white-collar crime; and (8) combat significant violent crime. These priorities lead to FBI investigations, any one of which may at some point utilize FRT to develop leads or advance the case. FRT is an important method that the FBI can use in support of these priorities.

When seeking to identify an individual from a photograph, whether that individual is a suspect, victim, or witness, the FBI will send queries to systems such as the NGI IPS and OBIM's IDENT. The FBI may also utilize commercial FRT services for this purpose.

The FBI also leverages FRT to triage image and video evidence recovered in the course of an investigation. Such triaging may take the form of clustering to determine the number of subjects within a set of images and videos or locating specific individuals within a set of images and videos.

In all cases, FBI personnel must treat information resulting from FRT as an investigative lead only (not as a positive identification) and use established investigative methods to substantiate or invalidate the investigative lead.

5.3.2 The Combined DNA Index System (CODIS)

CODIS is a LE tool developed by the FBI that blends forensic science and computer technology by using DNA profiles to link violent crimes or identify criminal suspects. It enables the electronic exchange and comparison of DNA profiles between federal, state, and local forensic laboratories. CODIS links violent crimes, identifies known offenders, and identifies missing and unidentified persons. CODIS software development began as a pilot program in 1990 with 14 state and local laboratories. Today, CODIS software is in 205 domestic forensic laboratories and 125 international laboratories representing 61 countries. The FBI's Laboratory provides the CODIS software to domestic and international LE DNA laboratories at no cost.

CODIS is a distributed database with three hierarchical levels (or tiers)—local (LDIS), state (SDIS), and national (NDIS)—that flows information upward to each level. All three levels may contain forensic and offender-related indices. An LDIS laboratory generally contains forensic-related indices only and uploads those records to the SDIS-level laboratory for searching and storage. SDIS laboratories serve as the communications pathway between the local and national levels and perform intrastate searches.

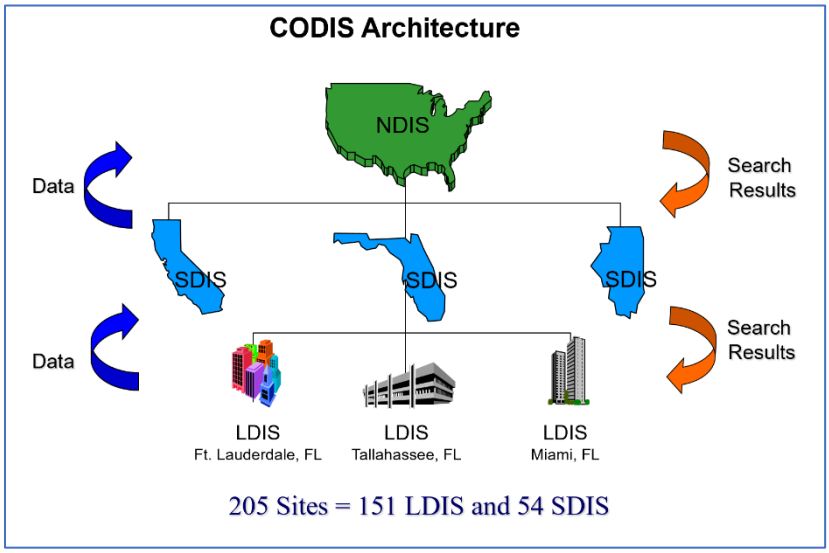

Figure 12 - CODIS Architecture: Local, State, Federal Certified Lab Relationship

The National DNA Index System was implemented in October 1998. NDIS is the highest level of CODIS, containing DNA records contributed by federal, state, and local participating forensic laboratories. NDIS is administered by the FBI and facilitates the interstate searching of DNA records. All 50 states, the federal government, the Department of Defense, the District of Columbia, and Puerto Rico participate

in NDIS. There are currently over 23 million DNA records in NDIS and over 675,000 investigations have been aided by CODIS.[71]

CODIS generates investigative leads in cases where biological evidence is recovered from crime scenes. For example, matches in the Forensic Index can link crime scenes, possibly identifying serial offenders. As a result, police from multiple jurisdictions can coordinate their respective investigations and share the leads they independently develop. Matches made between the Forensic and Offender Indices provide investigators with the identity of suspects. Since names and other personally identifiable information are not stored at NDIS, DNA analysts in CODIS laboratories that share profile matches contact each other to confirm candidate matches.

The DNA Identification Act of 1994 (34 U.S.C. §12591 *et seq.*; hereinafter "Federal DNA Act") authorized the establishment of the National DNA Index. This federal law specifies the categories of data lawfully maintained in NDIS and sets forth requirements for CODIS laboratories on quality assurance, privacy, and expungement.

Laboratories participating in NDIS (NDIS participating laboratories) are required to comply with the Federal DNA Act; the FBI Director's *Quality Assurance Standards for DNA Databasing and Forensic DNA Testing Laboratories* (QAS); the NDIS Privacy Act Notice; and the NDIS Operational Procedures.[72] All laboratories in the hierarchy are considered NDIS participating labs if they upload DNA records to NDIS. The Federal DNA Act governs what DNA records are eligible for NDIS upload. The gatekeeper of these records is the FBI's NDIS Custodian. State DNA database laws specify what DNA samples can be captured and databased at the state and local levels. At the state level, a State CODIS Administrator is responsible for compliance with all applicable state and federal laws.

CODIS Core Loci and Software. A CODIS DNA profile contains analysis results at each of the 20 Core Loci.[73] These loci are LE identification markers chosen specifically because they are not located within a gene or protein coding region. Instead, these markers are found in non-coding regions of the DNA molecule that do not reveal sensitive personal information such as medical conditions, genetic predispositions, or disease status that could compromise privacy interests.

No personally identifiable information associated with known DNA samples are stored using the CODIS software except DNA records in the Missing Persons Index, which may include a date of birth.

Figure 13 - DNA and PII

A full CODIS DNA profile contains a total of 40 numbers, representing 2 numbers for each of the 20 CODIS Core Loci. The CODIS software uses algorithms to compare the numbers in the DNA profile with other DNA profiles in the database. These algorithms are static and do not change during the search process. In addition, CODIS software does not integrate machine learning into its comparison algorithms.

Physical and computer safeguards are enforced to ensure the privacy of the DNA record information. These include locating CODIS servers in physically secure spaces, limiting access to servers and workstations to authorized CODIS users, and the use of a secure communications network by CODIS

laboratories that is restricted to criminal justice agencies. To protect the privacy of the DNA record information, the Quality Assurance Standard (QAS) and NDIS Operational Procedures restrict the release of personally identifiable information to instances in which an offender match is confirmed.[74]

The Federal DNA Act limits who may access DNA information in the National DNA Index. Access is generally restricted to criminal justice agencies for LE identification purposes. Defendants are also permitted access to their DNA sample and the analysis performed in connection with their case. If all personally identifiable information is removed, DNA profile information may also be accessed by criminal justice agencies for population statistics purposes, identification research, protocol development, or quality control reasons. The unauthorized disclosure of DNA data in the National DNA Index is subject to a criminal penalty not to exceed $250,000, imprisonment for one year, or both a fine and imprisonment.[75]

How does CODIS work? CODIS compares a target DNA record against other DNA records in the database. For example, in a sexual assault case when an evidence kit is captured from the victim, the DNA profile of the suspect may be developed from the swabs in the kit. The suspect's forensic profile is then searched against the state database of convicted offender and arrestee profiles. If the forensic profile generates a match to a known profile in the Convicted Offender or Arrestee Index, the laboratory follows mandatory procedures to confirm the match. Only if the match is confirmed will the laboratory obtain the identity of the suspected offender. Confirmation protocols include the analyst's evaluation of the DNA profiles and a review of the demographic information of the known individual before any identifying information is released. A forensic match to an offender profile in CODIS may be used to establish probable cause to obtain a search warrant authorizing the capture of a biological reference sample from the suspect. Once acquired, the casework laboratory can then perform DNA typing on the known reference sample to develop a DNA profile that can be used as evidence in court.

The forensic profile is also searched against the state's crime scene DNA database called the Forensic Index. If a candidate match against Forensic Index occurs, the laboratory will follow their match confirmation procedures. If confirmed, the match will have linked two or more crimes together. LEA investigating these connected can then share information obtained during each investigation and possibly develop additional leads.[76]

For CODIS cases involving missing person or unidentified human remains, when a search result involves DNA profiles that may have originated from the same individual, the term 'match' is used. Examples include unidentified human remains that generate a match to an offender, or a missing person generates a match to a forensic unknown. Match confirmation procedures that involve missing persons or unidentified human remains are like those described above. For searches involving DNA samples contributed by close biological relatives of a missing person, when the results indicate that the remains may be those of the missing person, the term 'association' may be used. Associations are made by using an identity search for single family references or a pedigree search for a ranked list of associations.

Established procedures direct which DNA records are searched for matches that will generate investigative lead information. One technique, known as familial searching, is a deliberate search of a LE database to identify close biological relatives of an offender whose profile is included in CODIS. This type of search is performed after a normal CODIS search has produced no matches. Familial DNA searching is not performed at NDIS but is legally authorized by several state jurisdictions.[77]

Privacy Protections. In 1996, anticipating the creation of the national DNA database, and in compliance with the *Privacy Act*, DOJ published a SORN for the NDIS.[78] As required by law, this Notice contains a description of the individuals covered by the system; the types of DNA records to be stored and searched in NDIS; the purpose and routine uses of the system; the practices for storing, accessing, and retaining the DNA records; and records access procedures.

Two additional published SORNs cover CODIS and NDIS records. They are the FBI Central Records System, FBI-002, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017);[79] and DOJ Information Technology, Information Systems, and Network Activity & Access Records, DOJ-002, 86 Fed. Reg. 132 (July 14,2021).[80]

Finally, the FBI has issued, and the Department of Justice has approved, PIAs for both CODIS[81] and NDIS. The CODIS PIA also addresses the DNA Index of Special Concern (DISC) for Rapid DNA searches. Together, these PIAs address: the purpose of CODIS/NDIS; system tiers and relevant indices; authorized system users; legal authorities authorizing capture and use of the information; the types of information captured, accessed, stored, and disseminated; limitations on information sharing; maintenance of privacy and security controls; and privacy risks and mitigation.

NDIS Procedures Board. In 2004, the FBI empaneled the NDIS Procedures Board composed of the federal, state, and local stakeholders from NDIS participating laboratories. The purpose of the Board was to develop procedures governing the operation of the National DNA Index. Chaired by the Chief of the FBI's CODIS Unit, the current Board consists of two representatives from the FBI Laboratory's DNA units, the NDIS Custodian, six representatives from state and local forensic DNA laboratories, the Scientific Working Group on DNA Analysis Methods (SWGDAM) Chair, and a representative elected by the State CODIS Administrators. The Board meets periodically to address issues raised by CODIS users and Administrators; provides guidance to the FBI and CODIS users on operational issues; and ensures that operational procedures comply with federal law and regulations. NDIS Procedures address many topics, including participation in NDIS; authorized CODIS users and DNA records; profile searching; approved CODIS Core Loci; expert systems, kits, and instruments; confirmation procedures for matches; and hit dispositioning. The NDIS Operational Procedures Manual is publicly available at the FBI's CODIS website.[82]

Quality Assurance. The Federal DNA Act directed the formation of a DNA Advisory Board composed of scientists from the public and private sectors. The Board's charge was to recommend quality assurance standards for use by forensic DNA testing laboratories. Its recommendations were originally adopted and issued by the FBI Director in 1998 and were most recently revised in 2020. The QAS are augmented by statutory requirements for laboratory accreditation and external audits every

two years.[83] When the statutory term for the DNA Advisory Board expired, the SWGDAM was tasked with recommending revisions to these QAS to the FBI Director.

SWGDAM serves as a forum to discuss, share, and evaluate forensic biology methods, protocols, training, and research to enhance forensic biology services. The full SWGDAM body meets twice a year but its committees and working groups frequently meet to develop guidance and supporting materials for the forensic DNA community. While SWGDAM makes recommendations for QAS to the FBI Director, only the Director is authorized by the Federal DNA Act to issue standards and to ensure that NDIS participating laboratories comply with those standards.

Federal law requires that CODIS participating laboratories undergo an external audit every two years to assess their compliance with the QAS. In addition, the Office of the Inspector General at the Department of Justice audits CODIS laboratories for compliance with both the Federal DNA Act requirements and their adherence to the NDIS Operational Procedures.[84] The FBI's CODIS Unit also conducts audits of NDIS participating laboratories as part of its administration of the National DNA Index System.[85]

5.3.3 Rapid DNA

Another tool in the CODIS hierarchy is Rapid DNA, the fully automated process of developing a DNA profile from a reference sample in one to two hours without human interpretation.[86] The FBI's Rapid DNA Booking Station initiative seeks to immediately enroll a qualifying arrestee's DNA profile in CODIS so that every arrestee is searched against all unsolved crimes in CODIS within 24 hours.

The FBI has also established the DNA Index of Special Concern (DISC), which contains complete crime scene profiles from unsolved homicide, sexual assault, kidnapping, and terrorism cases. Using Rapid DNA, DISC profiles can be searched at near real-time during the booking process. An exact match will generate an immediate notification to the booking agency, arresting agency, and investigating agency.

The Federal DNA Act was amended by the Rapid DNA Act of 2017,[87] which authorizes the FBI Director to "issue standards and procedures for the use of Rapid DNA instruments and resulting DNA analyses."[88] The FBI Laboratory Division worked with the FBI's CJIS Division and the CJIS Advisory Policy Board (CJIS APB) Rapid DNA Task Force to integrate Rapid DNA into the booking station process. Together with SWGDAM and the NDIS Procedures Board, *National Rapid DNA Booking Operational Procedures Manual and Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies*, as required by the Rapid DNA Act, were approved in 2020.[89]

A set of rigorous requirements outlined in the *National Rapid DNA Booking Operational Procedures Manual* must be met for federal, state, and local booking agencies to receive the FBI's Approval to Operate Rapid DNA in the booking station. Key requirements include the passage of a state arrestee collection law; integration of electronic fingerprint capture to obtain an arrestee's State Identification Number in near-real time; and a booking process that ensures only qualifying arrestees are processed. The State CODIS Agency is the primary entity responsible for the implementation of Rapid DNA in the booking station. Booking agencies must work with their State CODIS Agency to ensure all requirements are met when implementing Rapid DNA. IT enhancements, including automated fingerprint capture (Live Scan) and criminal history information integration, are infrastructure investments needed for booking station submissions of arrestee DNA profiles to CODIS. The FBI routinely inspects the implementation of Booking Station Rapid DNA by participating State CODIS agencies. Rapid DNA in the booking station is in the early stages of adoption. Two states are currently online with at least one active Rapid DNA booking station in each jurisdiction.

Only Rapid DNA Booking instruments approved by the FBI and NDIS can be used in the booking station. The FBI's approval of Rapid DNA Booking instruments and training LE to properly use the approved devices are important measures to ensure that that Rapid DNA analysis maintains the quality, integrity, and public trust of the National DNA Index.

Rapid DNA implementation in the booking station has many benefits. They include improved compliance with sample capture requirements, expedited profile searching, and the generation of immediate investigative leads while arrestees are in custody. In this way, Rapid DNA has the potential to both resolve unsolved cases and enhance public safety by identifying offenders while they remain in custody, thus potentially preventing the commission of new crimes.

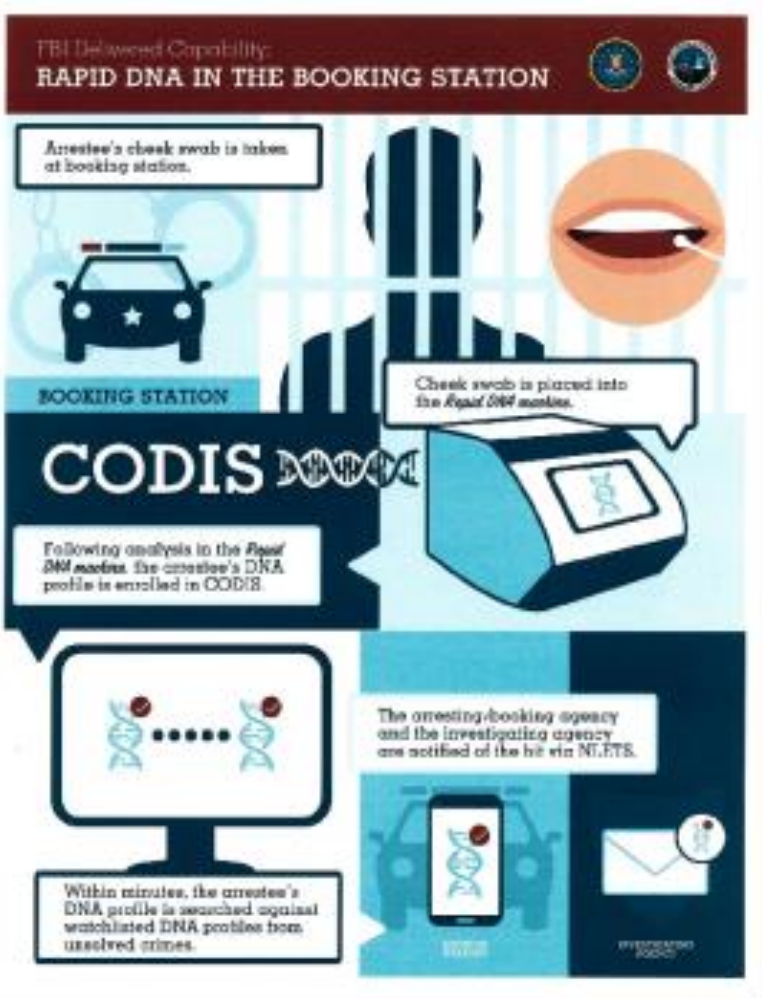

Figure 14 – FBI's Rapid DNA in the Booking Station

5.3.4 Investigative Genetic Genealogy

Another investigative tool used by the FBI is Investigative Genetic Genealogy (IGG)[90]. IGG is an investigative technique that combines DNA technology with traditional genealogy research to provide leads to LE from unknown crime scene DNA. IGG involves developing a genetic profile from crime scene DNA that is compatible with third-party online public genealogy services.

With IGG, the DNA profile developed from a crime scene sample is uploaded to direct-to-consumer (DTC) third-party[91] genetic genealogy services. Genetic associations made between the crime scene profile and potential biological relatives in DTC services, together with traditional genealogy research, can be used to provide LE with leads concerning the identity of the offender. The use of publicly available genealogy services distinguishes IGG from CODIS, which is a LE DNA database.

IGG Stages. Unlike CODIS, which uses short tandem repeat (STR) technology, IGG employs a high-density single nucleotide polymorphism (SNP) array to generate genetic data compatible with online genetic genealogy services. The SNP data file is uploaded to these genealogy services to locate genetic relatives of the source of the DNA (frequently referred to as the "person of interest").

There are several points during the IGG process at which LE interacts with vendor laboratories and third-party genealogy services. The steps of this process,[92] some of which are described below, typically include the following:

- Capture of a probative biological crime scene sample or unidentified human remains (UHR);
- Development of a short tandem repeat (STR) DNA profile (consisting of the CODIS Core Loci) from the captured sample;
- Pursuit of viable investigative leads, including a CODIS search using the STR DNA profile;
- Development of genome-wide SNP data from the captured sample;
- Upload to one or more third-party genealogy services using the SNP data to identify potential genetic relatives;
- Assessment of possible genealogical relationships between the potential genetic relatives and the person of interest, including building family trees;
- Investigation of leads generated by the genealogy research to identify the person of interest; and
- Obtaining DNA from the person of interest to develop an STR DNA profile with which to perform a one-to-one comparison to the crime scene STR DNA profile for exclusionary/inclusionary purposes;[93] or for a UHR, the capture of DNA from potential relatives for the development of an STR, YSTR, or SNP profile; or a mitochondrial DNA sequence to perform a kinship analysis comparison.

DTC testing and Genealogy Services. Most third-party genealogy services are maintained by DTC genetic testing providers. Currently, the largest providers are Ancestry, 23andMe, MyHeritage, and FamilyTreeDNA.[94] At this time, only GEDmatch[95] and FamilyTreeDNA permit LE access to their data, while allowing their users to opt-in or -out of LE searches.

Relative comparison services offered by DTC genetic testing providers and GEDmatch rank and report a user's matches according to how many centimorgans (cM) they share with each potential genetic relative. A cM is a measure of shared DNA segments or genetic linkage. The higher the number of shared cM, the closer the potential familial relationship.[96] After receiving this information, the user (or a genetic genealogist working on behalf of the user) can evaluate the genetic results and review/construct family trees to determine potential genealogical relationships. In some instances, relatives identified in a family tree might volunteer DNA samples for analysis to support or eliminate genetic relationships.

Law Enforcement Use. Generally, LEAs that currently employ IGG are using this technique on cold cases or unsolved violent crimes.[97] When collaborating with a forensic laboratory, the LEA will first send the crime scene sample to a forensic laboratory for STR DNA analysis and searching in CODIS. If the CODIS search fails to produce an investigative lead, the LEA or forensic laboratory may decide to use IGG according to applicable agency protocols.

Case acceptance criteria may include a review to ensure sufficient crime scene sample and/or DNA extract remains to proceed with IGG; consultation with the prosecutor's office to obtain approval or concurrence to use IGG; and the assurance that reasonable investigative leads will be pursued. Once approval is obtained, the LEA and/or laboratory will transmit the crime scene sample and/or DNA extract to a commercial genetic laboratory that will analyze the sample/extract using SNP technology.

The SNP data generated by the commercial laboratory is provided to the LEA for upload to one or more genetic genealogy services. The genealogy service(s) returns a list of the potential genetic relatives ranked by the amount of DNA shared with the uploaded profile. Trained personnel will then assess the genetic distances or potential relationships between those matches. Based upon the amount of shared DNA, these personnel will then construct and review family trees. Traditional investigative research can be used to evaluate whether, based on sex, age, location, and other relevant information, one or more potential biological relatives to the crime scene profile may be the person of interest. As an additional step, when a person of interest is identified, the LEA will obtain a DNA sample from that person, develop an STR DNA profile, and compare it with the crime scene STR DNA profile for exclusionary/inclusionary purposes.[98]

With a stated purpose "to promote the reasoned exercise of investigative, scientific and prosecutorial discretion," the U.S. Department of Justice issued an Interim Policy on Forensic Genetic Genealogical DNA Analysis and Searching in 2019.[99] This Interim Policy is applicable to all agencies in the Department of Justice and to all DOJ-funded IGG investigations at the federal, tribal, state, and local levels.

SECTION III: STAKEHOLDER VIEWS

6. Engagement and Analysis

In developing this report, the interagency committee engaged extensively with a wide range of stakeholders to gather diverse perspectives on the use of biometric technologies by law enforcement. The committee collaborated with the National Academy of Sciences (NAS), consulting through their Subcommittee on AI and Law Enforcement, and sought input from LEAs, civil rights and liberties organizations, criminal defense groups, and data privacy advocates. This engagement included written requests for comments and dedicated listening sessions.

Section 13(d) of Executive Order 14074 tasked the Attorney General with commissioning NAS to:

1. Conduct a comprehensive study of FRT, biometric information technologies, and predictive algorithms, with a focus on their use by law enforcement. This study was to assess how these technologies and algorithms are employed and address any concerns related to privacy, civil rights, civil liberties, accuracy, or disparate impacts.
2. Publish a report detailing the findings and offering recommendations on the use or restriction of these technologies by law enforcement.

By the time the Executive Order was issued in May 2022, NAS had already initiated a broad study on FRT at the request of DHS. Following this, the National Institute of Justice (NIJ) also requested NAS to conduct additional workshops on forensic DNA technologies and predictive policing technologies. This chapter outlines the NAS consensus study on FRT and the workshop on forensic DNA technologies, while the forthcoming workshop on predictive policing will be addressed in a future report aligned with Section 7.1 of Executive Order 14110, concerning the development and use of AI.

Additionally, this chapter includes a summary of external stakeholder comments and views, which reflect a variety of perspectives and may not align with the positions of DOJ, DHS, OSTP, or the interagency committee.

6.1 The National Academies of Sciences, Engineering, and Medicine FRT Study

In 2021, DHS OBIM requested that the National Academies of Sciences, Engineering, and Medicine (NASEM) conduct a study that considers current capabilities, future possibilities, societal implications, and governance of FRT. The FBI joined as a formal sponsor of the study in January 2022. The National Academies established a Committee on Facial Recognition: Current Capabilities, Future Prospects, and Governance, consisting of academics, legal scholars, biometric experts, law enforcement practitioners, and policy experts. The committee met in person in July 2022 and February 2023 and met virtually 16 times to receive briefings from experts and stakeholders, review relevant reports and technical literature, deliberate, and develop their report. The report was independently reviewed by individuals chosen for their diverse perspectives and technical expertise. NASEM released the consensus study report "Facial Recognition: Current Capabilities, Future Prospects, and Governance" in January 2024.[100]

While the study was commissioned independently of and prior to the publication of EO 14074, the consensus study highlighted several concerns relevant to EO 14074 around public trust in law enforcement, in addition to acknowledging that FRT "…can be a powerful aid for law enforcement in criminal and missing person investigations…" as noted elsewhere in this report. Some findings of both 1:1 and 1:N comparisons the report includes:

- "Many FRT systems deployed in the United States are trained on imbalanced, disproportionately White, data sets. As a result, the systems yield consistently higher false positive match rates when applied to racial minorities, including among populations that are Black, Native American, Asian-American, and Pacific Islanders. Although overall error rates are, in absolute terms, very low in the best systems today under ideal conditions, individuals represented in these populations are nevertheless at higher risk of being erroneously identified by certain facial recognition systems." As measured by NIST, a typical FRT system may have a 0.01 percent error rate on certain White populations (East European Males 20-35) and a 2 percent error rate on certain Black populations (West African Females 65-99).

- "FRT provides law enforcement with a powerful new tool for identifying individuals more rapidly, at a distance, and at greater scale and thus, depending on where and how it is used, has the potential to reinforce patterns or perceptions of elevated scrutiny by law enforcement and national security agencies, especially in marginalized communities. Put bluntly, some communities may be more surveilled than others, and increased scrutiny can lead to neighborhoods being designated as high-crime areas, a feedback loop that can further justify use of FRT or other technologies that disproportionately affect marginalized communities. Moreover, the use of FRT has raised concerns in some communities—including Black, Hispanic, and Muslim communities—reflecting in part differential intensity of past interactions with law enforcement and other government authorities."

- Reference galleries, notably those based on mug shots, do not include every possible individual of interest for a scenario and over retain individuals from particular groups. Differential representation in galleries—for example, uneven distribution of certain demographic features, such as age, gender, or ethnicity, between training images and reference images—increases the probability of a false positive match. On the other hand, individuals who are not in the gallery—because they never had a law enforcement contact—have no chance of false positive match or true match.

- Six of seven known cases of wrongful arrests in the United States involving identification using FRT are of Black individuals.[101] Factors contributing to the arrests were combination of systemic, technology, and human effects. These included over confidence in the technology, low-quality probe images (such as poor-quality screen capture from security camera footage), low-quality or dated candidate images (such as expired driver's license photos), poor institutional practices, (such as making arrests based solely or largely on FRT results), poor FRT procedures (such as using fixed-length candidate lists without minimum similarity thresholds), inadequate training, and poor police investigative processes.

- Human review of FRT matches in criminal investigations is integral to the process. But humans are fallible. A human review can produce false positives, leading to wrongful arrest, and false negatives, resulting in an unidentified suspect. The use of security camera footage to identify suspects in a criminal investigation is one of the most common applications of FRT. When humans review long lists of candidate photos, there tends to be opportunities for false matches. Scientific studies of "unfamiliar face comparisons" have demonstrated even the most proficient groups, forensic face examiners and super recognizers, have approximately one percent likelihood of assigning a highly confident match decision to a nonmatching pair of face images. Additionally, review accuracy depends on the demographics of reviewed faces, and humans of one race give reduced accuracy when reviewing photographs of another.
- The accuracy of FRT algorithms is increasing. False nonmatch error rates of state-of-the-art FRT systems are reducing annually by approximately a factor of two. A typical FRT algorithm has false nonmatch rate of about 0.3 percent at a false match rate of 0.0001 percent. The most accurate algorithms also generally have the lowest demographic variance.
- A reference database can include millions of individuals. With larger reference databases, the number of match candidates must be increased to maintain a constant match rate. Correspondingly, the false match rate increases but often at substantially smaller degree than the population increase.
- Indiscriminate use of FRT in public and quasi-public places can have significant impacts for privacy and related civil liberties—especially absent regulation or other controls on how such information is captured, stored, and used. Furthermore, the proliferation of both privately-owned and LE-operated cameras can amplify the threat.

The study committee issued several recommendations. Regarding "mitigating potential harms and laying the groundwork for more comprehensive action," the committee provided the following two recommendations regarding LE use of FRT to identify suspects in criminal investigations.

> Recommendation 1-3: The U.S. Department of Justice and U.S. Department of Homeland Security should establish a multi-disciplinary and multi-stakeholder working group on FRT to develop and periodically review standards for reasonable and equitable use, as well as other needed guidelines and requirements for the responsible use of FRT by federal, state, and local law enforcement. That body, which should include members from law enforcement, LE associations, advocacy and other civil society groups, technical experts, and legal scholars, should be charged with developing:
>
> a. Standards for appropriate, equitable, and fair use of FRT by law enforcement.
>
> b. Minimum technical requirements for FRT procured by LEAs and a process for periodically reevaluating and updating such standards.
>
> c. Standards for minimum image quality for probe images, below which an image should not be submitted to an FRT system because of low confidence in any ensuing match. Such standards would need to take into account such factors as the type of investigation

(including the severity of the crime and whether other evidence is available) and the resources available to the agency undertaking the investigation.

d. Guidance for whether FRT systems should (1) provide additional information about confidence levels for candidates or (2) present only an unranked list of candidates above an established minimum similarity score.

e. Requirements for the training and certification of LEOs and staff and certification of LEAs using FRT as well as requirements for documentation and auditing. An appropriate body to audit this training and certification should also be identified.

f. Policies and procedures to address LE failures to adhere to procedures or failure to attain appropriate certification.

g. Mechanisms for redress by individuals harmed by FRT misuse or abuse, including both damages or other remedies for individuals and mechanisms to correct systematic errors.

h. Policies for the use of FRT for real-time police surveillance of public areas so as to not infringe on the right of assembly or to discourage legitimate political discourse in public places, at political gatherings, and in places where personally sensitive information can be gathered such as schools, places of worship, and health-care facilities.

i. Retention and auditing requirements for search queries and results to allow for proper oversight of FRT use.

j. Guidelines for public consultation and community oversight of LE use of FRT.

k. Guidelines and best practices for assessing public perceptions of legitimacy and trust in law enforcement use of FRT.

l. Policies and standardized procedures for reporting of statistics on the use of FRT in law enforcement, such as the number of searches and the number of arrests resulting from the use of FRT, to ensure greater transparency.

Recommendation 1-4: Federal grants and other types of support for state and local LE use of FRT should require that recipients adhere to the following technical, procedural, and disclosure requirements:

a. Provide verified results with respect to accuracy and performance across demographics from the National Institute of Standards and Technology Facial Recognition Technology Evaluation or similar government-validated third-party test.

b. Comply with the industry standards called for in Recommendation 1-2—or comply with future certification requirements, where certification would be granted on the basis of an independent third-party audit.

c. Use FRT systems that present only candidates who meet a minimum similarity threshold (and return zero matches if no candidates meet the threshold) rather than returning a fixed-

length candidate list or "most-probable candidate" list when the output of an FRT system is being used for further investigation.

d. Adopt minimum standards for the quality of both probe and reference gallery images.

e. Use FRT systems only with a human-in-the-loop and not for automated detection of offenses, including issuing citations.

f. Limit the use of FRT to being one component of developing investigative leads. Given current technological capabilities and limitations, in light of present variations in training and protocols, and to ensure accountability and adherence with legal standards, FRT should be only part of a multi-factor basis for an arrest or investigation, in line with current fact-sensitive determinations of probable cause and reasonable suspicion.

g. Restrict operation of FRT systems to LEOs that have sufficient resources to properly deploy, operate, manage, and oversee them (an adequate certification requirement would presumably ensure that such resources were in place).

h. Adopt policies to disclose to criminal suspects, their lawyers, and judges on a timely basis the role played by FRT in LE procedural actions such as lead identification, investigative detention, establishing probable cause, or arrest.

i. Disclose to suspects and their lawyers, on arrest and in any subsequent charging document, that FRT was used as an element of the investigation that led to the arrest and specify which FRT product was used.

j. Publicly report on a regular basis de-identified data about arrests that involve the use of matches reported by FRT. The reports should identify the FRT system used, describe the conditions of use, and provide statistics on the occurrences of positive matches, false positive matches, and non-matches.

k. Publicly report cumulatively on any instances where arrests made partly on the basis of FRT are found to have been erroneous.

l. Conduct periodic independent audits of the technical optimality of an FRT system and the skills of its users, determining whether its use is indeed cost-justified.

On the topic of "fostering trust and mitigating bias and other risks," the committee provided the following recommendation:

> Recommendation 2: Developers and deployers of FRT should employ a risk management framework and take steps to identify and mitigate bias and cultivate greater community trust.
>
> Recommendation 2-1: Organizations deploying FRT should adopt and implement a risk management framework addressing performance, equity, privacy, civil liberties, and effective governance to assist with decision making about appropriate use of FRT.

Recommendation 2-2: Institutions developing or deploying FRT should take steps to identify and mitigate bias and cultivate greater community trust—with particular attention to minority and other historically disadvantaged communities. These should include:

a. Adopting more inclusive design, research, and development practices.

b. Creating decision-making processes and governance structures that ensure greater community involvement.

c. Engaging with communities to help individuals understand the technology's capabilities, limitations, and risks.

d. Capturing data on false positive and false negative match rates in order to detect and mitigate higher rates found to be associated with particular demographic groups.

6.2 OSTP Biometrics RFI

In 2021, the OSTP released a Request for Information (RFI)[102] on public and private sector uses of biometric technologies. OSTP received input and comments from various stakeholders across academia, civil society, and academia, and identified key recommendations:

- **Bans, Prohibitions, and Moratoria**: Some stakeholder submissions called for prohibitions on capturing or using biometric information without explicit consent; banning the use of any biometric technology (including face, voice, and gait) for mass surveillance or the use of facial recognition in a manner that could chill First Amendment activities or otherwise infringe on human or constitutional rights; and prohibiting the sale or transfer of biometric data to third parties.
- **Recommended Implementation Practices:** RFI respondents made numerous recommendations on various aspects of the implementation of biometric technologies, such as requiring consent or an opt-in system, plain language and transparent disclosures, data minimization and required audits to test effectiveness and identify biased outcomes, and human oversight for manual correction.
- **Disclosure**: Numerous RFI respondents recommended that the use of facial recognition or other biometrics during an investigation should be disclosed to defendants as a matter of due process. Respondents also advised that investigative biometric technologies should meet the same standards of accuracy and reliability expected of other forms of court admissible evidence and should demonstrate their capacity for just and equitable application prior to their implementation in the criminal legal system.

6.3 Summary of the NASEM DNA Workshop

On March 13, 2024, NASEM convened a two-day public workshop, "Law Enforcement Use of Probabilistic Genotyping, Forensic DNA Phenotyping, and Forensic Investigative Genetic Genealogy Technologies: A Workshop."[103] The Committee's agenda explored how predictive forensic DNA technologies are currently being used in the criminal justice context across FSLTT actors; the reliability and accuracy of methods; relevant legal considerations and precedents that accompany the

technologies; and concerns and considerations (e.g., accuracy, analytical sensitivity and specificity, ethics, privacy, civil rights, civil liberties, and disparate impact) that need to be assessed in implementation and the use of genetic material by law enforcement. Three DNA technologies were examined during the workshop: PGS, forensic DNA phenotyping (FDP), and forensic investigative genetic genealogy (FIGG).

PGS has two main functions, to 1) deconvolute mixed DNA profiles and 2) calculate the likelihood ratio of a DNA profile comparison to a person of interest (POI) after separating the mixed profiles in the evidential sample. Forensic Science Service Providers (FSSPs) have been doing mixture deconvolution manually, however, the advent of PGS helps reduce mathematical errors, render consistency, and decrease the time needed for profile comparison, thus, it has been an important technology to help LE solve serious crimes. It is important to acknowledge that sources of variation will still exist, even with the use of PGS, that are external to use of the software such as human and technological factors inherent in processing a sample and using the software. Use of PGS has helped DNA mixture interpretation evolve to providing a statistical weight in the form of an LR which makes use of more variables within the DNA chromatographic profile, such as peak height. Through a trained user, the LR generated by PGS helps put the evidence in context for a LE investigator to exclude suspects, follow leads, and pursue the possibility of securing more evidence.

Four needs surrounding PGS technology were echoed throughout the workshop:

- The need for training. An analogy shared was that we do not need to be mechanics to drive a car, but we need to know how to operate and maintain it. As PGS users, forensic analysts do not need to be statisticians, but they do need to understand PGS to recognize inconsistencies, sufficiently operate the software, and maintain its use. In addition, a training need is present for judges and attorneys. While attorneys and judges are not users, they make decisions in the courts associated with this technology and need to be able to translate PGS strengths and limitations in a court of law.

- The need for fair and equal access to PGS. A license for a commercial PGS is cost-prohibitive for the prosecution and defense, alike, creating a disparate impact on defendants. It is also cost-prohibitive to researchers who want to study, understand, and describe its implementation.

- The need to prohibit the blocking of e-discovery of evidence. Assertion of trade secret protection prevents adversarial scrutiny by expert witnesses which may disproportionately harm communities that are already overrepresented in the criminal legal system.

- The need for independent government oversight, regulation, and independent review of PGS. The call for oversight should cover auditing, verification and validation of the software, and validation of software by those with no ownership or investment in its use.

To address these needs, multiple ideas were put forth by the workshop as solutions or steps towards addressing the need. The first was to incorporate procurement guidelines and conditions for federal grants to FSLTT LEA. An example would be requiring adherence to standards relating to PGS for a

LEA to receive federal grants. This condition would incentivize LEAs to abide to a minimum standard of use. The second was to make trade secrets available for independent review through the use of protective orders. This idea would help increase transparency of the software and allow for appropriate adversarial scrutiny. Lastly, the workshop suggested that PGS should be subject to peer-review and independent research. Making PGS more available for the legal community and researchers increases transparency and, ultimately, equity.

There are benefits to using PGS, such as decreasing subjectivity in DNA profile interpretation. Although PGS provides more information for the factfinder, more training is needed to understand the impact of this information. The need for independent government oversight and regulation in PGS was echoed throughout the workshop, and we will see it repeated in discussions on FDP and FIGG.

A second way of using the genetic material recovered in an investigation is FDP, a technology that helps predict physical characteristics from DNA samples. FDP makes use of genetic variations linked to specific traits to predict physical characteristics such as eye color, skin color, and hair type. It then uses statistical techniques to predict a range of physical characteristics based on the genetic variations in a sample. FDP is being applied by LE through contracting with external vendors or private consultants to generate predicted images of perpetrators or missing persons. The goal from these images is to generate investigative leads. Currently, FDP is not widely adopted, yet, according to the workshop, has proved useful in some notable cases and detrimental in others. A benefit of this technology is the broad application of it which ranges from criminal cases to unidentified human remains and missing persons cases. However, improperly communicating the meaning of an FDP result to the public can further marginalize persons of color.

FDP accumulates intelligence on physical traits to narrow a list of suspects or missing person by a probable range of characteristics. A differentiation must be made between the DNA markers that are targeted in PGS from those targeted in FDP. The DNA profile generated by an FSSP using PGS contains markers that can be directly compared between evidence and an individual, whereas, in FDP, the markers are not individual-specific, and a comparison cannot be made. Currently, physical traits such as hair color, skin color, ancestry, and age range can be predicted. These traits are not produced from one gene; they are 'polygenic' meaning multiple genes are involved with producing a trait. A misconception that ancestry predicts the physical traits of a person, and vice versa, was noted at the workshop. Ancestry and physical traits are independent tests that complement each other as intelligence, not substitute. The workshop emphasized that the probability of traits should not be combined. In addition, the workshop indicated that the limitations of FDP may be holding back its utility. FDP cannot predict body choices or modifications, nor can it inform scientists when the genetic material that gets captured in an investigation was deposited. Although the results that FDP provides are based on probability, interpreting the result is subjective. The workshop posed a question of who should be responsible for understanding these limitations, the researchers developing the markers, LE as the end user, the media that disseminates the results, or everyone involved in the technology.

Multiple needs for FDP were identified by the workshop and summarized as the following:

- The need for research. As a less mature technology, FDP requires more research. For example, a threshold for accuracy should be identified and evaluated in the lab using pristine and real-world conditions. Research is also needed on the design and use of prediction models and the performance of the predictions on independent test sets. Additionally, research is needed in understanding which and how many visual outputs are provided and how they aid in interpretation by society to begin answering the question of "what benefit comes from releasing a visual representation." An available standardized dataset is also necessary to make the most accurate predictions. Lastly, data about the current use of FDP needs to be captured to replace antidotal evidence and to begin making more informed conclusions about the technology. These are research areas raised during the workshop that not only need to be addressed, but the findings need to be reported via peer-reviewed publication.
- The need for regulation and oversight. It was recognized that some research is necessary to inform regulation and oversight. Guidelines are needed on reporting results, including the caveats, and regulation for providing images to the public as this is where harm can be done to all communities but most specifically marginalized communities.
- The need for training. Educating researchers about the downstream impacts of FDP can help provide them a better understanding of the use of the technology to then mitigate concerns proactively. Training is necessary for the different actors and consumers involved with the use of FDP for them to understand the terms of its use and its limitations and disclaimers.

Lastly, the workshop explored how genetic material obtained during a forensic investigation can undergo advanced DNA sequencing techniques and traditional genealogical research methods in IGG. This technology involves entering the DNA profile into a genealogy database which uses algorithms to identify potential familial relationships between the sample and database users. Family trees are then constructed by a genealogist to help identify candidates of the unknown forensic sample. The DNA sequencing needed for upload into a genealogy database is typically outsourced to a vendor laboratory as it extends beyond the traditional DNA testing done by traditional FSSPs. LEA are increasingly staffing experts in genealogical research to conduct genealogical research and build family trees for IGG. Currently, this technology is being used at limited LEA, however, it is rapidly expanding in use and demand.

IGG has two components, DNA sequencing techniques and genealogical research, both of which have been scientifically tested and determined to be technically sound. Putting these two methods together for investigative purposes is where the novelty lies. An IGG candidate sample is first identified when no hit in CODIS is made and meets specific conditions for DNA sequencing. Next, the DNA profile generated from advanced sequencing, like FDP, is used for indirect comparisons and in this technology, for kinship analysis in a genealogical database. Traditional genealogical research using publicly available information is conducted to produce an investigative lead. Any investigative leads are confirmed with direct comparisons of a traditional DNA profile by an FSSP. IGG has been an option when all other investigative techniques have been exhausted and the genetic material is of sufficient quantity and quality for the sequencing technique. To date, greater than 1,000 cases have benefited from IGG in the United States which include criminal, cold, unidentified human remains (UHR), and missing persons cases. IGG has not garnered as much use abroad. It was noted that seeing IGG being used for present cases and not only cold cases, is ideal as it helps increase public safety. Interestingly, based on public surveys, there is strong public support for the use of IGG, a finding that has not changed over time. In fact, more than 90% of survey respondents believe that IGG should be used for investigating violent crimes. The workshop discussed that the duality of these two scientific methods brings about a limitation for tribes, in that DNA testing is incongruent with how tribes determine kinship and is performed outside the sovereignty of the tribe. A separation of the methods presents their own limitations, samples for DNA testing need to meet a threshold of quality, quantity, and mixture status to generate a DNA profile for upload into a genealogy database, while genealogical research uses public information therefore databases may have errors because of adoptions and misattributed relationships.

The resounding message of the workshop was that IGG has the potential to prevent serial offenders, deter potential offenders, prevent wrongful convictions, clear backlogs, and cold cases but additional needs need to be addressed. Addressing the addition needs will ensure individuals' privacy, civil rights, and ensure civil liberties are protected. The following needs were identified in the workshop:

- The need for training. There is a need to educate users of IGG workflows including but not limited to understanding and adhering to database terms of service (ToS), using accredited labs and vendors, and its limitations. LE needs training on the limitations and ramifications of IGG to help manage expectations of family and victims. While the public needs to be informed and engaged to understand how their genetic information may be used if they opt-in for LE use.

- The need for regulation and oversight. A best practice recommendation was a specific need stated by most at the workshop. Oversight is needed, and it was recommended that this federally supported committee appointed with diverse stakeholders can help drive policy. Lastly, regulation is needed to hold those accountable who misuse the technology, for example those that are not using accredited vendors or laboratories, those that are not abiding by the ToS for public databases, or those that are not confirming an IGG lead with traditional DNA testing so that consequences are realized.

- The need to maintain public trust and safety. Moving IGG use toward present cases can increase public safety, especially for serial offenders. Identifying who and defining why people are IGG experts is a necessary step to maintaining public trust. As policies, laws and ToS are created and revised, IGG actors must adhere to them to protect the rights and privacy of those involved in the investigative process and genealogical research. All authorities should be cognizant of "function creep" of using genetic database information to ensure public trust remains intact.

During the workshop, panelists discussed Maryland as an example for addressing these needs with an enacted House Bill that establishes requirements and procedures for IGG. Initially, a ban was placed on using IGG in Maryland, stakeholders then focused on educating legislatures and actors on IGG to create a piece of legislation that protects the privacy, civil rights, and civil liberties of individuals. The National Technology Validation and Implementation Collaborative (NTVIC) recently published policies and procedures for IGG providing an additional example of progress being made towards the identified needs. Additionally, the largest consumer genealogy database available to law enforcement has more prominently placed the decision for an individual to 'opt-in' or 'opt-out' to their genetic information being searchable by LE. With the rapidly expanding use of IGG, addressing these needs dictates acceleration of activities toward fulfilling the needs.

Six thematic needs quickly and repetitively emerged about PGS, FDP, and IGG: transparency, regulation, accountability, education, research, and funding. They include:

Transparency – Examples of a lack of transparency by vendors were brought to light during the workshop, including PGS developers, commercial FDP companies, and public genealogy databases. A lack of transparency was noted regarding how conclusions of these technologies are used to implicate people. Failure to communicate risks and limitations of technologies to those impacted by their use decreases transparency.

Regulation – Oversight and regulation was noted as a need for all three technologies discussed which should emphasize the frequency of its mentioning at the workshop. The federal government was identified as the body that needs to bring diverse stakeholders to the table to enact regulation and oversight on the use of these technologies. There is a need for not only best practice recommendations, standards, audits, and accreditation but laws that are enforceable to regulate conduct.

Accountability – Stemming from upholding and enforcing regulations, accountability is needed. All actors involved in the use of these technologies need to be held liable for not adhering to regulation. Actors may include researchers, FSSPs, vendors, software developers, LE, reporting officials, and policy makers.

Education – The need for a determination regarding who needs to be educated, on what, and how is expansive is critical. Users of the technologies need specialized training that may extend into new scientific and statistical concepts. Researchers need to be educated about downstream potential uses of technology they are developing. All parties need to be educated on new regulation to use these technologies effectively and equitably. The public also needs to be educated, not only about the technologies and their limitations but understanding how their genetic information can or may be used, their rights surrounding genetic data, and interpreting consent forms.

Research – Specific research needs were identified for each technology as well as overall research needs. A call for quantitative and qualitative research on the disproportionate impact of these technologies on brown and black communities was made. Additionally, a multi-site survey on DNA cases, the technology used, crime rates, clearance rates, and other factors was suggested to help document societal impacts of these technologies. Data could be gathered with regulated reporting on the use of these technologies.

Funding – The need that underlies the above five thematic needs is funding. Research funding is necessary to ensure the accuracy and reliability of these technologies, that societal impacts are understood, and these technologies do not have a disparate impact on people. Discussions of funding also included two recommendations, to add procurement requirements to federal funds to incentivize awardees to adhere to regulation and incorporate a public education component to all awards.

6.4 Public Request for Input and Listening Sessions

In 2023, the Department of Justice solicited public input on LE use of facial recognition and biometric technologies. In response, stakeholders from civil society, academia, and industry provided detailed 32 responses and raised a number of key insights and concerns. Various themes arose from public responses, including around recommendations for prohibited uses, evaluation and audits, due process protections, training and oversight, notice and disclosure, and other topics.

Multiple responses suggested prohibitions on particular LE uses of FRTs, and some groups called for a federal moratorium on the use of all FRT by LE and immigration agencies. Some responses called for prohibiting the use of FRT and other biometric technologies in public places and in any setting that could impact the ability of individuals to exercise their First Amendment rights. Some organizations requested that LE limit acceptable uses to specific cases, such as only for investigation of violent crimes, or when granted a search warrant or supported by probable cause. Another organization called for prohibiting the use of FRT by any program covered by Title VI of the Civil Rights Act of 1964, and creating a limited waiver system, which could be granted on a case-by-case basis when a specific technology has been affirmatively shown to be not discriminatory on the basis of protected characteristics.

Respondents also noted the importance of data protection, minimization, and retention requirements, such a prohibition on the retention of biometric data after identity is confirmed. Various groups also suggested prohibiting the use of illegally obtained probe and reference gallery images for FRT, including images captured in manners that violate state or federal privacy, copyright, or other laws.

Multiple responses recommended the creation of guidance and policies for required notice and disclosure to individuals and their legal representation upon arrest or any LE engagement that involved the use of an FRT. In addition to a notice system, certain advocacy groups stressed the need for contestability, so that individuals and defendants have the opportunity to contest and challenge use of FRT, including through conducting independent tests of the system's accuracy and functionality. In line with that goal, various responses called for FRT service providers and LE to ensure there is a mechanism to produce a record that can be used to audit or review the information used to make a match to a person.

Third-party audits and certifications were a key theme in stakeholder comments. Multiple responses called for DOJ and DHS to require regular independent auditing of all surveillance technologies both prior to deployment and periodically thereafter, which would be made transparent or available in some form to the public. Additionally, responses called for required specialized training for LE that use or engage with FRTs.

Multiple responses requested that any federal guidance or policies be extended to SLTT governments, and that federal agencies require all recipients of new grants and contracts to also comply with requirements. Many state and local LEAs have received federal funding and grants for FRT. For example, as of 2014, Pinellas County, Florida had received approximately $15 million in federal grants for its facial recognition program. Stakeholders raised concerns that FRT systems purchased through federal funds, such as Pinellas' system, have few—if any—reporting requirements for transparency.[104]

Finally, some responses discussed the importance of OMB's draft memorandum on federal government use of AI, and the need for comprehensive impact assessments to document the benefits and risks of LE use of technologies including FRT.

One respondent included concerns regarding DNA technologies. Two concerns were noted: DNA technology's high privacy risks and the transparency needed to ensure justice and accountability. Being that DNA technologies makes use of an unchangeable part of a person and can contain sensitive information, the following protections were recommended by the respondent: capture of reference samples being limited to those charged of a crime of violence, capture and analysis of DNA must require a warrant, DNA processing should only be available for the purposes of identifying an individual, database must assure the use of the genetic information is limited to its intended purpose, and DNA samples and its record must be destroyed after its purpose has been served. The transparency concern made by the respondent highlighted multiple examples of the lack of access to algorithms, source code, parameters, population baselines, and other information regarding the use of probabilistic genotyping software. They argue that without access, errors and bias cannot be identified and defendants do not have a full and fair opportunity to mount a defense or exercise their Confrontation Clause rights.

The call for comments received one response from a group representing local LEAs. The response stressed the critical role of FRT, forensic genetic genealogy (FGG), and Rapid DNA technologies in generating investigative leads, ensuring public safety, and supporting emergency management missions. The group acknowledged the importance of effective policies to manage risk and protect the public's privacy, civil liberties, and civil rights, and highlighted that harm can occur when policies of FRT usage is not strictly followed. Consequently, the group supports the establishment of robust FRT and FGG usage policies.

Three industry groups also provided responses. Responses emphasized the need for robust and accurate technologies, such as those able to mitigate fake or spoofed biometrics. Given the continual improvement in technology, LEAs should use the most recent systems and only use FRT algorithm versions that have been directly evaluated by rigorous testing such as NIST Face Recognition Technology Evaluation (FRTE). Responses also noted that while a technology is often not harmful itself, the misuse of a technology can cause harm and infringe on civil liberties. The groups recommended that forensic biometric analysis always be an option following crimes or emergency events. One response cautioned that without FRT, police operate "manually by looking through hundreds of mugshots with victims, canvassing areas with photos or searching a database using vague suspect descriptions or names" to identify persons of interest. On the other hand, the same response also recommended that real-time biometrics for surveillance be restricted (e.g., to identifying terrorists or finding missing persons) and only be authorized by court order. One response recommended that all FRT reviewer matches be confirmed by a second reviewer unconnected with the investigation. Yet another response stated that investigators should treat FRT matches as investigative leads "with the same skepticism as an anonymous tip." One response recommended that policy should mandate all operational candidate lists be government-owned to close the possibility of bypassing lawful investigative procedures. Multiple responses recommended that FRT use in a criminal investigation should be discoverable under applicable rules of evidence. All responses stressed the need for adequate training, and all responses highlighted principles for responsible use of FRT.

SECTION IV: BEST PRACTICES AND GUIDELINES

7. Overview and Organization

This chapter seeks to bring together lessons learned from years of implementing biometric activities, especially facial recognition technology, for specific federal law enforcement activities and attempts to provide guidance to a broader audience of law enforcement, as required by EO 14074. The chapter emphasizes the need for policies that reflect actual use cases and are limited to that scope, transparent and fully engage appropriate communities and stakeholders in their creation, and that privacy, civil rights and equal treatment be of paramount import when a biometric system—especially those containing FRT—are considered. This underscores the need for a way forward that is cohesive and representative of all equities both within federal government, and with its external stakeholders. Last, the chapter highlights the requirement that biometric technologies be tested and continue to be developed within minimal demographic differential treatment, and that every aspect of a biometric architecture adhere to legal requirements and appropriate standards.

7.1 Fingerprint, Iris, and DNA

In addition to the best practices specific to FRT, DOJ and DHS refer FSLTT LEAs to the widely accepted standards and best practices for use of DNA, iris, and fingerprint systems, as detailed in Section V of the report.

7.2 Facial Recognition Technologies (FRT)

Cognizant that stakeholders' primary interest may be limited to specific domains, the best practices and their associated guidelines have been categorized as policy, operational, and technical.

7.2.1 Policy

Best Practice: FSLTT LEAs should prohibit the use of FRT probe photos or other biometric data captured in violation of existing laws and policies, as well as AI models known by the agency to be trained on photos or biometric data captured in violation of existing laws, Federal government guidance, or agency policy.

Guideline: LEAs should not use photos or biometric data they know or believe to have been captured in violation of the 1st, 4th, 14th Amendment; other constitutional protections; applicable federal, state, or local laws; or existing government-wide or agency guidance. This includes the capture and submission of photos based solely on individuals exercising their First Amendment right to lawful assembly.

Biometric data should not be captured, disseminated, or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations). Capture, use, dissemination, or retention of biometric data should not be based solely on individual demographic characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, gender, disability) or ability.[105]

To implement this best practice, LEAs should document and assess the provenance of the data used to train or fine-tune AI models when developing or procuring AI-enabled biometric systems, requiring any vendors to provide such information if possible. Agencies should prohibit the use of AI models that are known by the agency to be trained on photos or biometric data that was captured in violation of existing laws or guidance.

Best Practice: FSLTT LEAs should specifically articulate the authority that permits the capture of FRT biometric data or associated PII, which should be reflected in public documentation whenever possible.

Guideline: LEAs should specifically articulate the authority that permits the capture of biometric data or associated PII. The purpose(s) for which PII is captured should be specified at the time of initial data capture or upon subsequent changes to information capture authorities, business processes, or other factors affecting the capture and handling of the PII, in addition to where a system change creates new privacy risks. Subsequent use of this data should be limited to the purpose for which the PII was captured and follow standard data minimization practices. This information, along with any changes to programs' primary purposes, should be reflected in public documentation, whenever possible. Agencies should also establish a routine program review process to assess whether the program's purpose is being met and whether modifications are required.

PII, according to OMB Circular A-130, means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Biometric characteristics (such as fingerprints, iris, facial scans, and DNA) are always PII because they may be used to distinguish an individual's identity by means of unique physical characteristics. In fact, biometric characteristics are particularly sensitive forms of PII because they are immutable, thus increasing the risk of harm if control of the data is lost.

Best Practice: FSLTT LEAs should have strict criteria to govern the acceptable use of FRT systems in investigations—considering factors such as the nature of the investigation, the likelihood of generating a true match, and the testing and evaluation performance of the particular FRT system and relevant data—and should document these in public policies and procedures whenever possible.

Guideline: LEAs should have strict, well-documented criteria for the use of FRT systems in investigations, which should be documented in public policies and procedures whenever possible. These criteria may consider:

- The nature of the investigation or criminal act being investigated (e.g., identifying missing person/victim versus possible suspect in a criminal investigation);
- The likelihood, based on information gathered during the investigation, that the use of FRT or other FRT biometric system will generate a valid hit;
- The testing and evaluation performance of the FRT biometric system;

- The image or input sample quality, and whether inputs should not be submitted to an FRT system or FRT biometric system because of low confidence in any ensuing comparison;
- The type of further investigative steps that will be taken to confirm any candidates found by the FRT biometric system.

Agencies should consider developing these criteria with stakeholder inputs and public engagement.

Best Practice: FSLTT LEAs should have policies and procedures in place to address the improper use of an FRT biometric system. Agencies should have consequences for improper uses of a biometric system, such as terminating system access in cases of intentional misuse.

Guideline: LEAs should have internal oversight procedures in place—such as audits, assessments, and system logs of system use and impacts—to ensure that biometric-related queries are being conducted consistent with policy and avoid discriminatory or biased outcomes. Agencies should also implement a process for personnel to report suspected cases of misuse or abuse, including negligent use. Agencies should also have policies and procedures to address LE failures to adhere to procedures or failure to attain appropriate certification or training.

LE should consider terminating any employee or contractor's access to a biometric system after intentional misuse or improper dissemination of system records. In the case of accidental or negligent misuse, the operator should undergo additional training to ensure adherence to agency policies and practices.

Best Practice: When employing FRT systems that use AI, SLTT LEAs are strongly encouraged to follow applicable Federal guidance and prevailing scientific standards for appropriate, equitable, and fair use of FRT.

Guideline: Federal agencies that use AI-enabled FRT systems that impact rights or safety or systems that are presumed to be rights and safety impacting are required to follow relevant Federal guidance, such as OMB M-24-10. In accordance with guidance from M-24-10, by December 1, 2024, Federal agencies are required to implement concrete safeguards when using AI in a way that could impact Americans' rights or safety. Some agency uses of AI are presumed to be rights-impacting, including law enforcement "conducting biometric identification (e.g., iris, facial, fingerprint, or gait comparisons); sketching faces; reconstructing faces based on genetic information."

Under the Federal guidance, rights-impacting AI is required to meet certain requirements, including:

- Conducting an impact assessment documenting the purpose and benefits of the AI, the potential risks, the stakeholders who would be most impacted, and the quality and appropriateness of the relevant data.
- Testing the system in a real-world context.
- Conducting ongoing monitoring to ensure the system's functionality and any changes in impact on rights and safety. Agencies are also required to conduct ongoing monitoring to specifically assess and mitigate AI-enabled discrimination.

- Testing the system against a representative range of human facial variability.
- Conducting up-front and ongoing monitoring for algorithmic discrimination.
- Providing low-burden, timely, ongoing opportunities for input from affected communities, and incorporate feedback from accordingly affected communities.
- Notifying negatively affected individuals and maintaining human consideration and remedy processes.

SLTT law enforcement agencies are strongly encouraged to follow applicable Federal government-wide guidance when they use FRT systems that use AI.

Best Practice: FSLTT LEAs should have policies in place to prohibit the use of commercially available FRT systems that have not been approved by the agency for use.

Guideline: LEAs should provide clear guidance that FRT systems not approved by their agencies are expressly disallowed for use during the course of duty. Agency processes for system approval may vary, but there should be procedures and consequences to address the use of unapproved systems, such as software as a service commercially available for purchase by the public. Agencies should have criteria for approving the use of a specific FRT biometric system, including results from independent testing and evaluation, the source of relevant training or gallery data, accuracy performance measures across demographic groups, and other key factors. Agencies should follow ISO/IEC 19795 for FRT performance testing and reporting.

Best Practice: FSLTT LEAs should specify—and disclose in public documentation whenever possible—any independent assessments and benchmarks of FRT biometric systems, which should be measured using standardized methodologies in as close to an operational context as possible.

Guideline: LEAs should set benchmarks for acceptable performance that must be achieved under real-world conditions for FRT systems to be used and should ensure that these values are publicly available whenever possible. These benchmarks may vary depending on the use case and purpose of investigation (e.g., identifying a victim of human trafficking may tolerate a different threshold compared to identifying a possible suspect in a criminal case). Agencies must articulate a clear reason for not publishing independent assessments and benchmarks and specify the reason in public documentation.

Whenever possible, agencies should test FRT systems both before deployment and regularly after deployment to ensure that these benchmarks are maintained as the system is used. Federal entities, such as the DHS's MdTF and others, should support testing and evaluation of biometric technologies used by SLTT. Agencies are strongly encouraged to not use FRT systems unless they have been evaluated by NIST as part of the FRTE or can provide test data comparable to that available through NIST testing.

Best Practice: FSLTT LEAs should disclose information about their use of FRT systems in publicly available documentation, including the type of FRT system and general purpose of use, whenever possible.

Guideline: Whenever possible, LEAs should provide public notifications prior to use of a FRT system, including the type of FRT system and its purpose. These general notices align with similar reporting requirements and disclosures for government use of (AI) through the Federal AI Use Case Inventories.[106] Certain FRT systems may be excluded from required notifications, specifically those used as a component of a national security system or within the intelligence community.

With the potential for facial images to be easily captured without consent or without a custodial interaction (as opposed to giving a fingerprint to receive a benefit, or have DNA captured due to an arrest), LEAs have a responsibility to actively promote a common understanding of FRT technology and agencies' use and non-use of it. Agencies should establish and make publicly available policies and procedures that ensure respect for privacy, civil rights, and civil liberties. Many Departments and agencies have created systems for investigating possible violations. For example, the DHS CRCL has an established complaint process to investigate allegations of violations of civil rights and civil liberties related to the Department's use of biometrics and provide recommendations for the development and implementation of applicable additional safeguards.

7.2.2 Operational

Best Practice: In LE investigations, FSLTT LEAs should use FRT identification candidate results only as an investigative lead and not as the sole basis for identification or probable cause.

Guideline: FRT should be only part of a multi-factor basis for an arrest or investigation, and FRT should not be the sole basis for probable cause, consistent with some state laws and policies.[107] Law enforcement must also carefully review the results and consider the adequacy of probe inputs, particularly those with lower quality. LE should carefully consider the system's minimum similarity threshold (if one is used) before using candidates for investigative leads. These thresholds should be based on standards set by independent testing authorities, such as NIST's threshold for the FRTE.

Best Practice: Where multiple FRT candidate results are returned, FSLTT LEAs should manually review top candidate results from a candidate list before focusing on one candidate result for further investigation.

Guideline: LEAs should require that all top candidate results from a candidate list should be manually reviewed and adjudicated before identifying one of those candidates, if any, as an investigative lead. If a search only produces one candidate result above a minimum similarity threshold, the system should display a message to the operator to ensure the candidate result is not interpretated as a true match without further investigation. Agencies should consider using multiple, independent human reviewers to adjudicate results whenever possible.

In line with this best practice, agencies should require technology vendors to configure FRT systems to provide a list of candidate results rather than a single candidate result whenever there are multiple candidates above a minimum similarity threshold.

Best Practice: FSLTT LEAs should retain detailed internal logs of FRT system use for auditing and compliance with existing requirements.

Guideline: LEAs should retain detailed information about the use of FRT systems to support oversight and auditing. This should generally include information on both inputs and outputs and should include search timestamps; search inputs; search query parameters; user information; probe quality information; user location information; and other information as appropriate. This information should be preserved for a reasonable length of time, as specified in retention schedules, in case of challenges. This information should also include investigatory information, such as a short description of the kind of investigation. Information captured and retained for auditing and compliance cannot be used for other purposes to prevent the misuse of PII. Such information should be secured according to existing cybersecurity requirements and other best practices to ensure the security of data.

Best Practice: FSLTT LEAs should require technical and policy training for agency personnel who will use FRT systems. For FRT systems, that should include training on interpreting similarity scores displayed by a system and the adjudication of results.

Guideline: LEA users who are authorized or have access to FRT systems should be trained on an agency's biometric policies and technical operations prior to use. Users should be retrained at regular intervals and whenever the biometric system is significantly updated, to ensure the proper training of all operators. Additionally, agencies should limit system access to individuals who have received training.

There are various existing resources that law enforcement may incorporate into training. For example, the FISWG has numerous resources that provide guidance on training the trainer, training the examiner, setting out a code of ethics, preserving image quality, comparing face images for investigative leads, and more.[108]

Best Practice: FSLTT LEAs should retain system performance documentation and testing results about the FRT systems sufficient to allow for independent evaluation and/or auditing and should require technology vendors to provide the testing and evaluation results for the system version that is procured by agencies, not results for a previous or adjusted versions of the system.

Guideline: LEAs should retain documentation of the system design, training data, implementation, testing regime, and the results of third-party evaluations for FRT systems. Documentation should meet industry and third-party standards for auditing. If using a vendor, the agency should ensure that the vendor provides this information to the LEA.

7.2.3 Technical

Best Practice: FSLTT LEAs should have minimum quality criteria for input biometric data used for FRT systems, which should align with existing standards set by independent testing and standard-setting bodies.

Guideline: LEAs should set minimum quality criteria for FRT probe data and reference gallery images. These quality criteria should be based on independent standards. Whenever possible, LEAs should publish these minimum quality criteria to ensure transparency and responsible use. These minimum quality criteria may depend on the use. For example, the minimum acceptable criteria for generating leads on the identity of a victim of child trafficking may differ from the minimum threshold for inputs in generating investigatory leads on a suspect or perpetrator for a criminal case. Agency criteria should take into account such factors as the type of investigation (including the severity of the crime and whether other investigative leads are available) and the resources available to the agency undertaking the investigation.

Best Practice: FSLTT LEAs should minimize the risks of automation and confirmation bias for users through the configuration of systems and policies and procedures governing use, such as by carefully considering the benefits and risks of FRT systems that present similarity scores on candidate results for identification searches.

Guideline: LEAs should configure FRT systems to minimize automation or confirmation bias, such as by aligning with the recommended configurations from independent certified organizations and standard-setting bodies to ensure responsible use by agencies and protections for the public's rights and safety. Agencies should consider how FRT systems can minimize automation bias, such as by providing an unranked list of candidates for human review or displaying information about the similarity scores for candidate results. Agencies should consider the benefits and risks to displaying such information directly to the operator or whether it should be available, but not shown by default. Agencies should require technology vendors to design systems to minimize risks of automation bias and ensure the availability of information on technical specifications, including similarity scores.

For example, FRT systems could provide a list of candidate results (rather than a single identification or candidate result). This could include a ranked listing of candidate photos with similarity scores including caveats and caution that further investigation is required to determine the subject's identity and to avoid concluding that the top ranked candidate result is necessarily the "best." Agency training should discuss how operators can interpret any disclosed similarity scores and should have policies in place regarding how to use candidate results of different similarity scores in investigations.

As the research on mitigating automation bias and standards on configuration continue to develop, FSLTT agencies should follow and adapt to these independent standards, policies, and criteria where consistent with applicable laws.

Best Practice: FSLTT LEAs should ensure FRT systems have a minimum similarity threshold for candidate results, which may vary depending on a variety of criteria and should only be overridden in exigent circumstances.

Guideline: LEAs should use FRT systems that present candidate results who meet a minimum similarity threshold (and return zero results if no candidates meet the threshold). The minimum similarity threshold should be overridden only in exigent circumstances, such as when human life is at risk. Whenever possible, agencies should validate selected thresholds based on independent testing of the FRT algorithm using use-case relevant image datasets to confirm selected thresholds provide expected error rates. The minimum similarity threshold may vary depending on the use case, such as generating leads on the identity of a victim of child sexual abuse as compared to generating possible leads on a suspect or perpetrator for a criminal investigation.

Best Practice: FSLTT LEAs should implement existing accredited and ISO-recognized standards for FRT biometric systems and data.

Guideline: LEAs should ensure the implementation of both ANSI/NIST common formats and NIEMOpen robust data models and highly refined sets of technical specifications to assure data is exchanged correctly and efficiently with their partners. LEAs should also require that any procured systems from vendors or other entities meet these standards. These standards will help ensure data interoperability and analysis.

Best Practice: Federal agencies should have testing and evaluation requirements for SLTT grantees for grants that fund the procurement or development of FRT systems and should require that SLTT grantees follow applicable OMB M-24-10 requirements, as appropriate.

Guideline: Federal agencies that provide grants and other financial support for SLTT adoption of FRT systems should require grant and funding recipients to undergo quality control testing, or use systems that have undergone quality control testing, and require entities to provide verified results on accuracy and performance across demographics. If such requirements are not possible, Federal agencies should strongly recommend testing and evaluation criteria on SLTT grantees.

Federal grants and other financial support for SLTT adoption of FRT should also require grant and funding recipients to follow applicable practices set out in the OMB M-24-10 that would be required if any acquired systems were used by Federal agencies. These include applicable requirements for rights-impacting AI, such as notice, disclosure, maintaining records, system accuracy thresholds, training operators, and system performance requirements.

This may be reflected in current agency practices and policies. For example, DOJ currently requires the recipients of JAG funds for FRT adoption to have "policies and procedures in place to ensure that the FRT will be used in an appropriate and responsible manner that promotes public safety; and protects privacy, civil rights, and civil liberties; and complies with all applicable provisions of the U.S. Constitution, including the fourth amendment's protection against unreasonable searches and seizures, the first amendment's freedom of association and speech, and other laws and regulations. Recipients utilizing funds for FRT must make such policies and procedures available to DOJ upon request."[109]

SECTION V: TECHNICAL DISCUSSION

8. Biometric Technology Accuracy, Standards, and Use Cases

Biometric standards define the minimum baseline relationships between and within biometric devices and systems to assure performance, accuracy, and interoperability. They are essential to assuring the quality and reliability of identity products, improving processes, and ensuring consistency and greater transparency. Without standards, biometric activities are significantly less trustworthy, reliable, or useful. *The International Organization for Standardization (ISO) creates different types of standards that apply to biometrics identity systems such as DHS OBIM IDENT, and algorithms of all modalities discussed in this report – fingerprint, face, iris, and DNA. Their guidance should be strongly considered.*

Standard bodies consist of scientists and researchers, system operators, and in many instances, official country or institutional designees. International Committee for Information Technology (INCITS) M1 is the U.S. standards body for biometrics. Internationally, Subcommittee 37 (SC37) of the ISO is focused solely on biometrics and brings together 170 national standards organizations from across the globe, with 110 international biometric standards published to date, which include requirements, and 20 other technical reports produced by six working groups.[110] ISO/IEC JTC 1/SC 37 is the "Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems." *Most of the ISO publications by its six working groups focus on either common file frameworks or biometric programming interfaces, and these publications should be strongly considered to as they pertain to law enforcement biometric activities.*[111] Of note, five overarching guidance documents are available from ISO that are of particular importance:

(1) The ISO/IEC 39794[112] data interchange standard establishes requirements on biometric data capture, data encoding, and data interoperability. The standards have 18 parts, each dedicated to a specific modality, such as face, fingerprints, or DNA. One adopter of the standards is the International Civil Aviation Organization (ICAO), which uses the standards to regulate data appearing on all electronic passports.

(2) The ISO/IEC 29794[113] sample quality standards define tests that should be applied to captured biometric samples, specifically finger, face, iris, and overall frameworks for sample quality criteria. The standards aim to support detection of poor samples likely to causes errors, and to provide a quantitative survey capability to summarize quality across an enterprise.

(3) The ISO/IEC 19795[114] and ISO/IEC 30107[115] standards govern the conduct of biometric tests. There are ten documents in the 19795 series focused on topics such as test design, statistical bounds, scenario tests, operational tests, template protection, interoperability, and demographics. The 30107 series guides tests of components or systems that detect subversive presentations to cameras, including those on mobile devices.

(4) The ISO/IEC SC 37 Biometric Vocabulary "establishes a systematic description of the concepts in the field of biometrics pertaining to recognition of human beings. This document also reconciles variant terms in use in pre-existing International Standards on biometrics against the preferred terms, thereby clarifying the use of terms in this field."[116] *Considering the variability in definitions used by law enforcement communities to describe their biometric activities, all biometric system operators and their ecosystem should adhere to the ISO biometric vocabulary*.

(5) The ISO "Cross-jurisdictional and societal aspects of biometrics- General guidance"[117] has been updated to include privacy by design principles, addressing end-to-end "biometric technologies designed to capture, process and record biometric information" with regard to legal and societal constraints, privacy and data protection of identified individuals, accessibility[118] for the widest population possible, and health and safety related to biometric capture. *Because biometric systems directly affect individuals and their personally identifiable information, ISO's guidance on societal aspects of biometrics should be considered and consulted not simply from a societal perspective, but also from the vantage point of making these systems work well with and for humans.*

The International Association for Identification (IAI) is a professional forensic association that educates and provides certifications for professionals in the field of biometrics.[119] Working closely with IAI is NIST, who operates the Organization of Scientific Area Committees for Forensic Science (OSAC) by promulgating forensic standards and guidelines.[120] Closely aligned with OSAC is the FISWG, who works with 59 different LEAs across 14 countries, and private industry, to encourage "proper application of face identification and face recognition technologies," as well as develop guidelines and best practices for both face and iris technologies.[121] All FISWG activities are approved and published through OSAC, with 34 documents currently published. Also, in alignment with NIST is the ANSI, while not a standards-making institute, "provides a framework for fair standards development… and standards-based solutions." NIST, through ANSI, did, in one instance, provide the data format interchange of fingerprint, facial and other biometric information standard. ANSI/NIST-ITL today, along with NIEMOpen communication protocols, stipulates critical interoperability standards used by DHS and DOJ today.

While standards are in constant promulgation and review, for the purposes of this report, the focus is on standards of import relating to face recognition technologies. This section begins with discussion of image quality, as image quality, along with other factors, is often a significant differentiator in how well a face algorithm works, to return a candidate list. In investigative or LE settings, once a candidate list is returned, human examination takes place to determine what candidate on the list may result in a positive match to the original probe image submitted to the system. This is where human examination becomes critical, and the training and certification around human examination, as it is this adjudication that can help guide an investigation to a particular individual. Then the testing of the system itself is of importance, for combination of factors including accuracy, demographic differential harmonization, and end-to-end system operability. The last element to discuss is the sharing of data once adjudicated, and the system's interoperability with others to share that data.

Image Quality. Image quality is an essential element to assuring algorithmic accuracy while providing a minimum baseline to assess face quality in a vendor agnostic manner. Thus, setting standards for face image quality is essential to improving overall biometric system performance. While as of publication of this report ISO SC37 does not have a published face image quality standard, resolution of a standard is underway with a publication date expected in March 2025. The new standard, "ISO Information Technology—Biometric sample quality—Part 5: Face"[122] "will characterize face image quality into static and dynamic properties that affect image quality, delineating methods for quantifying the quality of the face images."[123] ISO SC37 states the reasoning for a face image standard as follows: "Even though face recognition error rates dropped massively with the introduction of algorithms based on deep learning, they…depend on the imaging process, human factors design, level of biometric capture subject cooperation, the particular comparison algorithm, and associated threshold and decision logic."[124]

ISO lists a series of "drivers for improved capture" as follows: improved useability of images, increasing size of systems and volumes of images, increasing number of face programs, use of cameras for face recognition that are not designed to capture face (unlike fingerprint and iris devices), and increasing use of face images not captured using image design specifications that are used for IDs but rather captured in the "wild."[125] *Recognizing the importance of image quality to algorithmic performance is a foundational element to any biometric system, and upon publication, ISO's Face Image standard should be strongly considered by biometric operators.*

Human Examination Training and Certification. When a candidate list of face images is returned in a one-to-many search against a probe image, a human examiner must conduct a variety of analyses to proficiently determine if the probe image may result in a match to any of the ranked returns in the candidate list. While procedure and processing in handling of candidate lists is critical, critical to those affected by face recognition determinations is the accuracy of that examination conducted by a trained face examiner. To date, essential learning and training occurs through the FBI and the private sector. *FISWG has numerous guides that train the trainer, train the examiner, set out code of ethics, preserve image quality, compare face images for investigative leads, and more. These should be actively used by law enforcement, as applicable, to assure all examiners are well trained to make the best adjudications possible.*

Assuring that training has occurred to the appropriate level requires accreditation. The IAI is in the process of both defining the roles of **Certified Facial Examiner (CFE)** and the **Certified Facial Reviewer (CFR)** and finalizing certifications for both roles. The CFR adjudicates initial candidate lists, while the CFE adjudicates the facial comparison. *Within these processes, there should be a rigorous process of memorializing actions related to the examination, and controls on who handles what data when.*

8.1 FRT Standards

Law Enforcement Use of One-to-Many Search to generate investigative leads. In contrast, one-to-many search FRT is used by law enforcement regularly to help develop investigative leads. In a one-to-many search, a photo depicting the subject being sought is used as the "probe." The template generated from this probe photo is then compared against the templates of all subjects contained in the gallery. A set of gallery photos whose templates have the highest similarity scores are presented to the user as a candidate list for adjudication. Depending on the system and user preferences, this candidate list may include dozens of gallery subjects, or as few as two. During the adjudication process, a trained user[126] must determine if any of the candidates returned by the system represents a potential match to the subject in the probe image. If such a potential match is identified, it is considered an investigative lead only and it must be substantiated or invalidated through established investigative methods before any action is taken against the individual.

While humans recognize people using a variety of characteristics beyond facial features (such as skin tone, hair color and style, and overall body appearance) FRT only uses actual facial features to differentiate amongst face images to differentiate amongst face images. While commercial algorithms used by law enforcement differ, generally recognized features include the eyes, nose, mouth, and eyebrows, as well as the facial outline and skin texture. The appearance of these features can change with facial expression, aging, and health, as well as the pose of the face relative to the camera (e.g., profile view versus front view). Obstructions such as hair and eyeglasses may further alter the appearance of these features (or obscure them), as can changes in lighting, both in terms of intensity and direction, which may result in shadows or highlights. Overexposure (too much light) can reduce the visibility of features on the faces of people with pale skin, whereas underexposure (too little light) can reduce the visibility of features on the faces of people with darker skin.

This last point bears further explanation, given concerns about potential differences in FRT algorithm performance across different demographic groups. FRT algorithms do not rely upon skin tone to differentiate one person from another. Rather, when skin tone and lighting together reduce the visibility of features on the face, the algorithm has less information to process, making it harder to differentiate one person from another. This is reflected in some algorithms performing differently for people with darker skin than for those with lighter skin.[127]

Beyond lighting, the visibility of facial features in images is also affected by other aspects of the photographic process and differences in the cameras which capture those images. Spatial resolution (i.e., number of pixels across the face), sensitivity of the camera sensors to changes in tonality, lens quality, and blur due to factors such as camera or subject motion or poor focus all influence the appearance of a face in an image, as does post-capture processing such as the amount and type of compression used. FRT uses an algorithm to represent an image of the face as a set of biometric features called a template. The template can be characterized as a point within the multidimensional space. When comparing a probe to a gallery image, the FRT algorithm computes the distance between the probe's coordinate and the coordinate of the gallery image. The similarity score reflects the proximity of these two templates. The FRT algorithm is developed through a process of machine

learning in a way that projects the templates in 3D to maximize the match scores in a set of training images.

An algorithm's representation of a human face is constructed using pixels of an image and not the human face itself. Due to a high degree of variance in the presentation of a person's face, whether from different facial expressions; angles and poses; illumination in varying degrees of light and shadow; camera focus, quality, angle, blur and other capture conditions; makeup, sunglasses, eyeglasses, mustaches, beards, hairstyles, hats and other occluding factors; or wrinkles, weight loss/gain, hair loss and other natural aging progressions, an algorithm's representation of a face will vary to a larger degree than biometric identifiers that are based on more stable genetic characteristics like a person's voice, fingerprint, iris or DNA. For example, while fingerprints are usually captured on a dedicated touchpad, capture conditions for face images will vary, akin to the differences among photos of a person in a family photo album. Furthermore, the algorithm's process of generating a representation is not a perfectly invertible function, such that a person's identity may be easily derived from the representation. Rather, a representation is useful only in conjunction with the particular version of the algorithm that created it and other candidate representations for comparison.

In any comparison of two facial images the algorithm computes a similarity score for those images. If an FRT system functions in a manner that requires a decision regarding identity must be made based on that similarity score alone – as is the case in the 1:1 *Verification* scenario – then there will be four possible outcomes:

- the FRT system correctly defines it as a match and it is ("true accept" or "true positive");
- the FRT system correctly defines it is a non-match and it is a non-match ("true reject" or "true negative");
- the FRT system defines it as a match when it actually is a non-match ("false accept" or "false positive"); and
- the FRT system defines it as a non-match when it really is ("false reject" or "false negative").

To make a match vs. non-match determination following comparison, a system operator or user selects a match threshold, and if the algorithm's similarity score of a comparison of two templates exceeds the threshold, the software deems it a match, while a similarity score below the threshold results in a non-match determination. A face recognition algorithm can minimize the false match rate by setting a very demanding, high threshold that would require near-identical images of a person but that would produce a high false non-match rate as the person could present in a different manner (with/without makeup, good/bad lighting, off-pose, etc.). Alternatively, the algorithm can minimize the false non-match rate by setting a lower threshold that would deem a match for any candidate who looks somewhat similar. Biometric performance is measured as a tradeoff between the false non-match rate and the false match rate, where the goal is to minimize both by selecting a threshold that ideally accurately separates all the true matches above the threshold from all the true non-matches below the threshold.

Accuracy and Algorithmic Development. The facial features, expression, obstructions, exposure, and image quality discussed above can influence the match score generated by an FRT algorithm when two image templates are compared. The best performing algorithms are robust to the impact of these variations on template generation (and match score). Algorithms developed using training images consisting of lots of pictures of the same individuals end up being very good at minimizing the superficial variations in face images. Similarly, algorithms trained on many individuals within a demographic group are better at identifying others within that group.

A key challenge for developers of FRT algorithms, however, is how to make sure that the algorithm does not return a high match score when comparing images of two people who look comparatively similar, as might happen especially with individuals who are related to one another, such as siblings. To increase the variance in templates (i.e., the differences between two templates) and thus reduce the chance of misidentifying any one person, developers must train their algorithms using a large, diverse set of pictures of different people. In this way, algorithms can be refined to be sensitive to minor differences in the features of people who look similar, such as people within the same demographic group.

FRT algorithm developers must endeavor to encompass the variety of facial appearances across a wide range of demographic groups in their training data. Comprehensive training images will incorporate variety and balance across sex, race, and age demographic populations. In the absence of less fulsome training data, a FRT algorithm may not be able to adequately detect fine facial variations that occur between individuals in each demographic population and may be less likely to correctly differentiate two people from one another.

Operators of FRT systems need to mitigate the impact of any such deficiencies, and it is for this reason that *a federal government law enforcement best practice is to require that a trained individual conduct a manual review of any candidate list generated by a one-to-many FRT search before identifying one of those candidates (if any) as an investigative lead.*

Accuracy Testing Results. 1:1 FRT systems base the decision of whether two facial images represent the same individual using a threshold score. If the match score exceeds the threshold score, then the decision may be made to declare the two images are a "match." If the match score is below the threshold, then a decision may be made to declare the two images a "non-match."

Because each algorithm may compute similarity scores differently, they will have different thresholds. For the NIST FRTE for 1:1 algorithms,[128] NIST selects a threshold score that corresponds to a uniform false match rate across all algorithms that fixes a certain false match rate and reports the corresponding false non-match rate associated with that threshold. In the initial 1993 tests, the false match rate was fixed at 10^{-3} (equivalent to 1 in 1,000) and the corresponding false non-match rate hovered around 80%.[129] Since then, the technology has improved and NIST now reports false match rates at 10^{-6} (equal to 1 in 1,000,000) with corresponding false non-match rates around 10-3 (equal to 0.1%). In 30 years, the false match rate has improved by a factor of 1,000x while the false non-match rate has simultaneously improved by a factor of 800x.[130]

In contrast to the 1:1 scenario, a one-to-many search system compares a probe against all of the subjects enrolled in a gallery and generates a match score for each comparison. NIST testing of algorithms differentiates one-to-many search system operations into either "Investigation Mode" or "Identification Mode." Identification mode is often used in scenarios wherein a user purports to be included in the gallery of enrolled subjects in order to gain a benefit from being recognized, such as in the case of ticketed passengers boarding an airplane. As long as comparison of the user's face results in a match to one of the faces in the gallery at a score above a given threshold, they are considered "identified" and the benefit is granted.

Investigation mode refers to the typical LE scenario in which officials seek to develop a "lead" by identifying an unknown subject by comparing their image against all enrolled subjects in the gallery. A candidate list of enrolled subjects is returned to the operator in order of match score, regardless of whether the match score exceeds a given threshold. The operator must then adjudicate the candidate list to determine if a potential match is present. There is no fixed length for a candidate list, but the FBI Next Generation Identification Photo System (NGI-IPS) default length is 20 candidates.

A "Rank 1 match" occurs if the identity of the probe image corresponds to the top scoring candidate. Similarly, a Rank 10 match occurs if the identity of the probe image corresponds to any of the top 10 scoring candidates.

According to the latest one-to-many search report from NIST,[131] leading algorithms – including those used by DHS and DOJ - in one-to-many search applications have Rank 1 match rates of 99.9% when running mugshot probe images against mugshot galleries. This means that the Rank 1 candidate list would include a "false match" at Rank 1 0.1% of the time, when using a mugshot as a probe image. Lower quality images, such as those captured by immigration kiosks or ATM-style cameras, lead to reduced accuracy with the best performing algorithms achieving Rank 1 match rates just above 95%.

It bears repeating, however, that in the best practice LE application of one-to-many searches "leads" are set, rather than "identifications," so the term "match" is not wholly appropriate. "Leads" must be confirmed or refuted through further investigative steps, such as witness statements, to corroborate a biometric match.

8.1.1 Facial Recognition Testing

The underpinning to any biometric accuracy is its test and evaluation, and many organizations around the world perform biometric testing, including testing on open-source data sets, in operational scenarios, and on face image quality. In the USG, the premiere algorithmic test facility is also the premiere test facility in the world for biometric test and evaluation in numerous testing scenarios - NIST. At DHS, operational testing scenarios as well as algorithmic development for the purpose of improving algorithmic performance against issues pertaining to demographic differentials, for example, are evaluated at the MdTF.

NIST conducts FRTE and Face Analysis Technology Evaluation (FATE) to examine developer submitted algorithms for accuracy and other performance characteristics. For the most part, NIST FRTE testing has focused on technology testing involving operationally captured face images, such as one-to-one comparisons in a border crossing scenario or searching a mugshot phone against a gallery of existing driver licenses to detect previous enrollments. Such testing occurs today in an ongoing manner allowing developers the ability to submit algorithms and receive benchmark test results in a matter of weeks, and updated results daily.[132]

While the current NIST FRT testing provides useful insight into algorithm performance, law enforcement has a need to understand how face algorithms withstand uncontrolled settings with variants such as light, angle, hardware and software interoperability, and the hats, glasses and other accessories that obstruct faces. Between 2014 and 2017, NIST conducted a study called "Face In Video Evaluation (FIVE)"[133] using algorithms available in the 2015 time frame. The report "…documents situations where face recognition of non-cooperative persons is accurate enough to satisfy some operational requirements. It also demonstrates cases where the core recognition technology fails to compensate for deficient imaging. That notwithstanding, subjects appearing in video can be identified with error rates approaching those measured in cooperative face recognition, but only if image quality reaches the level attained in engineered systems such as e-Passport gates."[134] NIST recently announced plans to conduct a new test in 2024 of FRT in video, *Face In Video Evaluation (FIVE) 2024*. This program will be added to the on-going FRTE and will provide additional insight for any agency which uses Closed-Circuit Television (CCTV) images as probes.[135]

Beyond NIST testing, other agencies support FRT testing. For example, the MdTF, funded by the DHS Science & Technology Directorate, also regularly conducts vendor testing in a variety of scenarios. As a result, DHS components regularly engage MdTF to pre-test false positives, false negatives, capture and image quality, and overall accuracy prior to pilot deployments in scenarios architected to mimic a specific operational use case.

The United Kingdom's National Physical Laboratory (NPL) has also conducted testing. In 2023, they published a study that addressed real-world use of FRT LE settings. The *Facial Recognition Technology in Law Enforcement Equitability Study, Final Report*[136] examined FRT use in several scenarios, including "Retrospective Facial Recognition" in which CCTV images of unknown subjects are compared against a gallery of approximately 116,000 individuals in order to identify them, as well as "Operator Initiated Facial Recognition" in which mobile phone images of the unknown subjects were compared against the gallery. Of note, the gallery and probe subjects were balanced across both gender (Female/Male) and "self-identified ethnicity" (Asian, Black, and White) based on United Kingdom standard codes. As described further below, in both scenarios, the NPL found that operators performed without error, with a true match rate of 100% and no false matches at the highest test thresholds using images captured on the same day. False positives were observed at a rate of 1:6,000 for a watchlist size of 10,000 at the default threshold setting. The study also notes that equitability of false positives will depend on the threshold setting of the operational system, with the higher likelihood of false positive identifications for "black" subjects at lower thresholds.

Finally, there is active academic research testing FRT performance under a few conditions which helps inform best practices in the use of FRT by law enforcement. One notable paper discussed below *Demographic Disparities in 1-to-Many Facial Identification*"[137] by Bhatta and colleagues describes research which simulated the use of low-quality CCTV images as probes in a one-to-many search scenario like those used in the LE context.

8.1.2 The Issue of Demographic Differentials

According to NIST, *demographic differentials* are exhibited when a FRT algorithm's ability to "match two images of the same person… from one demographic group to another" differs.[138] An algorithm is an inexact representation of the data used to develop it. When an algorithm performs comparisons in real time, it also must deal with differentials in image quality of the probe image, as discussed previously. While both bias and disparate treatment are important potential or actual societal costs of the human action taken on the algorithmic output, the focus in this section is on the *science* of how algorithms are tested for demographic differentials, the research and development to help understand and solve the problem. Finally, the report takes a special look at the work being done at DHS's MdTF on both fronts, including, testing, research, and evaluation.

8.1.2.1 Demographic Differential Testing

A December 2019 NIST Report[139] examined accuracy issues related to differences in the performance of face recognition algorithms based on demographics. This report noted that face recognition algorithms may have significant performance variations based on differences in gender, age, and race or country of birth. In general, this study found that algorithms performed worse on people of color, females, and children and the elderly, with these groups showing higher false match rates. A frequently overlooked finding of this study was that some developers (including a DOJ and DHS algorithm supplier) provided highly accurate identification algorithms for which false positive differentials were undetectable across all examined demographic groups. This finding highlights the necessity to select algorithms with care and take steps to mitigate performance shortcomings.

As demonstrated by testing performed by NIST, MdTF, and others, in the last five years, algorithm developers have achieved great success in addressing differences in performance associated with demographics. Extremely low error rates now exist across demographics, which include gender, age, and race. As currently reported (February 2024) in the NIST FRTE,[140] one leading algorithm (from the same DOJ supplier noted above) has an overall true match rate of 99.83%. The demographic group for which this algorithm has the highest true match rate is those born in East Asia with an accuracy of 99.85%, which the group with the lowest true match rate is those born in West Africa with an accuracy of 99.79%. In other words, there is only a 0.06% difference between the best and worst true match performance.

The values reported immediately above reflect performance on high quality images comparable to visa photos. As noted above, lower quality images will result in lower accuracy regardless of demographic, but two studies noted above demonstrate progress on this front. In particular, the NPL *Facial Recognition Technology in Law Enforcement Equitability Study, Final Report*[141] from 2023 reported perfect performance across all demographic groups (Asian, Black, and White) in both the "Retrospective Facial Recognition" use case with CCTV images and "Operator Initiated Facial Recognition" use case with mobile device images.

However, this NPL study also reported on one area for improvement in a "Live Facial Recognition" use case. While neither DOJ nor DHS uses live facial recognition, this study provides insight on how a "lights out" one-to-many search FRT system might perform. In this study, "watchlists" of 10,000 and 1,000 subjects were used as one-to-many search galleries for searching using probe images acquired using CCTV. The study used a commercial algorithm with its default match threshold. Across five different deployments, the system achieved an 89% true match rate for both watchlist sizes, false match rates were 0.017% (1 in 6,000) for the 10,000 subject gallery and 0.002% (1 in 60,000) for the 1,000-subject gallery.

The NPL report noted that while the best true match rate was achieved for the Asian-Female cohort and the poorest true match rate was for the Black-Female cohort, the observed differences were not determined to be statistically significant. In summary, this study found the system to be equitable across all demographics in both true match and false match metrics.

Finally, the research by Bhatta and colleagues noted above[142] examined the impact of lower quality images on Rank 1 returns across Black-White and Female-Male demographics using state-of-the-art algorithms and a gallery of mug shot quality images. This study considered loss of resolution due to both image blur and reduction in image size and examined the impact these modifications would have on false match rates, assuming a "lights out" scenario in which the Rank 1 candidate is declared as the match (a scenario which does not reflect the common practice in law enforcement but simplifies the statistical analysis).

In the absence of blur or reduction in size, the state-of-the-art algorithms generated the lowest false match rate for the Black Male demographic, followed, in order by the White Male, White Female, and Black Female demographics. In all cases, the "lights out" false match rate is below 0.1%. The state-of-the-art algorithms remain robust to blur and loss of resolution, up to the point where there is strong pixelization and loss of detail in the images. The "lights out" false match rate for the most highly blurred full-size images remains at approximately 0.1% for Black Males, while rising to approximately 1.3% for Black and White Females. Reduction in size has a more significant impact, with "lights out" false match rates approaching 10% when images have been reduced to only 28x28 pixels.

8.1.2.2 Operational Perspective on Demographic Differentials

The best way to avoid a misidentification is to correctly identify the person being sought. On this front, while demographic differentials issues will persist, the algorithms in use by DHS and DOJ today rank amongst the top of NIST testing, with true match rates more than 99.4% across all demographic groups examined by NIST (when using country of origin as a proxy for race). In fact, the rates exceed 99.6% for all but one country.

Nevertheless, both DOJ and DHS continue to promote research to address the issue. The work by Bhatta and colleagues noted above, *Demographic Disparities in 1-to-Many Facial Identification*,[143] was funded by the FBI, which looks to such research to identify where biometric systems and procedures may need to be modified to improve the overall performance. The results of that study, for example, suggest that when probe images are of lower quality, extra quality control will likely be necessary, perhaps in the form of a third technical review beyond the normal two-person review. Such quality control steps acknowledge the potential for variable performance of the technology to ensure they can be used in a reliable and responsible manner.

8.1.2.3 DHS Science and Technology (S&T) Maryland Test Facility

The MdTF is used to perform rigorous face, finger and iris capture and comparison testing of biometric and identity technologies in standards-compliant scenario tests that simulate DHS operational technology use-cases as defined by ISO/IEC 19795-21.[144] The MdTF opened in the summer of 2014 to support the DHS S&T and CBP's Apex Air Entry/Exit Re-engineering (AEER) project. The AEER project created a partnership between S&T and CBP to test and evaluate operational processes using biometric and non-biometric technologies. The MdTF continues to support multiple projects for the DHS S&T Biometrics and Identity Technology Center including those that inform both DHS and other external agencies to evaluate and implement solutions in their operational environments.

MdTF Rallies. The MdTF has held Biometric Technology Rallies since 2018 to test a variety of scenarios, such as high throughput multimodal systems (2019), face recognition systems with masks (2020 and 2021), and group processing (2022). Other systems tested at MdTF include Global Entry, Modified Egress, officer borne cameras, non-contact fingerprint systems, CBP's Traveler Verification Service (TVS), the agency's facial comparison technology which supports comprehensive biometric entry and exit procedures in the air, land, and sea environments,[145] TSA's Credential Authentication Technology (CAT) System, and mobile driver's license implementations. Recently, the MdTF has started testing remote identity systems as part of the 2023 Remote Identity Validation Technology Demonstration, which assesses document validation, selfie to document comparison, and presentation attack detection.

Findings. Generally, the face recognition systems evaluated as part of scenario and technology tests and the MdTF show strong performance. For example, in the 2021 Rally the median system correctly identified 95% of volunteers that were not wearing masks.[146] In 2022, the median system correctly identified 93% of individuals that interacted with a biometric system in groups of 2 and 4.[147] Consistently, most errors in an overall biometric system are driven by acquisition systems (i.e., cameras) failing to find and submit a quality face sample. Errors of the comparison systems in MdTF evaluations (i.e., failing to provide a positive match to a sufficiently

Maryland Test Facility:

One of a Kind

Currently the only biometric testing lab in the world that conducts evaluations that mimic operational environments of a use case.

Rallies test end-to-end performance of a biometric system, including the acquisition and comparison components, system operator, end user and subject feedback, allowing for discovery of issues at many stages in a biometric system workflow, such as a camera failing to acquire usable images of a subject. These performance aspects may be overlooked by traditional technology evaluations, which tend to focus on specific system components, such as the comparison algorithm, and also do not use live data, but pre-existing data.

Rallies also enable MdTF to acquire new data collections, including meta data about test subjects, such as their self-reported race or skin tone.

This enriched ground-truth data allows disaggregated performance measurement, such as is required to measure demographical differentials.

J. J. Howard, A.J. Blanchard, Y.B. Sirotin, J.A. Hasselgren, A.R. Vermury, (Oct. 2018) "An investigation of high-throughput biometric systems: Results of the 2018 DHS Biometric Technology Rally. Presented at 2018 IEEE 9th

Figure 15 - MdTF Snapshot

good quality image) have typically been only a fraction of camera errors (failing to submit a quality image).

Demographic Differential Findings. Since 2021, Rally results have been reported disaggregated across race, gender, and skin tone. In 2021, MdTF found lower median system performance for volunteers that self-identified as Black or African American relative to volunteers that identified as White. Researchers also found lower performance for volunteers that self-identified as females versus males, and for volunteers with darker skin versus lighter skin. However, results varied by system. The best system identified 99% of Males and 100% of Females, for example. It also identified both 100% of volunteers with dark skin and 100% of volunteers with light skin. Most of these demographic differentials are driven by acquisition systems failing to find and submit a quality face sample at equal rates across demographic groups.

In the tested scenarios, false rejections due to failures to acquire far exceeded false rejections due to failures to provide a true match response and were the main cause of differences in performance across demographic groups. DHS sponsored research has also shown, that when an image is acquired, there is a correlation between the strength of the match and skin tone, with light skinned individuals on average having a higher score. These effects existed on over 50% of tested algorithms in a 2023 study.[148] Many of these concepts from DHS research and demographic testing the Rallies were formalized in a new international standard (ISO/IEC 19795-10:2024) for evaluating equitability in biometric systems, that published in October 2024.[149]

Solving Demographic Differentials. Across four published research papers, the MdTF considers the causes of demographic differentials in face recognition to be nuanced and complex, with many researchers defining—and attempting to solve—demographic differentials differently.

Nonetheless, MdTF research has shown that face recognition systems, nearly universally, exhibit what is known as the *broad homogeneity* effect. This term was first coined by DHS S&T researchers in 2019. It means that face recognition algorithms tend to think different individuals that share demographic characteristics are more similar than those that do not.[150] For example, a white male will provide a match response to another white male at a higher rate than a white male will provide a match to an Asian Female. Individuals and organizations sometimes call this characteristic of face recognition systems "biased." However, that description misapplies the definition of "biased," which generally means to unfairly apply a set of criteria to one group and not another. Face recognition, in contradiction with the definition of "bias," does this for all groups. White males provide a match to other white males at a higher rate just as Asian Females provide a match to other Asian Females at a higher rate.

DHS S&T researchers in 2021 identified "demographic clustering" in the feature space of most face recognition algorithms as the root cause of this phenomena.[151] Demographic clustering means that two face recognition templates (mathematical models of the face) from different individuals that share demographic characteristics such as age, race, and gender, are likely closer to each other in template space than the templates from individuals that do not share demographic characteristics. What this means is that when an algorithm clusters together demographically similar individuals by skin tone

and gender, there is an increased likelihood of misidentification. For example, an African American male compared with a match result to a gallery of other African American males is more likely to be mis-identified as compared to a white male with a comparison result of a match to that gallery creating a false positive differential due to gallery composition. This type of clustering is peculiar to face recognition, as DHS S&T showed that iris recognition algorithms, tested on the same individuals, did not cluster people by race or gender.

In 2022, DHS S&T researchers proposed a method for mitigating this face recognition "clustering" effect, using linear dimensionality reduction techniques.[152] While theoretical, this approach to ignoring race and gender feature of the face, while still focusing on distinguishing features, could be applied during face recognition training and allow for more "fair" face recognition algorithms. It is unclear if face recognition vendors have identified this approach as a priority or applied it the training of their models. However, if applied, this technique could allow for more optimal human algorithm teams in face recognition tasks, decreasing the overall error rate of such activities.[153]

8.2 Fingerprint Technology Accuracy and Standards

Fingerprint comparison algorithms typically employ level two fingerprint details, such as minutia, to verify or identify a person's identity. Essentially, the process begins with modeling a fingerprint as shown below. The digital fingerprint image is automatically analyzed for minutia points (features) and mapped. The minutia map is transformed into a stream of data referred to as a template. The template is processed as a probe (when determining identity) or stored as a reference template (when enrolling an individual).

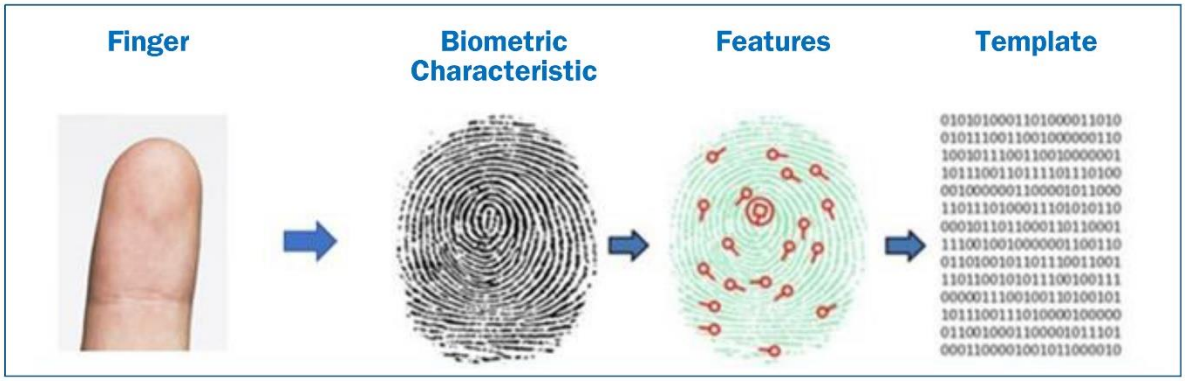

Figure 16 - Modeling Fingerprints

The probe is compared to one or more reference templates. The comparison activity is an act of comparing complex patterns. Each comparison activity yields a score representing the similarity of the probe to each reference template. The similarity score is evaluated against a previously determined threshold level. If the similarity score is above the threshold setting, the result is a positive match. If below the threshold setting, the result is a negative match.

As with face recognition, a positive match typically indicates that the person is who the biometric system says they are. A negative match typically indicates that the person is not who the biometric system says they are. In some instances, the ABIS using fingerprint algorithms are incorrect. In some cases, an error occurs in a statistical test when a true claim is (incorrectly) rejected. This is called a false reject. In other cases, an error occurs in a statistical test when a false claim is (incorrectly) not rejected. This is called a false accept.[154]

An automated biometric recognition system employing fingerprints as a modality can be evaluated for false reject and false accept rates through testing. The international standard ISO/IEC 19795 series can be used to confidently determine error rates. Another source to determine error rates for different fingerprint algorithms is the NIST Fingerprint Vendor Technology Evaluations. For the top performing fingerprint algorithms (that are properly tuned) they exhibit approximately 1% or less error rate.

8.2.1 Fingerprint Technology Standards

The fingerprint modality is included in all major biometrics standards, both domestic and international. The first fingerprint minutiae-based standard published by NIST was the ANSI/NBS-ICST 1-1986. While several revisions have been made since 1986, including a name change to the ANSI/NIST-ITL, the updates to the standard are designed to be backwards compatible, with new versions including additional information.

The ANSI/NIST-ITL defines fingerprint imagery as follows: Type 4 (Fingerprint Image Descriptive Information); Type-7 (Ten print Fingerprint Card Images); Type-9 (Fingerprint Minutiae Information), Type-13 (Latent Friction Ridge Images), Type-14 (Variable Resolution Fingerprint Images), and Type-15 (Palm Print Images). These type classifications were incorporated into the NIEM Biometric Data Model in 2012 as one of the initial three modalities (along with facial images and scars, marks, and tattoos).

NIEMOpen (previously the National Information Exchange Model (or NIEM)) provides an extensive data model and process for facilitating information exchange. The NIEMOpen Biometrics Sub-Committee provides a domain specific data model that aligns to the ITL Biometric Standard and harmonizes across stakeholder transmission protocols, i.e., DoD EBTS, DHS IXM and DOJ EBTS.

While the ANSI/NIST-ITL standard provides the guidelines for the exchange of biometric information between various federal, state, local, tribal, and international systems, the FBI EBTS defines requirement to which agencies must adhere when electronically communicating with the FBI. All versions of the EBTS are designed to be backwards compatible, with new versions including additional information. The latest version of the EBTS sets forth the requirements for submitting biometrics into the FBI's Next Generation Identification System.[155]

The ISO, in conjunction with the International Electrotechnical Commission (IEC) provides ongoing development, refinement and revision of biometric related standards under Joint Technical Committee 1, Sub Committee 37 (SC37), who have developed fingerprint related standards as follows:

Biometric Data Exchange Formats Standards

- ISO/IEC 19794-1:2011 Part 1: Framework
- ISO/IEC 19794-2:2011 Part 2: Finger minutiae data
- ISO/IEC 19794-3:2006 Part 3: Finger pattern spectral data
- ISO/IEC 19794-4:2011 Part 4: Finger image data
- ISO/IEC 19794-8:2011 Part 8: Finger pattern skeletal data
- ISO/IEC 19794-15:2017 Part 15: Palm crease image data

Biometric Sample Quality Standards

- ISO/IEC 29794-1: 2016 Part 1: Framework
- ISO/IEC 29794-4: 2017 Part 4: Finger image data

Prior to implementation, and to assure that biometric systems used by law enforcement are continually optimized at the highest level of security, privacy, efficiency and accuracy, routine performance testing at standardized levels should be determined as part of procurement activities per ISO 37's 19795 and 30107, as discussed previously. For example, the DHS Face Recognition Directive of 2023 requires such testing for any new or existing DHS biometric instance, a protocol followed by DHS components who voluntarily contract with the MdTF, funded by its Science and Technology Directorate. There are a few key elements to performance testing including the following tests: (1) **threshold**, (2) **algorithmic accuracy**, (3) **operational**, and (4) **demographic differential**.

- *When a threshold is incorporated into a use case, FISWG has a new document to help understand how to set accuracy thresholds*[156] *that should be consulted.*
- In regard to algorithmic accuracy testing, NIST's ongoing Face Recognition Technology Evaluation in one-to-many search is predominantly used to test the capabilities of a particular algorithm, showing results on different features such as speed, template size, accuracy (over various data types/qualities), and demographic performance.[157] *Biometric system operators should consult and consider NIST evaluations prior to procurement of a commercial vendor algorithm.*
- While there is a higher likelihood that an algorithm will perform well operationally if it has performed well in NIST testing, variability in front end capture will change accuracy results operationally. Thus, ISO's testing standards contains protocols for both scenario and operational testing.[158] *Existing and new biometric programs, prior to implementation and in regularly scheduled intervals, should conduct operational testing either by a credible third party, or with tests internally devised that meet ISO quality standards.*
- DHS S&T is currently leading the international effort at ISO to create specific testing for demographic differentials. *ISO/IEC DIS 19795-10 provides essential protocols to "quantify biometric system performance variation across demographic groups,"*[159] *and should be closely considered. From that vantage point, biometric technology system owners should minimize differentials and document with transparency what that differential is, how the system tolerates that differential, and what outcomes are acceptable and why.*

Interoperability and Data Sharing. While biometric algorithms are essential micro components of a biometric enterprise that help identify or verify individuals, that information's value is limited by the ability to share it appropriately with the right partners. As a result, interoperability protocols are key to sharing biometric information with the partners in the agreed upon format.

Within DHS, **OBIM's Futures Identity Program's Biometric Standards Reference Manual** is an updated interoperability document that "makes recommendations for biometric data formats implemented in the IDENT *eXchange Messages (IXM) Specification, v. 6.0.9.0.9*, transmission specifications employed for interoperability with external biometric systems, biometric sample quality standards, and best practices."[160] *For those law enforcement organizations seeking to share data with OBIM systems, adherence to this manual is critical.*

To effectively exchange identity data across jurisdictional lines or between dissimilar systems made by different manufacturers, standards specify a common format for the data exchange. This is important since data may be stored or transmitted in original or processed versions, such as a video clip where a face may be raw (as captured), cropped, compressed, or otherwise transformed. This is also the case with fingerprints where friction ridge minutiae are often required to be processed to be useful. Information compiled and formatted in accordance with this standard may be recorded using machine-readable media and may be transmitted by data communication facilities. Law enforcement, criminal justice agencies, and other organizations that process biometric data use the standard to exchange identity data. To enable interoperability, the U.S. government's biometric enterprise's interoperability is dependent upon **ANSI/NIST-ITL (current version 2015) Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information.**[161] Today this standard enables biometric interoperability between DHS, DOJ, DOS, INTERPOL, and NATO. It has also been adopted globally and is used for interchange of all biometric data in law enforcement.

While the ANSI/NIST-ITL standard provides baseline protocols for data, **NIEMOpen** attempts to answer the call on generalized interoperability and data sharing by assuring systems that have never exchanged information before – or "talked" – can do so, even if they speak slightly different languages. "Rather than starting from scratch, NIEMOpen can save organizations time and money by providing consistent, reusable, and repeatable data terms, definitions, and processes."[162] NIEM started as a partnership of the DOJ and DHS, beginning its work in 2008, with an initial mission to provide a common semantic approach to biometric data exchange.

NIEM transitioned to OASIS, an ANSI-accredited and ISO-recognized standards development organization, in October 2022.[163] With the alignment to standards development organization OASIS, NIEMOpen is now able to formally put forth its specifications as international standards and has access to a broader based community of both public and private sector professionals and organizations. In addition, NIEMOpen provides executive and technical training detailing everything from justification for usage of its protocols, to domain creation and implementation.[164] *LE and vendors should implement both ANSI/NIST common formats and NIEMOpen robust data models with highly refined sets of technical specifications to assure data is exchanged correctly and efficiently with partners.*

The FBI's NGI System provides LE and national security partners with the ability to identify latent prints obtained from evidence related to criminal and terrorism investigations. The governing policies and applicable laws, regulations, and Executive Orders for latent services are referenced in the FBI's PIA for the Next Generation Identification Latent Services.[165] Additional biometric specifications are compiled by the FBI's Criminal Justice Information Services Division (CJIS) and are publicly available.

DHS, DOJ, and OSTP endorse the FBI's policies and procedures as best practices for latent print services.[166]

8.3 Iris Recognition Technology and Standards

The iris is the ring that exists around the pupil of the eye. It ranges in colors from light grey, to blue, green, or brown. The iris consists of intricate layers containing muscles, collagen fibers, elastic fibers, vessels, various cells, and nerves. Together these layers create distinct patterns within the iris that are as unique to an individual as their fingerprints.

Professor John Daugman of Cambridge University created the first iris recognition algorithm in 1997. The algorithm, still widely used today, encodes the distinct patterns in the iris to identify individuals. Iris images are captured in the near-infrared (near-IR) color spectrum with a specialized camera. Near-IR imagery allows high quality visualization of the structures in the iris without the impediment of eye color. The iris algorithm finds the iris within that near-IR image and unrolls it, essentially creating a barcode known as iris code. This code contains pattern information specific to that individual iris. During enrollment, the iris code is saved in a repository with other iris enrollments. Iris searches operate in the same way. The algorithm locates the iris in the search image, creates the iris code, and compares that specific code against all the other codes kept in the repository. NIST's ongoing assessment of iris recognition algorithm performance shows the top performer's accuracy at over 99.99%.[167] Searches are completed by a 100 percent lights-out process, i.e., no human intervention is involved. The current NGI System's iris algorithm has a demonstrated accuracy of over 99 percent.

The following standards, published by the (ISO)/International Electrotechnical Commission (IEC), outline specifications for iris image capture and file formats required for exchange of information and interoperability between biometric systems:

> ISO/IEC 19794-6:2011: Information technology – Biometric data interchange formats – Part 6: Iris image data[168]
>
> ISO/IEC 29794-6:2015 - Information technology—Biometric sample quality—Part 6: Iris image data.[169]

In 2018, NIST created a document, summarizing these standards: *Iris Cameras: Standards Relevant for Camera Selection.*[170]

8.3.1 Iris Recognition Technology Standards

An iris submission is conducted in accordance with ANSI/NIST-ITL 1-2011 Publication, *Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information*.[171] ANSI/NIST-ITL Biometrics Standard. IRIS information is categorized under Type 17 (IRIS Image). Recent updates to the standard

include the 2013 Update and 2015/2018 XML Working Group efforts, though the maturity of the IRIS modality results in few modifications in later releases. NIEMOpen provides an extensive data model and process for facilitating information exchange. The NIEMOpen Biometrics Sub-Committee provides a domain-specific data model that is aligned to the ITL Biometric Standard and harmonizes across stakeholder transmission protocols (DoD EBTS, DHS IXM and DOJ EBTS). The Type-17 IRIS Record was added in NIEM Release 3.1 in 2013 and has been continually harmonized with ITL releases through current release 5. For individuals that have an existing FBI UCN, contributors can conduct a Biometric Image Submission (FIS) transaction to have the iris images added to the existing NGI record.

To help ensure that the highest quality iris images are captured, the NIST has published and widely distributed a "best practices" guide.[172] This is augmented by significant outreach efforts by FBI iris personnel to contributing agencies to assist them in developing departmental best practices.

In 2014, NIST published three documents providing guidance for proper capture of an iris image as part of NIST's Iris Exchange (IREX) program. These documents are geared towards users of iris recognition systems, generally local law enforcement, and are shared as a part of the FBI's Biometric Specification NGI Iris Service page.[173]

NIST Iris Expert's Group (IEG)

In 2015, NIST began hosting a forum for US government agencies, academia, and commercial vendors with vested interest in iris recognition called Iris Expert's Group (IEG).[174] The group meets annually to discuss topics affecting the iris recognition community and make recommendations as necessary. Members of IEG determined that there was a lack of standards pertaining to iris recognition, setting up monthly discussion groups that have produced standards documents on iris image capture and human iris examiner training that are currently in review at the OSAC. The group continues to work on standards in conjunction with their counterparts at the OSAC for publication by a Standards Development Organization (SDO). In 2018, NIST created a document summarizing these standards, *Iris Cameras: Standards Relevant for Camera Selection*.[175]

Organization of Scientific Area Committees for Forensic Science (OSAC) Facial & Iris Identification Subcommittee

OSAC was created by NIST in collaboration with DOJ in 2014. The purpose of OSAC is to "establish standards and best practices within and between [forensic science] disciplines related to terminology, methodologies, and training."[176] OSAC consists of seven scientific area committees, encompassing 22 discipline-specific subcommittees.[177] An Iris Task Group was added under the Facial Identification Subcommittee in 2021 to facilitate publication and adoption of standards documents being produced in IEG. The subcommittee was renamed to Facial and Iris Identification Subcommittee in 2024 when it was determined there is a need for more standards and best practices in the iris recognition community.

8.4 DNA Technology and Standards

8.4.1 FBI's Scientific Working Group on DNA Analysis Methods (SWGDAM)

Forensic DNA typing is a mature discipline. Since the first use of forensic DNA in the late 1980s, the FBI Laboratory has led national efforts to promulgate and continually revise national DNA typing standards, guidelines, and best practices. This work is conducted by the FBI's SWGDAM. SWGDAM is a body comprised of approximately 50 scientists (members and guests) who represent international, federal, state, and local forensic DNA laboratories and academia. SWGDAM meets on a regular basis to discuss relevant scientific topics and to draft, review, and revise DNA typing standards, guidelines, and best practices. SWGDAM's work products are publicly available. SWGDAM serves as a scientific forum to discuss, share, and evaluate forensic biology methods, protocols, training, and research to enhance forensic biology services. SWGDAM scientists serve as the DNA technical leaders or CODIS Administrators for their laboratories and offer practitioner perspectives on various DNA technologies and their operational applications.

The full SWGDAM body meets twice a year. However, its various committees and working groups meet on a more frequent basis to develop guidance and supporting materials for the forensic DNA community. SWGDAM guidelines serve as best practices for the U.S. forensic DNA typing community. The guidelines are publicly available online.[178]

DHS, DOJ, and OSTP endorse the FBI DNA QAS, the SWGDAM guidelines, and the FBI's DNA typing policies and procedures as best practices for forensic DNA typing.

8.4.1 Quality Assurance Standards for DNA Testing Laboratories

The Federal DNA Identification Act of 1994 directed the formation of a DNA Advisory Board (DAB) composed of scientists from the public and private sectors. The DAB's charge was to recommend QAS for use by forensic DNA testing laboratories. Its recommendations were originally adopted and issued by the FBI Director in 1998. The FBI's QAS were most recently revised in 2020. The QAS is augmented by statutory requirements for laboratory accreditation and external audits every two years. When the statutory term for the DAB expired in 2000, the SWGDAM was tasked with recommending revisions to the QAS to the FBI Director. While SWGDAM makes its recommendations, only the FBI is authorized by the Federal DNA Identification Act to issue standards and to ensure that all NDIS participating laboratories comply with those standards. The FBI's QAS for DNA Testing Laboratories and for DNA Databasing Laboratories are publicly available.[179]

Laboratories performing forensic DNA analysis that participate in the FBI's National DNA Index are subject to federal statutory requirements relating to quality assurance and privacy.[180] As early as 2006, laboratories that contributed DNA records to the national index were required to achieve and maintain accreditation (ISO 17025). Additionally, laboratories that conduct forensic DNA analysis are required to follow the FBI's QAS for DNA Testing Laboratories QAS.[181] These laboratories are also required to comply with rules governing the limited access and disclosure of DNA record information.[182] Moreover, federal law requires that laboratories undergo an external audit by qualified forensic DNA analysts every two years to document compliance with the QAS.[183]

The QAS describes the quality assurance requirements that laboratories performing forensic DNA testing must follow to ensure the quality and integrity of the data they generate. The QAS encompass all aspects of forensic analysis including quality assurance; organization and management; personnel;

training; facilities; evidence control; validation; analytical procedures; equipment calibration and maintenance; reports; review; proficiency testing; corrective action; audits; professional development; and outsourcing. .[184]

There are several QAS requirements regarding scientific validation. Validation is the process by which a scientific method is evaluated to determine its efficacy and reliability for forensic casework analysis. Validation studies identify the capabilities and limitations of a method and support a laboratory's development of standard operating procedures. Internal validation studies are subject to review for compliance with the QAS during external audits (Standard 15.2.2).

The QAS also has specific requirements regarding the validation of new software (Standard 8.8.). These include developmental validation; the acquisition of test data; the capabilities and limitations of a new method; internal validation; and the accumulation of laboratory-derived test data to demonstrate that the methods and procedures perform as expected. Standard 8.8.1.1 of the QAS requires that the underlying scientific principle(s) of software be documented in a publicly available format or in a peer-reviewed scientific journal. In accordance with these requirements, PGS developers have published their underlying scientific principles in peer-reviewed scientific journals.[185, 186]

The QAS also requires that individual forensic DNA laboratories validate the methods they use in DNA casework (QAS, Standard 8.8.2). In addition, several domestic and international professional forensic science organizations, including the SWGDAM[187] and the OSAC,[188] have published standards and guidelines that provide detailed guidance on validating probabilistic genotyping software.[189, 190, 191, 192, 193] Following these validation principles, the results of the FBI Laboratory's initial PGS validation study were published in a peer reviewed journal.[194] Moreover, a large compilation of data from the internal validation experiments of 31 different laboratories has been published. Collectively, these studies and many other scientific papers explore the variables and range of conditions encountered during DNA casework and demonstrate the sensitivity, specificity, accuracy, and reliability of PGS (specifically the STRmix™ software).[195]

Accredited forensic DNA laboratories must also comply with international and national standards such as ISO/IEC 17025: 2017[196] and ANSI National Accreditation Board (ANAB) AR 3125,[197] respectively, used by accreditation bodies during their conformity assessments. These standards require that testing methods (including software) used in forensic laboratories are fit for their intended purpose (ISO 17025: 2017, Standard 7.2.2).

DOJ and Laboratory-Level Requirements. DOJ has published Uniform Language for Testimony and Reports (ULTRs) applicable to several forensic disciplines practiced by DOJ laboratories.[198] Among these publications is the ULTR for Forensic Autosomal DNA Examinations Using PGS.[199] This document provides Department examiners a set of approved conclusions, qualifications, and limitations to be used during testimony and in published reports concerning DNA typing results generated by probabilistic genotyping systems.

In addition, quality management system documents for DNA typing at the FBI and ATF laboratories are available.[200] These documents include quality assurance measures and standard operating procedures for probabilistic genotyping examinations, interpretation, and reporting.

As a result of rigorous validation, accreditation requirements, regular assessments, standards, guidelines, and legal precedent, probabilistic genotyping is the current gold standard that aids analysts in the interpretation of single-source and mixed forensic DNA samples. It is a reliable, robust, and informative method for forensic DNA interpretation and for computing the statistical support for inferred genotypes.

8.4.2 FBI Laboratory DNA Policies and Procedures

The FBI Laboratory conducts STR, YSTR, and mitochondrial (mtDNA) DNA typing. The Laboratory's DNA policies and procedures are publicly available online.[201]

8.4.3 DNA Interoperability and Standards

Standards ensure common frameworks support exchange across the stakeholder specifications. ANSI/NIST-ITL—the primary DNA standard upon which DoD stakeholder DNA messaging protocols are based—is the ANSI/National Institute of Standards and Technology (NIST)-ITL Biometric standard. DNA was first included in the ANSI/NIST-ITL standard in the 2011 version, though DNA records and references predated this release in support of DOJ FBI's CODIS. In 2012, the INCITS updated its Biometrics Standards Framework (19794-8) to align the DNA Record with the ITL release. A 2020 ITL Working Group further updated the DNA Standard, aligning with both NIEM and INCITS.

Federal law requires that CODIS-participating laboratories undergo an external audit every two years to assess their compliance with the QAS. In addition, the Department of Justice's Office of the Inspector General audits CODIS laboratories for compliance with both the requirements of the Federal DNA Identification Act and adherence to the NDIS Operational Procedures. The FBI's CODIS Unit also conducts assessments of NDIS-participating laboratories as part of its administration of NDIS. The NDIS Operational Procedures manual is publicly available.[202]

NIEMOpen—The NIEMOpen Biometrics Sub-Committee provides a domain specific data model that is aligned to the ITL Biometric Standard and harmonizes across stakeholder transmission protocols (DoD EBTS, DHS IXM and DoJ EBTS). In 2013, NIEM release 3.0 included Type-18 DNA as aligned to the ITL standard 2013 Update. Release 5.0 was updated to align to 2020 ITL DNA Working Group Updates.

8.5 Interagency Collaboration

In 2003, the Executive Office of the President's National Science and Technology Council, Committee on Technology and Committee on Homeland and National Security, established a Subcommittee on Biometrics. The purpose of the Subcommittee "was to advise and assist the Committees and other coordination bodies of the Executive Office of the President on policies, procedures and plans for federally sponsored biometric and identity management activities. The Subcommittee will facilitate a strong, coordinated effort across federal agencies to identify and address important policy issues, as well as research, testing, standards, privacy, and outreach needs."[203]

The Subcommittee distributed a "Biometrics Catalog," described as a "US government sponsored database of information about the biometric technologies including research and evaluation reports,

government documents, legislative text, new articles, conference presentations, and vendors/consultants published at www.biometricscatalog.org."[204]

In 2006, the Subcommittee published a 57 page "Privacy & Biometrics: Building a Conceptual Framework"[205] with the end goal to:

> Bring the functional architecture of privacy to the functional architecture of biometrics. For each structural element of biometrics, the relevant portion of the privacy framework is applied and discussed. The integration of privacy and biometrics through interlaced functional architectures provides a conceptual foundation for designing and deploying privacy protective biometric systems without compromising efficient and effective operations. Privacy protective biometric technology provides an opportunity to connect information and individuals in a way that is both reliable and respectful.[206]

In 2009, the Subcommittee, now called the NSTC Subcommittee on Biometrics and Identity Management, published "Supplemental Information in Support of NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards."[207] That document established baseline requirements for today's federal biometric enterprise, insisting that the identity management systems supporting homeland and national security – those of DOD, DHS, and DOJ – be assessed to conform to data format and interoperability standards, biometric samples, metadata, and procurement requirements. It was this Subcommittee that also produced government-issued standards, including the IDENT Exchange Messages (IXM) Specification and the DOD Electronic Biometric Transmission Specification. Together, these specifications are still in use by both DOD and DHS today.[208] In addition to supporting standards, the Subcommittee also published a Catalog of USG Biometric Product Testing Programs, listing "Federal biometric testing and certification programs,"[209] to work alongside its standards protocols in assisting federal agencies in standing up viable biometric programs.

The last action of the Subcommittee took prior to its dissolution was creation of a "Registry of USG Recommended Biometric Standards, Version 5.0."[210] Released in September 2014, it covered standards for biometric algorithms of finger, face, scars/marks/tattoos/iris/DNA and other biometrics, as well as biometric transmission profiles that allow for the exchange of data. The dissolution of the Subcommittee left a leadership gap in interagency collaboration on biometrics.

SECTION VI: CONCLUSION

This report offered a comprehensive overview of key biometric technologies and their use to support the important LE and national security missions at DHS and DOJ. The *responsible* use of biometrics by federal law enforcement has been the mainstay goal of both Departments since the expansion of biometric use in the post 9/11 era. These technologies have proven time and again to be critical tools that benefit Americans, including facilitating secure and efficient travel and promoting safety and security by helping deter and investigate crime, terrorism, and other threats.

Biometrics technologies do not exist, however, in a vacuum; they are subject to continual improvement in efficacy and accuracy through innovation, research, and development; scientific research and advancement; and international standards and testing. Moreover, they are applied in a complex socio-political context that is informed by law, policies, procedures, and norms. Like any other LE tool, responsible use of biometrics is vital to engender public trust, transparency, and equity among the communities served by use of the technologies.

As the report makes clear, DHS and DOJ have a robust framework of guardrails in place for the biometric technologies they use for LE ends. This framework ensures the protection of privacy, civil rights, and civil liberties for individuals utilizing or subject to biometric systems, usability accommodations, and transparency with the public when such systems are under development and when deployed. The framework includes compliance with international biometrics standards. And it includes continual testing, evaluation, and improvement of biometric technology systems to ensure they perform at high levels of accuracy, biometric data protection and in closing the gap on the issue of demographic differentials that has dogged FRT discussions, in particular.

The report's best practices and guidelines offer a resource to FSLTT LEAs as they look to identify and utilize these technologies. Some states, localities, and other LE partners have already implemented policies to govern their use of biometrics, including ensuring a biometric match is not the sole basis for probable cause. Where additional development is needed, the content in this report outlines recommended policies, privacy, civil rights and civil liberties protections, standards, and other areas for consideration.

Like any technology, biometrics will continue to evolve in the coming years. As they do, ensuring transparency and engagement with the public and other stakeholders will be important to inform how the federal government responsibly implements biometrics programs. New use cases will also emerge, as will the need for improved interoperability and data sharing among LE partners. Given these dynamics, a strong, informed, and coordinated interagency approach to biometrics policy will be vital to maintaining U.S. national and homeland security.

Addendum:

State and Local Activity to Address LE Use of FRT

There is diverse FRT use at the state and local level. Where some state and local legislatures have been active in attempting to restrict or implement oversight on oversight on LE use of FRT, other state executive agencies have stood up biometric identity management systems that include facial recognition, drafted appropriations justifications, and more than half have signed FBI Memorandums of Understanding (MOUs) to share face images with the FBI's NGI.[211]

As of the writing of this report, 39 states have not restricted face recognition technologies, while eleven have limited or qualified its use in some manner. At least 11 state or local LEAs have invested in their own internal standalone identity management systems that include face recognition: Arizona,[212] Arkansas,[213] Delaware,[214] Indiana,[215] Michigan,[216] Nevada,[217] Pinellas County Florida (serves 243 local, state, and federal agencies that run close to 8,000 searches per month),[218] New York,[219] North Dakota,[220] South Carolina,[221] Tennessee.[222] These systems, even at the local level like Pinellas County, often service the entire state, other state jurisdictions, and federal partners as well. Other states and localities are pursuing either use of commercial face services, sometimes alongside their own identity management system. According to the Brookings Institution, about 17% of police departments use the outside, commercial face services of Clearview AI (3,100 of 18,000) as of 2021.[223]

Eleven states and the District of Columbia have restricted face recognition, although there is a wide swath of allowances and disallowance amongst those who have passed legislation addressing LE use of face recognition technologies. These are: Alabama,[224] Colorado,[225] Illinois,[226] Kentucky,[227] Maine,[228] Massachusetts,[229] New Hampshire,[230] Utah,[231] Vermont,[232] Virginia,[233] Washington[234] and the District of Columbia.[235] Five of these states (Colorado, Illinois, Maine, Utah, Washington) have restricted face recognition use by all its government workers, including law enforcement. The remainder place restrictions on law enforcement only. Meanwhile, California[236] let its ban related to face recognition coupled with body worn cameras expire in July 2023; California at the state level has no limits on face recognition use. Washington passed the first face recognition limitation law, requiring the use of testing performance metrics, but the law was not replicated elsewhere. The Washington law also exempted federal mandates or partnerships.

The strongest thread running through state and local law and policies – whether technically restricting or permitting face recognition technology use – is that the technology is not to be the "sole basis for probable cause." Such is clarified, for example, by Alabama, Colorado, Kentucky, Virginia, and by policy in Georgia's Cobb County,[237] and the cities of New Orleans[238] and New York City.[239] While no state fully bans LE use of face recognition, some are highly restrictive, with Maine and Vermont some of the most. Maine does not permit search of any other face databases other than its own driver license face repository but does permit use for probable cause for "serious crimes" and to identify missing, endangered, or deceased individuals. Vermont initially had a complete ban in place, but five months later reversed to make an allowance for child exploitation digital evidence.

Another nine states failed to pass restrictions: Connecticut,[240] Hawaii,[241] Idaho,[242] Iowa,[243] Kansas,[244] Louisiana,[245] Minnesota,[246] Nebraska,[247] and Tennessee.[248] Meanwhile, New Hampshire and Oregon's only restriction on face recognition technologies is with body worn cameras. Iowa and Kansas sought to ban face recognition with body worn cameras, but those measures failed.

Ohio's Attorney General conducted a task force on police use of face recognition technologies and found derogatory commentary about misuse by police mainly unfounded.[249] That report includes twelve recommendations.[250] Much of Ohio now uses the face services of Clearview AI.[251] Wisconsin completed its own comprehensive face recognition technology legislative activity report.[252]

Some of the most nuanced information related to FRT at the state and local level are proactive activities to provide guidance, policies, and appropriations justifications for LE face recognition activities. Of importance is that the issue of LE use of face recognition technologies has resulted in at least two major LE associations drafting lengthy and detailed reports, one providing guidance on implementing a responsible face recognition identity system, the other cataloguing use cases related to face recognition. Some of these nuances are:

- **State law codification of identity/face recognition services for LE use**
    - Delaware[253]
    - North Dakota[254]
- **Published face recognition technologies policies**
    - Three states:
        - Indiana[255]
        - Michigan[256]
        - West Virginia[257]
    - Five local jurisdictions:
        - Albuquerque, NM[258]
        - Cobb County, GA
        - Orlando, FL
        - New York City, NY[259]
        - Pinellas County, FL
- **Published state/local guidance by association**
    - Major Chiefs Association publishes *State Model FRT Policy*[260]
    - IJIS + International Association of Chiefs Police publishes *Law Enforcement Face Recognition Use Case Catalogue*[261]

- **Published appropriations justifications**
    - Arizona[262]
    - Arkansas
    - South Carolina[263]
    - Tennessee
    - West Virginia[264]

The highest volume of activity to fully ban face recognition use by LE occurred at the local level, with 28 localities passing significant limits on use of face recognition technologies, two of which reversed their decisions (Baltimore, MD[265] and New Orleans, LA). Most of these bans were enacted before 2022, with the exception of Anchorage, Alaska, which passed a ban in 2023.[266] These restrictions were concentrated in eight localities in both California[267] and Massachusetts[268] and one jurisdiction each in Louisiana, Maryland, Minnesota,[269] Mississippi,[270] Ohio,[271] Pennsylvania,[272] Texas,[273] Washington,[274] and Wisconsin.[275] Baltimore allowed its ban to expire as 2021 ended. New Orleans reversed its ban, articulating 18 crimes where face recognition could be applied.

About this Analysis

This analysis was initiated due to the focus on state and local guidelines required by the biometrics portion of the EO. All state and local legislative, policy, appropriations and task force activities within the states and associations that represent state/local activities was canvased. Data was parsed into the following categories:

- State level legislative activities to restrict use of face recognition in some form for:
    - all of government
    - law enforcement only
- Legislative expirations or reversals
- All local law activities, to limit or enable LE use
- Face recognition activities outside of legislatures, such as federal MOUs, appropriations, policies, statements, task forces, reports
- Unique attributes or details of an activity

This research is limited to what is publicly available, and does not include any proprietary or inside information, and thus does not purport to be comprehensive. Work on this topic requires ongoing attention.

Endnotes

[1] Executive Order 14074. (2022, May 25). *Advancing effective, accountable policing and criminal justice practices to enhance public trust and public safety* (Section 13(e)). Federal Register. https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and

[2] International Organization for Standardization. (2022). *Information technology—Vocabulary, Part 37: Biometrics* (ISO/IEC 2382-37:2022(E)). https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[3] National Commission on Terrorist Attacks Upon the United States. (2004). *Staff report of the National Commission on Terrorist Attacks upon the United States: 9/11 and terrorist travel*. https://govinfo.library.unt.edu/911/staff_statements/911_TerrTrav_Monograph.pdf

[4] National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission final report* (pp. 385-386). https://govinfo.library.unt.edu/911/report/911Report.pdf

[5] National Security Presidential Directive/NSPD-59 & Homeland Security Presidential Directive/HSPD-24. (2008, June 5). https://www.govinfo.gov/content/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf

[6] For existing authority for biometric interoperability prior to HSPD-24 and NSPM-7, see, e.g., Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, P.L. 104-208 codified at 8 U.S.C. § 1365a; Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000, P.L.106-215, codified at 8 U.S.C. § 1365a; Section 205 of the Visa Waiver Permanent Program Act of 2000, P.L. 106-396 codified at 8 U.S.C. § 1379; Section 403(c) and 414 of the US PATRIOT ACT, Public Law 107-56 codified at 8 U.S.C. § 1379, 8 U.S.C. § 1365a note; Section 202, 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002, Public Law 107-173 codified at 8 U.S.C. §§ 1722, 1731; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L.108-458 codified at 8 U.S.C. § 1365b; Section 711(d) of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L.110-53 codified at 8 U.S.C. § 1187.

[7] Privacy Act of 1974, 5 U.S.C. § 552A, *Privacy and Other Civil Liberty Implication.*

[8] Public Law 106-215, 8 U.S.C. § 1365a. (1999). *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*.

[9] Public Law 106-396, 8 U.S.C. § 1379. (2000). *Amendment to Immigration and Nationality Act of 1957*.

[10] Public Law 107-56, 8 U.S.C. § 1379, 1365a. (2001). *The Patriot Act*.

[11] Public Law 110-53, 8 U.S.C. § 1187. (2007). *Implementing recommendations of the 9/11 Commission Act*.

[12] Public Law 108-458, 8 U.S.C. § 1365b. (2004). *Amendment to the National Security Act of 1947*.

[13] U.S. Department of Justice. (n.d.). *The Attorney General's guidelines for domestic FBI operations*. https://www.justice.gov/archive/opa/docs/guidelines.pdf

[14] FBI. (2023, September 20). *Electronic Biometric Transmission Specification (EBTS) version 11.2*. FBIbiospecs. https://fbibiospecs.fbi.gov/file-repository/ebts-v11-2_final.pdf/view

[15] Federal Bureau of Investigation. (2020, June 16). *Criminal Justice Information Services (CJIS) security policy*. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf

[16] U.S. Department of Justice. (n.d.). *The Attorney General's guidelines for domestic FBI operations*. https://www.justice.gov/archive/opa/docs/guidelines.pdf

[17] Grother, P., et al. (2024, September 18). *Face recognition technology evaluation (FRTE) Part 2: Identification* (NIST Interagency Report 8271 Draft Supplement). National Institute of Standards and Technology. https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

[18] While biometrics like DNA are used for identification of individuals, face recognition technology (FRT) results are used as investigative leads that require further corroboration and are not considered positive identification. This different treatment arises because the field of FRT has not achieved the precision of biometrics like DNA.

[19] National Institute of Standards and Technology. (n.d.). *Face recognition technology evaluation (FRTE) "1 identification."* NIST. https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf

[20] Prest, E. M., & Winn, P. (2020, October 29). *Privacy impact assessment for the Next Generation Identification Iris Service*. U.S. Department of Justice, Federal Bureau of Investigation. https://www.fbi.gov/file-repository/pia-ngi-iris-service.pdf

[21] Katsanis, S. H., & Wagner, J. K. (2012). Characterization of the standard and recommended CODIS markers. *Journal of Forensic Sciences, 58*(August), S169–S172. https://doi.org/10.1111/j.1556-4029.2012.02253.x

[22] Buckleton, J.S., Bright, J.A., Gittelson, S., Moretti, T.R., Onorato, A.J., Bieber, F.R., et al. *The Probabilistic Genotyping Software STRmix: utility and evidence for its validity*, J. Forensic Sci. 64 (2019) 393 – 405.

[23] Scientific Working Group on DNA Analysis Methods (SWGDAM). (2015). *Guidelines for the validation of probabilistic genotyping systems*. https://www.swgdam.org/_files/ugd/4344b0_22776006b67c4a32a5ffc04fe3b56515.pdf (Accessed February 23, 2024).

[24] Kelly, H., Bright, J. A., & Buckleton, J. S. (2014). A comparison of statistical models for the analysis of complex forensic DNA profiles. *Science & Justice, 54*(1), 66–70.

[25] Jeanguenat, A. M., Budowle, B., & Dror, I. E. (2017). Strengthening forensic DNA decision-making through a better understanding of the influence of cognitive bias. *Science & Justice, 57*, 415–420.

[26] Buckleton, J. S., Bright, J. A., Gittelson, S., Moretti, T. R., Onorato, A. J., Bieber, F. R., et al. (2019). The probabilistic genotyping software STRmix: Utility and evidence for its validity. *Journal of Forensic Sciences, 64*, 393–405.

[27] Bright, J. A., Richards, R., Kruijver, M., Kelly, H., McGovern, C., Magee, A., ... & Buckleton, J. S. (2018). Internal validation of STRmix™: A multi-laboratory response to PCAST. *Forensic Science International: Genetics, 34*, 11–24.

[28] *United States v. Gissantaner*, 990 F.3d 457, 467 (6th Cir. 2021) ("[a]ll in all, STRmix satisfies Rule 702 and the case law construing it. In the words of Rule 702, it is the "product of reliable principles and methods"); *U.S. v. Anderson*, 2023 U.S. Dist. LEXIS 86810 (M.D. Penn. 2023) (TrueAllele); *People v. Wakefield*, 2022 N.Y. LEXIS 819 (N.Y. Ct. App. 2022) (TrueAllele); *State v. Simmer*, 935 N.W.2d 167 (Neb. 2019) (TrueAllele); *Commonwealth v. Foley*, 38 A.3d 882 (Pa. 2012) (TrueAllele); *People v. Davis*, 290 Cal. Rptr. 3d 661 (Cal. Ct. App. 2022) (STRmix); *Whittley v. State*, 2022 Tex. App. LEXIS 6336 (Tex. Ct. App. 2022) (STRmix found reliable); *U.S. v. Buck*, 2021 U.S. Dist. LEXIS 60421 (C.D. Cal. 2021) (court found that the scientific community has determined STRmix is reliable); *U.S. v. Green*, 2021 U.S. Dist. LEXIS 242578 (W.D.N.Y. 2021) (challenge to STRmix denied); *People v. Wilson*, 143 N.Y.S.3d 466 (N.Y. Ct. App. 2021) (True Allele held reliable); *United States v. Lewis*, 442 F. Supp. 3d 1122, 1155 (D. Minn. 2020) ("[T]here is no doubt that STRmix has gained general acceptance."); *United States v. Washington*, No. 8:19CR299, 2020 WL 3265142, at *2 (D. Neb. June 16, 2020) ("Authority and evidence demonstrate that STRmix is generally accepted by the relevant community."); *People v. Blash*, 2018 V.I. LEXIS 86 (V.I. 2018) (STRmix); *People v. Muhammad*, 326 Mich. App. 40, 931 N.W.2d 20, 30 (2018); *People v. Bullard-Daniel*, 54 Misc. 3d 177, 42 N.Y.S.3d 714, 724–25 (N.Y. Co. Ct. 2016); *United States v. Christensen*, 2019 U.S. Dist. LEXIS 24623 (C.D. Ill. 2019) (STRmix) ("STRmix has been repeatedly tested and widely accepted by the scientific community."); *United States v. Oldman*, 2018 U.S. Dist. LEXIS 232762 (D. Wy. 2018) (STRmix) (collecting cases); *U.S. v. Russell*, 2018 U.S. Dist. LEXIS 232864 (D. N.M. 2018) (STRmix) ("[STRmix's] analyses are based on calculations recognized as reliable in the field."); *United States v. Pettway*, 2016 WL 6134493, at *1 (W.D.N.Y.

Oct. 21, 2016) (discussing "exhaustive[ ] research[ ]" concluding that "the scientific foundations of the STRmix process are based on principles widely accepted in the scientific and forensic science communities").

[29] Parkavi, R., Chandeesh Babu, K. R., & Kumar, J. A. (2017). Multimodal biometrics for user authentication. In *2017 11th International Conference on Intelligent Systems and Control (ISCO)* (pp. 501–505). IEEE. https://doi.org/10.1109/ISCO.2017.7856044

[30] Ulery, B., Hicklin, A., Watson, C., Fellner, W., & Hallinan, P. (2006). *Studies of biometric fusion* (NISTIR 7346). National Institute of Standards and Technology. https://www.nist.gov/publications/studies-biometric-fusion

[31] Ulery, B., Hicklin, A., Watson, C., Fellner, W., & Hallinan, P. (2006). *Studies of biometric fusion* (NISTIR 7346). National Institute of Standards and Technology. https://www.nist.gov/publications/studies-biometric-fusion

[32] U.S. Department of Homeland Security. (2023, September 11). *Use of face recognition and facial capture technologies* (DHS Directives System 026-11). https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_026-11-use-face-recognition-face-capture-technologies.pdf

[33] U.S. Department of Justice. (2024, October). *Compliance Plan for OMB Memorandum M-24-10*. U.S. Department of Justice. https://www.justice.gov/media/1373026/dl

[34] U.S. Department of Justice, Bureau of Justice Assistance. (2024, September). *Edward Byrne Memorial Justice Assistance Grant (JAG) Program Frequently Asked Questions (FAQs)* (p. 20). https://bja.ojp.gov/doc/jag-faqs.pdf ("[For] JAG funds to be used for Facial Recognition Technology (FRT), the recipient must have policies and procedures in place to ensure that the FRT will be used in an appropriate and responsible manner that promotes public safety; and protects privacy, civil rights, and civil liberties; and complies with all applicable provisions of the U.S. Constitution, including the fourth amendment's protection against unreasonable searches and seizures, the first amendment's freedom of association and speech, and other laws and regulations. Recipients utilizing funds for FRT must make such policies and procedures available to DOJ upon request."

[35] U.S. Department of Homeland Security. (n.d.). *Privacy impact assessments (PIAs): A comprehensive collection*. Retrieved October 30, 2024, from https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29 This list is not comprehensive but represents an illustrative collection of cross-component and collaborative considerations regarding the use of biometry on an enterprise level. A complete list of published PIAs.

[36] U.S. Department of Justice. Office of Privacy and Civil Liberties. (n.d.). *DOJ systems of records*. Retrieved October 30, 2024, from https://justice.gov

[37] Grother, P., et al. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects* (NISTIR 8280). https://doi.org/10.6028/NIST.IR.8280

[38] Federation of American Scientists. (n.d.). National Crime Information Center (NCIC). Retrieved October 30, 2024, from https://irp.fas.org/agency/doj/fbi/is/ncic.htm

[39] IDENT will be replaced by the Homeland Advanced Recognition Technology (HART) system in the near future; however, all interoperability functions will remain the same.

[40] Federal Register. (2024, February 9). *The Federal Register*. https://www.ecfr.gov/current/title-28/chapter-I/part-20

[41] Federal Bureau of Investigation. (2022, March 10). *Privacy impact for the next generation identification latent services*. https://www.fbi.gov/file-repository/pia-next-generation-identification-latent-services.pdf/view.

[42] Federal Bureau of Investigation. (2023, June). *DOJ approved FBI next generation identification biometric interoperability privacy impact assessment*. https://www.fbi.gov/file-repository/pia-next-generation-identification-biometric-interoperability.pdf/view

[43] U.S. Department of Justice. (n.d.). *Foreign arrest fingerprints maintained by the FBI*.

[44] Federal Bureau of Investigation. (n.d.). *An ORI is a unique number identifying the authorized contributor of the biometric event to the NGI System*.

[45] U.S. Department of Justice. (n.d.). *A UCN is a unique number assigned to each identity maintained in the NGI System*.

[46] U.S. Department of Justice. (n.d.). *NCIC is a criminal justice system maintained by the CJIS Division that has separate privacy documentation*. Law enforcement users across the country query its files millions of times per day.

[47] The retention of sex offender records is currently under negotiation.

[48] Federal Bureau of Investigation. (2019, October 19). *NGI IPS privacy impact assessment (PIA)*. https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

[49] Civil fingerprints and other associated biometrics (i.e., photos) are submitted to the FBI for criminal background checks for non-criminal justice purposes, such as employment, licensing, and security clearances. Civil photos are not available for searching or dissemination to law enforcement agencies except when an individual also has a record in the criminal identity group. In this instance, all biometrics, including photos, become associated with the criminal identity and are available for searching and dissemination.

[50] Although national security photos are retained in the NGI System, their dissemination is strictly controlled by the FBI CJIS Division and the owners of the records. In general, national security photos are not disseminated to state and local law enforcement agencies unless the owner of the national security record coordinates with the LE submitter of the probe photo in the event of a potential investigative lead. Otherwise, the LE submitter will have no knowledge of the record.

[51] Federal Bureau of Investigation. (2024, January 21). *The FBI updated the NGI System's FR algorithm*.

[52] The patterns used in the NGI IPS algorithm may not correlate to obvious biological anatomical features such as the eyes, nose, or mouth.

[53] Facial Identification Scientific Working Group. (n.d.). *FISWG*. Retrieved April 3, 2024, from https://www.fiswg.org/documents.html

[54] U.S. Federal Register. (n.d.). *Privacy Act of 1974; System of Records*. Retrieved April 3, 2024, from https://www.federalregister.gov/documents/2019/10/09/2019-21585/privacy-act-of-1974-system-of-records

[55] U.S. Federal Register. (n.d.). *Privacy Act of 1974; System of Records*. Retrieved April 3, 2024, from https://www.federalregister.gov/documents/2019/10/09/2019-21585/privacy-act-of-1974-system-of-records

[56] U.S. Department of Homeland Security. (n.d.). *Artificial Intelligence Use Case Inventory*. Retrieved November 15, 2024, from https://www.dhs.gov/data/AI_inventory

[57] U.S. Immigration and Customs Enforcement. (n.d.). *Homeland Security Investigations*. Retrieved January 28, 2024, from https://www.ice.gov/about-ice/homeland-security-investigations

[58] U.S. Immigration and Customs Enforcement. (n.d.). *Enforcement and Removal Operations (ERO)*. Retrieved January 28, 2024, from https://www.ice.gov/about-ice/ero

[59] U.S. Department of Homeland Security. (2019, June 18). *Privacy threshold analysis: Homeland Security Investigations Child Exploitation Investigations Unit*.

[60] U.S. Department of Homeland Security. (2010, January 14). *Privacy impact assessment for the Enforcement Integrated Database (EID)*.

[61] U.S. Department of Homeland Security. (2019, May 14). *Privacy impact assessment update for the Enforcement Integrated Database (EID) – EAGLE, EDDIE, and DAVID* (DHS/ICE/PIA-015(j)).

[62] U.S. Federal Register. (2018, May 3). *Privacy Act of 1974: System of records*. https://www.federalregister.gov/documents/2018/05/03/2018-09362/privacy-act-of-1974-system-of-records

[63] U.S. Department of Homeland Security. (2019, May 14). *Privacy threshold analysis update for Intensive Appearance Technology Services System (IATSS)*.

[64] U.S. Secret Service. (n.d.). *Authorized collection of information maintained in FDNS*. Retrieved October 30, 2024. The USSS is authorized to collect information maintained in its FDNS pursuant to 18 U.S.C. § 1029(d), 1030(d), 3056, and 3056A; 5 U.S.C. § 1104 and 9101; Executive Order 9397 (as amended); and 5 C.F.R. Chapter 1, Subchapter B, Parts 731, 732 and 736. Supporting authority includes Pub. L. 92-544 (Title II) and Pub. L. 107-56 (Title II). Supplemental regulatory authority includes 28 CFR 0.85, Part 20, and 50.12.

[65] U.S. Department of Homeland Security. (2022, October 25). *DHS privacy threshold analysis for the U.S. Secret Service Forensic Services Division System*.

[66] U.S. Department of Homeland Security. (2017, May). *DHS privacy impact assessment for the Forensic Services Division System* (DHS/USSS/PIA-017).

[67] U.S. Department of Homeland Security. (2020, May 8). *DHS privacy impact assessment for the Forensic Services Division System* (DHS/USSS/PIA-017(a)).

[68] U.S. Department of Homeland Security. (2024, May 6). *Privacy Impact Assessment (PIA) for the United States Secret Service: PIA-USSS-017B FSDS* [PDF]. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2024-05/24_0506_priv_pia-usss-017b-fsds.pdf

[69] U.S. Secret Service (USSS). (n.d.). *Probe images and candidate lists within investigative case file*. Subject to Records Control Schedule DAA-0563-2013-0001, approved by the National Archives and Records Administration (NARA).

[70] U.S. Department of Homeland Security. (2024, May). *Privacy Impact Assessment (PIA) for the United States Secret Service: DHS-USSS-PIA-033 USSS use of facial recognition technology* [PDF]. Department of Homeland Security. https://www.dhs.gov/publication/dhsussspia-033-usss-use-facial-recognition-technology

[71] Federal Bureau of Investigation. (n.d.). CODIS-NDIS statistics. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis/codis-ndis-statistics

[72] Federal Bureau of Investigation. (n.d.). *DNA Identification Act of 1994* (34 U.S.C. §12591 et seq.), the FBI Director's Quality Assurance Standards for DNA Databasing and Forensic DNA Testing Laboratories, privacy act notice on the National DNA Index System, and the NDIS Operational Procedures Manual. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[73] Federal Bureau of Investigation. (n.d.). *The 20 CODIS core loci*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[74] Federal Bureau of Investigation. (n.d.). *NDIS operational procedures manual*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis (pp. 71-78).

[75] U.S. Code. (n.d.). *34 U.S.C. §§12592(b)(3), 12593(c)*.

[76] Federal Bureau of Investigation. (2023). *QAS standard 11.3 and NDIS operational procedures manual chapter 6.0 confirmation and hit dispositioning*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[77] Federal Register. (2008, December 10). *Vol. 73, No. 238*, 74937. Massachusetts Forensic Science Oversight Board. (2021, March 24). *Report on S. 2480, "An Act Permitting Familial Searching and Partial DNA Matches in Investigating Certain Crimes," and related recommendations pertaining to G.L. c. 22E governing the Massachusetts*

Statewide DNA Database. Retrieved from https://www.mass.gov/doc/forensic-science-oversight-board-familial-dna-searching-report-march-24-2021/download

[78] Department of Justice. (n.d.). *Privacy Act of 1974; New System of Records*. Retrieved April 3, 2024, from https://www.justice.gov/opcl/docs/61fr37495.pdf

[79] Department of Justice. (n.d.). *Privacy Act of 1974; New System of Records*. Retrieved April 3, 2024, from https://www.govinfo.gov/content/pkg/FR-1998-02-20/pdf/98-4206.pdf

[80] Department of Justice. (n.d.). *Privacy Act of 1974; New System of Records*. Retrieved April 3, 2024, from https://www.justice.gov/opcl/page/file/1419896/download

[81] Federal Bureau of Investigation. (n.d.). *Privacy Impact Assessment for the Combined National Deoxyribonucleic Acid (DNA) Index System (CODIS)*. Issued by Erin M. Prest, Privacy and Civil Liberties Officer. Retrieved April 3, 2024, from https://www.fbi.gov/file-repository/pia-combined-national-deoxyribonucleic-acid-dna-index-system-codis-031423.pdf

[82] *NDIS Operational Procedures Manual*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[83] Federal DNA Identification Act, 34 U.S.C. § 12592(b)(1), (2). Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[84] U.S. Department of Justice, Office of the Inspector General. (2018). *Combined DNA Index System Audits*. Retrieved from https://oig.justice.gov/reports/codis-ext.htm

[85] Department of Justice. (n.d.). *Privacy Act of 1974; New System of Records*. Retrieved April 3, 2024, from https://www.govinfo.gov/content/pkg/FR-1998-02-20/pdf/98-4206.pdf, pp. 8-9, 11-12.

[86] *34 U.S.C. § 12591(a)(5)(B). Retrieved from https://www.govinfo.gov/link/uscode/34/12591*

[87] Rapid DNA Act of 2017, Public Law 115-50 (2017-2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/510/text

[88] 34 U.S.C. § 12591(a)(5)(A). Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[89] *Standards for the Operation of Rapid DNA Booking Systems by Law Enforcement Booking Agencies and the National Rapid DNA Booking Operational Procedures Manual*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis

[90] U.S. Department of Justice. (2019). *Interim policy for forensic genetic genealogical DNA analysis and searching*. Effective 11/01/2019. Retrieved February 13, 2024, from https://www.justice.gov/olp/page/file/1204386/download The FBI uses the term investigative genetic genealogy (IGG) although the following terms may also be used to describe this technique: forensic genealogy, forensic genetic genealogy, forensic genetic genealogical DNA analysis and searching, forensic investigative genetic genealogy and investigative genealogy. See, for example, U.S. Department of Justice Interim Policy Forensic Genetic Genealogical DNA Analysis and Searching, Effective 11/01/2019, available at https://www.justice.gov/olp/page/file/1204386/download (last access date February 13, 2024).

[91] Wickenheiser R. A. (2019). Forensic genealogy, bioethics and the Golden State Killer case. Forensic science international. Synergy, 1, 114–125. https://doi.org/10.1016/j.fsisyn.2019.07.003 (last accessed February 22, 2024).

[92] The Marshall Project. (2019, July 16). In an apparent first, genetic genealogy aids a wrongful conviction case. https://www.themarshallproject.org/2019/07/16/in-an-apparent-first-genetic-genealogy-aids-a-wrongful-conviction-case (last accessed February 3, 2020). *See generally*, 1:114-125.

[93] ISOGG.org. (n.d.). *Autosomal DNA testing comparison chart.* https://isogg.org/wiki/Autosomal_DNA_testing_comparison_chart (last accessed February 22, 2024).

[94] ISOGG.org, https://isogg.org/wiki/Autosomal_DNA_testing_comparison_chart. (last access date February 22, 2020).

[95] Bettinger, B. (2017). The Genetic Genealogist: August 2017 update to the Shared cM Project. https://thegeneticgenealogist.com/2017/08/26/august-2017-update-to-the-shared-cm-project/ (last accessed February 3, 2020). GEDmatch is a third-party genealogy service. GEDmatch does not provide genetic testing services but instead provides a central location for users to upload and share their SNP file and provides tools to users to help them identify possible genetic relatives among other users of the service.

[96] Bettinger, B. (2017). The Genetic Genealogist: August 2017 update to the Shared cM Project. https://thegeneticgenealogist.com/2017/08/26/august-2017-update-to-the-shared-cm-project/ (last accessed February 3, 2020).

[97] Greytak, E., Moore, C., & Armentrout, S. (2019). Genetic genealogy for cold case and active investigations. *Forensic Science International, 299,* 103-113. https://doi.org/10.1016/j.forsciint.2019.05.028

[98] United States Department of Justice. (n.d.). Interim policy for forensic genetic genealogical DNA analysis and searching. https://www.justice.gov/olp/forensic-science. In UHR investigations, the law enforcement agency may need to obtain a DNA sample from the relative(s) of the person of interest for forensic DNA analysis for exclusionary/inclusionary purposes when no reference STR can be obtained.

[99] United States Department of Justice. (n.d.). Interim policy for forensic genetic genealogical DNA analysis and searching. https://www.justice.gov/olp/forensic-science.

[100] National Academies of Sciences, Engineering, and Medicine. (n.d.). Facial recognition: Current capabilities, future prospects, and governance. https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance (last accessed October 2024).

[101] At the time that the NASEM FRT report was published in December 2023, all six known cases of wrongful arrests involving FRT were of Black individuals. In January 2024, several news outlets reported on the wrongful arrest of a white man.

[102] Federal Register. (2021). Notice of request for information (RFI) on public and private sector uses of biometric technologies. https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies (last accessed October 2024).

[103] National Academies of Sciences, Engineering, and Medicine. (n.d.). Law enforcement use of probabilistic genotyping, forensic DNA phenotyping, and forensic investigative genetic genealogy technologies: A workshop. https://www.nationalacademies.org/our-work/law-enforcement-use-of-probabilistic-genotyping-forensic-dna-phenotyping-and-forensic-investigative-genetic-genealogy-technologies-a-workshop (last accessed October 2024).

[104] Kinsey, K. (2024, March 8). Testimony to U.S. Commission on Civil Rights. Policing Project at NYU School of Law.

[105] This list is not exhaustive; other factors such as psycholinguistics, neurolinguistics, biometric ID issues, medical privacy based upon linguistics, and equal protection may be relevant.

[106] White House. (2024). Draft guidance for 2024 agency artificial intelligence reporting per EO 14110. https://www.whitehouse.gov/wp-content/uploads/2024/03/DRAFT-Guidance-for-Agency-Artificial-Intelligence-Reporting-per-EO14110.pdf (last accessed October 2024). See draft guidance for 2024 agency artificial intelligence reporting per EO 14110.

[107] Alabama, Colorado, Kentucky, Virginia, and Georgia's Cobb County, and the cites of New Orleans and New York City have implemented this practice through statute or policy.

[108] Facial Identification Scientific Working Group. (n.d.). https://www.fiswg.org/

[109] Department of Justice, Bureau of Justice Assistance. (2024, September). *Edward Byrne Memorial Justice Assistance Grant (JAG) Program frequently asked questions (FAQs)* (p. 20). U.S. Department of Justice, Bureau of Justice Assistance. https://bja.ojp.gov/doc/jag-faqs.pdf

[110] ISO/IEC JTC 1/SC 37. (n.d.). Working groups. ISO/IEC JTC 1/SC 37 is made up of six working groups (WGs), each of which carries out specific tasks in standards development within the field of biometrics. The focus of each working group is described in the group's terms of reference. Working groups of ISO/IEC JTC 1/SC 37 are: ISO/IEC JTC 1/SC 37/WG 1 Harmonized Biometric Vocabulary; ISO/IEC JTC 1/SC 37/WG 2 Biometric Technical Interfaces; ISO/IEC JTC 1/SC 37/WG 3 Biometric Data Interchange Formats; ISO/IEC JTC 1/SC 37/WG 4 Technical Implementation of Biometric Systems; ISO/IEC JTC 1/SC 37/WG 5 Biometric Testing and Reporting; ISO/IEC JTC 1/SC 37/WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics. https://committee.iso.org/home/jtc1sc37 (accessed February 29, 2024).

[111] ISO. (n.d.). ISO committee catalogue. https://www.iso.org/committee/313770/x/catalogue/ (accessed February 9, 2024).

[112] ISO. (n.d.). Search results for 39794. https://www.iso.org/search.html?q=39794 (accessed February 29, 2024).

[113] ISO. (n.d.). Search results for 29794. https://www.iso.org/search.html?q=29794 (accessed February 29, 2024).

[114] ISO/IEC. (n.d.). ISO/IEC 19795 biometric performance testing and reporting. https://www.nist.gov/system/files/documents/2020/12/15/340_1_mansfield_panel_ibpc.pdf (accessed February 29, 2024).

[115] ISO/IEC. (2023). ISO/IEC 30107-1:2023: Information technology - Biometric presentation attack detection - Part 1: Framework. https://www.iso.org/standard/83828.html (accessed February 29, 2024).

[116] ISO/IEC. (2022). ISO/IEC 2382-37:2022 information technology vocabulary part 37: Biometrics. https://www.iso.org/standard/73514.html?browse=tc (accessed February 9, 2024).

[117] ISO/IEC. (2023). ISO/IEC 24714:2023(en) biometrics—Cross-jurisdictional and societal aspects of biometrics—General guidance. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24714:ed-1:v1:en (accessed February 23, 2024) https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24714:ed-1:v1:en

[118] ISO/IEC. (2023). ISO/IEC 24714:2023(en) biometrics—Cross-jurisdictional and societal aspects of biometrics—General guidance. Defines accessibility as “extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of user needs, characteristics and capabilities to achieve identified goals in identified contexts of use.” Note 1 to entry: Context of use includes direct use or use supported by assistive technologies. [SOURCE: ISO 9241-112:2017, 3.15]. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24714:ed-1:v1:en (accessed February 23, 2024).

[119] International Association for Identification. (n.d.). https://www.theiai.org/ (accessed February 9, 2024).

[120] National Institute of Standards and Technology. (n.d.). Organization of scientific area committees for forensic science. https://www.nist.gov/organization-scientific-area-committees-forensic-science (accessed February 9, 2024).

[121] Facial Identification Scientific Working Group. (n.d.). https://www.fiswg.org/ (accessed February 9, 2024).

[122] ISO/IEC. (2023). DRAFT ISO/IEC 29794-5:2023(CD3) information technology - biometric sample quality - Part 5: Face image data. ISO/IEC JTC 1/SC 37 (Biometrics)/WG 3, Secretariat: ANSI (October 2023).

[123] ISO/IEC. (2023). DRAFT ISO/IEC 29794-5:2023(CD3) information technology - biometric sample quality - Part 5: Face image data. ISO/IEC JTC 1/SC 37 (Biometrics)/WG 3, Secretariat: ANSI (October 2023), p. 1.

[124] ISO/IEC. (2023). DRAFT ISO/IEC 29794-5:2023(CD3) information technology - biometric sample quality - Part 5: Face image data. ISO/IEC JTC 1/SC 37 (Biometrics)/WG 3, Secretariat: ANSI (October 2023), p. viii.

[125] ISO/IEC. (2023). DRAFT ISO/IEC 29794-5:2023(CD3) information technology - biometric sample quality - Part 5: Face image data. ISO/IEC JTC 1/SC 37 (Biometrics)/WG 3, Secretariat: ANSI (October 2023), p. viii.

[126] Trained users of facial recognition systems in law enforcement may bear different titles such as "examiner," "reviewer," or "analyst." In some cases, those who bear these titles may carry responsibilities beyond candidate list adjudication.

[127] Cook, C. M., et al. (2023). Demographic effects across 158 facial recognition systems. Department of Homeland Security S&T Technical Paper Series. https://dhs.gov/publication/demographic-effects-facial-recognition-across-158-system-combinations-over-four-studies (accessed August 2023).

[128] National Institute of Standards and Technology. (n.d.). Face recognition technology evaluation (FRTE) 1:1 verification. https://pages.nist.gov/frvt/html/frvt11.html

[129] Phillips, P. J., et al. (1996). *FERET (Face Recognition Technology): Recognition algorithm development and test results*. Army Research Laboratory. https://www.nist.gov/system/files/documents/2021/04/27/feret3.pdf; Phillips, P. J. (2007). *FRVT 2006 and ICE 2006 large-scale results: Face recognition vendor test 2006*. National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51131

[130] Norman, J. (n.d.). Woodrow Bledsoe originates automated facial recognition. History of Information. https://www.historyofinformation.com/detail.php?id=2126 (accessed January 15, 2024).

Since its origin in the 1960s at Panoramic Research in Palo Alto, California, automated FRT has improved dramatically in terms of accuracy. Norman, Jeremy. "Woodrow Bledsoe Originates Automated Facial Recognition." History of Information, https://www.historyofinformation.com/detail.php?id=2126. Accessed 15 January 2024.

[131] Grother, P., Ngan, M., & Hanaoka, K. (2024). NISTIR 8271 draft supplement, face recognition technology evaluation (FRTE), part 2: Identification. https://www.nist.gov/publications/frvt_1N_report.pdf

[132] National Institute of Standards and Technology. (n.d.). *Face recognition technology evaluation (FRTE) 1:1 verification*. https://pages.nist.gov/frvt/html/frvt11.html

[133] National Institute of Standards and Technology. (2017, March). *Face in video evaluation*. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

[134] National Institute of Standards and Technology. (2017). *Face in video evaluation*. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

[135] Howard, J. J., Sirotin, Y., & Vermury, A. (2019). The effect of broad and specific homogeneity on the imposter distributions and false match rates in face recognition algorithm performance. In Proceedings of the 10th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2019), Tampa, FL.

[136] Mansfield, T. (2023). Facial recognition technology in law enforcement equitability study: Final report. National Physical Laboratory. https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

[137] Bhatta, A., et al. (2024). *Impact of blur and resolution on demographic disparities in 1-to-many facial identification*. Computer Vision and Pattern Recognition. https://arxiv.org/abs/2309.04447

[138]National Institute of Science and Technology. (2019, December 19). NIST study evaluates effects of race, age, sex on face recognition software. https://nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[139] Grother, P., et al. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects* (NISTIR 8280). https://doi.org/10.6028/NIST.IR.8280

[140] National Institute of Science and Technology. *Face recognition technology evaluation (FRTE) 1:1 verification*. https://pages.nist.gov/frvt/html/frvt11.html

[141] Mansfield, T. (2023, March). *Facial recognition technology in law enforcement equitability study, final report*. National Physical Laboratory. https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

[142] Bhatta, A., et al. (2024). *Impact of blur and resolution on demographic disparities in 1-to-many facial identification*. Computer Vision and Pattern Recognition. https://arxiv.org/abs/2309.04447

[143] Bhatta, A., et al. (2024). *Impact of blur and resolution on demographic disparities in 1-to-many facial identification*. Computer Vision and Pattern Recognition. https://arxiv.org/abs/2309.04447

[144] International Standards Organization/International Electrotechnical Commission (ISO/IEC). (2007). *19795-2:2007 Information technology–Biometric performance testing and reporting–Part 2: Testing methodologies for technology and scenario testing*. https://www.iso.org/standard/41448.html

[145] TVS is the backend matching service for all biometric entry and exit operations that use facial comparison, regardless of air, land, or sea. Regardless of the method of entry or exit (e.g., pedestrian, vehicle, cruise ship, vessel, or airplane), TVS conducts the backend biometric matching and provides a result to different CBP systems depending on the environment. The corresponding biographic data from the biometric match is then used in other systems to create the crossing record.

[146] MDTF. (2021). *2021 Biometric Rally results*. https://mdtf.org/Rally2021/Results2021

[147] MDTF. (2022). *2022 Biometric Rally results*. https://mdtf.org/Rally2022/Results

[148] Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L., & Vemury, A. R. (2023). *Demographic effects across 158 facial recognition systems*.

[149] International Standards Organization/International Electrotechnical Commission (ISO/IEC). (2007). *19795-10:2024 Information technology–Biometric performance testing and reporting–Part 10: Quantifying biometric system performance variation across demographic groups*. https://www.iso.org/standard/81223.html

[150] Howard, J. J., Sirotin, Y. B., & Vemury, A. R. (2019, September). The effect of broad and specific demographic homogeneity on the imposter distributions and false match rates in face recognition algorithm performance. In *2019 IEEE 10th international conference on biometrics theory, applications and systems (BTAS)* (pp. 1-8). IEEE.

[151] Howard, J. J., Sirotin, Y. B., Tipton, J. L., & Vemury, A. R. (2020). *Quantifying the extent to which race and gender features determine identity in commercial face recognition algorithms*. DHS Technical Publication Series.

[152] Howard, J. J., Laird, E. J., & Sirotin, Y. B. (2022, August). Disparate impact in facial recognition stems from the broad homogeneity effect: A case study and method to resolve. In *International Conference on Pattern Recognition* (pp. 448-464). Cham: Springer Nature Switzerland.

[153] Howard, J. J., Rabbitt, L. R., & Sirotin, Y. B. (2020). Human-algorithm teaming in face recognition: How algorithm outcomes cognitively bias human decision-making. *PLOS ONE, 15*(8), e0237855.

[154] IEEE Certified Biometrics Professional. (n.d.). *Biometric System Design and Evaluation* (Module 3, pp. 3-126).

[155] FBI. (n.d.). FBI-Certified Biometric Devices. Retrieved from https://fbibiospecs.fbi.gov/certifications-1/cpl

[156] FISWG. (2022). *FR Systems Operation Assurance: Scoring Thresholds v1.1* (Nov. 11, 2022). Retrieved from https://www.fiswg.org/fiswg_fr_sys_oper_assur_scoring_thresholds_v1.1_2022.11.04.pdf. FR Systems Operation Assurance: Scoring Thresholds v1.1 (Nov. 11, 2022). Scope, "Provide a detailed process and examples of how to evaluate scoring thresholds when adjusting operational workflows… This document will focus on how analysis can support a systematic process to determine appropriate facial scoring thresholds to support end user requirements. This document is relevant to systems that operate with automated workflows as well as investigative systems requiring a human practitioner to review a candidate list. Understanding how to evaluate facial biometric scoring is critical for both system accuracy and workflows of the human practitioners."

[157] NIST. (n.d.). *Face Recognition Technology Evaluation (FRTE) 1Identification*. Retrieved February 22, 2024, from https://pages.nist.gov/frvt/html/frvt1N.html

[158] ISO/IEC. (2007). *19795-2:2007/AMD 1:2015, Information technology: Biometric performance testing and reporting, Part 2: Testing methodologies for technology and scenario evaluation*. Retrieved from https://www.iso.org/standard/41448.html. This standard is reviewed every 5 years and updated. https://www.iso.org/standard/41448.html

[159]ISO/IEC. (n.d.). *DIS 19795-10, Information technology: Biometric performance testing and reporting, Part 10: Quantifying biometric system performance variation across demographic groups* (under development). Retrieved February 24, 2024, from https://committee.iso.org/standard/81223.html?browse=tc

[160] Boyd, J. (2024). *Biometric Standards Reference Manual for OBIM*.

[161] ANSI/NIST. (2015). *ITL 1-2015*. Retrieved from https://www.nist.gov/system/files/documents/2020/11/03/1.ANSI_NIST-SP-500-290e3.pdf. Prior to that, ANSI/NBS-ICST 1-1986, was published by NIST (formerly the National Bureau of Standards) in 1986. It was a fingerprint minutiae-based standard. Revisions to the standard were made in 1993, 1997, 2000, and 2007. Updates to the standard are designed to be backward compatible, with new versions including additional information. All of those versions use "traditional" encoding.

[162] NIEM. (n.d.). *About NIEM*. Retrieved February 23, 2024, from https://www.niem.gov/about-niem. In 2008, 'NIEM-conformant encoding' using Extensible Markup Language (XML) was adopted. NIEM is designed to provide a common semantic approach in XML applications. With some minor exceptions, the 2007 and 2008 versions of the standard are equivalent except for the encoding format. In 2009, an amendment to the 2007 and 2008 versions was approved that extended codes to handle multiple finger capture.

[163] NIEM. (n.d.). *NIEM Transition to OASIS Open Project*. Retrieved February 23, 2024, from https://www.niem.gov/about-niem/news/niem-transition-oasis-open-project

[164] NIEM. (n.d.). *NIEM GitHub repository*. Retrieved February 23, 2024, from https://niem.github.io

[165] Federal Bureau of Investigation. (n.d.). *Privacy Impact Assessment – FBI NGI Latent Services*. Retrieved from https://www.fbi.gov/file-repository/pia-next-generation-identification-latent-services.pdf/view

[166] Federal Bureau of Investigation. (n.d.). *Privacy Impact Assessment – FBI NGI Latent Services*. Retrieved from https://www.fbi.gov/file-repository/pia-next-generation-identification-latent-services.pdf/view

Federal Bureau of Investigation. (n.d.). *Next Generation Identification System*. Retrieved from https://fbilabqsd.fbi.gov/file-repository/latent-prints/frd-600-10-next-generation-identification-system.pdf/view

Federal Bureau of Investigation. (n.d.). *Resources for recording friction ridges and biometric training guides and documents*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/biometric-training

Federal Bureau of Investigation. (n.d.). *Recording legible fingerprints guidance*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/recording-legible-fingerprints

Federal Bureau of Investigation. (n.d.). *Training opportunities - Advanced comparison for tenprint examiners; scientific basics of fingerprints: Classifying, recording, and comparing including the scientific basics of palm prints – Recording; and universal latent workstation software (ULW) workshop*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/biometric-and-criminal-history-record-training

Federal Bureau of Investigation. (n.d.). *Ordering fingerprint cards and training aids*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/ordering-fingerprint-cards-and-training-aids

Federal Bureau of Investigation. (n.d.). *Recording friction ridges and biometric training guides and documents*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/biometric-training

Federal Bureau of Investigation. (n.d.). *Postmortem printing series training, deceased persons identification best practices, and recording legible fingerprint guidance*. Retrieved from https://fbibiospecs.fbi.gov/biometric-training

Palm Prints:

Federal Bureau of Investigation. (2021). *The FBI National Palm Print System (Tri-fold brochure)*. Retrieved from https://fbibiospecs.fbi.gov/file-repository/palm/palm-guide-brochure-06302021.pdf/view

Federal Bureau of Investigation. (2019). *Palm print capture poster*. Retrieved from https://fbibiospecs.fbi.gov/file-repository/palm/palm_print_poster_v2-0-rev10012019.pdf/view

Federal Bureau of Investigation. (n.d.). *Guidelines for capturing palm prints and supplementals*. Retrieved from https://le.fbi.gov/file-repository/guidelines-for-capturing-palm-prints-and-supplementals.pdf/view

Federal Bureau of Investigation. (n.d.). *Palm print training guides and resources*. Retrieved from https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/biometrics/biometric-training

[167] NIST. (n.d.). *IREX 10*. Retrieved from https://pages.nist.gov/IREX10/

[168] International Organization for Standardization. (n.d.). *ISO/IEC 50868:2014: Information technology—Biometric data interchange formats—Part 1: Fingerprint data interchange format*. Retrieved from https://www.iso.org/standard/50868.html

[169] International Organization for Standardization. (n.d.). *ISO/IEC 54066:2017: Information technology—Biometric data interchange formats—Part 3: Iris data interchange format*. Retrieved from https://www.iso.org/standard/54066.html

[170] National Institute of Standards and Technology. (2018). *Iris cameras: Standards for relevant camera selection*.

Retrieved from https://www.nist.gov/publications/iris-cameras-standards-relevant-camera-selection-2018

[171] Mangold, K. (2016). *Data format for the interchange of fingerprint, facial & other biometric information: ANSI/NIST-ITL 1-2011 NIST special publication 500-290 edition 3*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=921456 (Accessed April 1, 2024)

[172] NIST. (n.d.). *Iris Exchange (IREX) V: Guidance for iris image collection*. Retrieved from https://www.nist.gov/itl/iad/image-group/irex-v-homepage

[173] FBI. (n.d.). *NGI Iris Services—BioSpecs*. Retrieved from https://fbibiospecs.fbi.gov/biometric-modalities-1/ngi-iris-services

NIST. (n.d.). *Iris Experts Group II Homepage*. Retrieved from https://www.nist.gov/programs-projects/iris-experts-group-ii-homepage

[174] NIST. (n.d.). *Iris Experts Group II Homepage*. Retrieved from https://www.nist.gov/programs-projects/iris-experts-group-ii-homepage

[175] NIST. (2018). *Iris cameras: Standards for relevant camera selection*. Retrieved from https://www.nist.gov/publications/iris-cameras-standards-relevant-camera-selection-2018

[176] NIST. (n.d.). *About us: Organization and scientific area committees for forensic science*. Retrieved from https://www.nist.gov/organization-scientific-area-committees-forensic-science/about-us

[177] NIST. (n.d.). *OSAC organizational structure*. Retrieved from https://www.nist.gov/organization-scientific-area-committees-forensic-science/osac-organizational-structure

[178] Scientific Working Group on DNA Analysis Methods. (n.d.). *Guidelines for forensic DNA testing laboratories*. Retrieved from https://www.swgdam.org/. The guidelines are publicly available online.

[179] Scientific Working Group on DNA Analysis Methods. (n.d.). *Quality assurance standards for DNA testing laboratories*. Retrieved from https://www.swgdam.org/_files/ugd/4344b0_d73afdd0007c4ed6a0e7e2ffbd6c4eb8.pdf

[180] DNA Identification Act of 1994, Public Law No. 103-322, 34 U.S.C. § 12591 et seq. (1994).

[181] Scientific Working Group on DNA Analysis Methods. (2020). *Quality assurance standards (QAS) for forensic DNA testing laboratories*. Retrieved from https://www.swgdam.org/_files/ugd/4344b0_d73afdd0007c4ed6a0e7e2ffbd6c4eb8.pdf (last access date February 23, 2024).

[182] FBI. (2023). *National DNA Index System (NDIS) operational procedures manual*. Retrieved from https://le.fbi.gov/file-repository/ndis-operational-procedures-manual-version-12-070123.pdf/view (last access date February 23, 2024).

[183] 34 U.S.C. § 12592(b)(2)(A)(ii).

[184] Scientific Working Group on DNA Analysis Methods. (n.d.). *Quality assurance standards for DNA databasing laboratories*. Retrieved from https://www.swgdam.org/_files/ugd/4344b0_c9a1e24a86514f1eaffb9e35e4d04ea5.pdf

[185] Bright, J. A., Taylor, D., McGovern, C. E., Cooper, S., Russell, L., Abarno, D., et al. (2016). Developmental validation of STRmix, expert software for the interpretation of forensic DNA profiles. *Forensic Science International: Genetics, 23,* 226–239. https://doi.org/10.1016/j.fsigen.2016.07.005

[186] Perlin, M. W., Legler, M. M., Spencer, C. E., Smith, J. L., Allan, W. P., Belrose, J. I., et al. (2011). Validating TrueAllele DNA mixture interpretation. *Journal of Forensic Sciences, 56*(6), 1430–1447. https://doi.org/10.1111/j.1556-4029.2011.01777.x

[187] Scientific Working Group on DNA Analysis Methods. (n.d.). *SWGDAM publications and resources*. Retrieved from https://www.swgdam.org/. SWGDAM serves as a forum to discuss, share, and evaluate forensic biology methods, protocols, training, and research to enhance forensic biology services as well as provide recommendations to the FBI Director on quality assurance standards for forensic DNA analysis. SWGDAM is currently composed of scientists from federal, state, and local forensic DNA laboratories in the United States and Canada. All SWGDAM publications, including those addressing probabilistic genotyping validation and STR interpretation.

[188] Organization of Scientific Area Committees. (n.d.). *Mission and objectives*. Retrieved from https://www.nist.gov/organization-scientific-area-committees-forensic-science/osac-registry. OSAC's mission is to strengthen the nation's use of forensic science by facilitating the development of technically sound standards, expanding the OSAC Registry with standards that have completed a technical assessment, and promoting the implementation of those standards by OSAC's stakeholders and the forensic science community.

[189] Scientific Working Group on DNA Analysis Methods. (n.d.). *SWGDAM publications and resources*. Retrieved from https://www.swgdam.org/ SWGDAM as discussed in prior footnote in this section. Voluntary consensus OSAC standards, guidelines, and other documents.

[190] American National Standards Institute & Academy of Forensic Sciences. (2020). *ANSI/ASB Standard 018: Standard for validation of probabilistic genotyping systems*. Retrieved from https://www.aafs.org/sites/default/files/media/documents/018_Std_e1.pdf

[191] Coble, M. D., Buckleton, J., Butler, J. M., Egeland, T., Fimmers, R., Gill, P., Gusmao, L., Guttman, B., Krawczak, M., Morling, N., Parson, W., Pinto, N., Schneider, P. M., Sherry, S. T., Willuweit, S., & Prinz, M. (2016). DNA Commission of the International Society for Forensic Genetics: Recommendations on the validation of software programs performing biostatistical calculations for forensic genetics applications. *Forensic Science International: Genetics, 25,* 191–197. https://doi.org/10.1016/j.fsigen.2016.07.007

[192] European Network of Forensic Science Institutes. (2017). *Best practice manual for the internal validation of probabilistic software to undertake DNA mixture interpretation*.

[193] Forensic Science Regulator. (2020). *Guidance: Software validation for DNA mixture interpretation (FSR-G-223 Issue 2)*.

[194] Moretti, T. R., Just, R. S., Kehl, S. C., Willis, L. E., Buckleton, J. S., Bright, J. A., Taylor, D. A., & Onorato, A. J. (2017). Internal validation of STRmix for the interpretation of single source and mixed DNA profiles. *Forensic Science International: Genetics, 29,* 126–144. https://doi.org/10.1016/j.fsigen.2017.01.007

[195] Bright, J. A., Taylor, D., McGovern, C. E., Cooper, S., Russell, L., Abarno, D., et al. (2016). Developmental validation of STRmix, expert software for the interpretation of forensic DNA profiles. *Forensic Science International: Genetics, 23,* 226–239. https://doi.org/10.1016/j.fsigen.2016.03.008

[196] International Organization for Standardization. (2017). *General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025)*. Retrieved April 2024, from https://pecb.com/whitepaper/isoiec-170252017---general-requirements-for-the-competence-of-testing-and-calibration-laboratories

[197] ANSI National Accreditation Board. (n.d.). *Forensic science testing and calibration laboratories – Accreditation 7351 ANAB ISO/IEC 17025*. Retrieved April 2024, from https://anab.ansi.org/resource/iso-iec-17025-forensic-documents-resources/

[198] U.S. Department of Justice. (2018). *Uniform language for testimony and reports*. Retrieved from https://www.justice.gov/olp/uniform-language-testimony-and-reports

[199]U.S. Department of Justice. (n.d.). *Autosomal DNA examinations using probabilistic genotyping systems: Uniform language for testimony and reports*. Retrieved April 3, 2024, from https://www.justice.gov/olp/page/file/1095961/dl?inline

[200] U.S. Department of Justice. (n.d.). Forensic science. Retrieved from https://www.justice.gov/olp/forensic-science#posting

[201] Federal Bureau of Investigation. (n.d.). *DNA*. Retrieved from https://fbilabqsd.fbi.gov/file-repository/dna

[202] Federal Bureau of Investigation. (2022). *National DNA Index System (NDIS) operational procedures manual (version 11)*. Retrieved from https://le.fbi.gov/file-repository/ndis-operational-procedures-manual-version-11-070122.pdf

[203] Biometrics Subcommittee. (n.d.). Retrieved March 1, 2024, from https://www.biometrics.ninja/subcommittee

[204] National Science and Technology Council, Committee on Technology & Committee on Homeland and National Security, Subcommittee on Biometrics. (2006). *Privacy & biometrics: Building a conceptual foundation* (p. 3).

[205] National Science and Technology Council, Committee on Technology & Committee on Homeland and National Security, Subcommittee on Biometrics. (2006, September 15). *Privacy & biometrics: Building a conceptual foundation*.

[206] National Science and Technology Council, Committee on Technology & Committee on Homeland and National Security, Subcommittee on Biometrics. (2006). *Privacy & biometrics: Building a conceptual foundation* (p. 3).

[207] NSTC Subcommittee on Biometrics and Identity Management. (2009). *Supplemental information in support of the NSTC policy for enabling the development, adoption and use of biometric standards*. Retrieved from https://www.nist.gov/system/files/documents/2021/11/18/nstc_supplementaldocument08-10-09_biometricregistry.pdf (accessed March 1, 2024).

[208] Biometrics Ninja. (n.d.). *Standards*. Retrieved March 1, 2024, from https://www.biometrics.ninja/standards

[209] Biometrics Ninja. (n.d.). *Standards*. Retrieved March 1, 2024, from https://www.biometrics.ninja/standards

[210] National Science and Technology Council. (2014). *Registry of USG recommended biometric standards (Version 5.0)*. Retrieved from https://web.archive.org/web/20161222000844/http://www.biometrics.gov/Standards/Registry_v5_2014_08_01.pdf (accessed March 1, 2024).

[211] Federal Bureau of Investigation Criminal Justice Information Services Division. (2013). *Memorandum of understanding between the Federal Bureau of Investigation Criminal Justice Information Services Division and the North Dakota Attorney General Bureau of Criminal Investigation concerning the search of probe photos against the North Dakota Attorney General Bureau of Criminal Investigation photo repository* [signed May 21, 2013]. https://oversight.house.gov/wp-content/uploads/2017/03/North-Dakota-MOU.pdf; *Memorandum of understanding between the Federal Bureau of Investigation Criminal Justice Information Services Division and the South Carolina Law Enforcement Division, concerning the search of probe photos against the South Carolina Department of Motor Vehicles facial recognition database and criminal (mug shots and probation photos) facial recognition database* [signed April 8, 2013]. https://oversight.house.gov/wp-content/uploads/2017/03/South-Carolina-MOU.pdf

[212] Arizona Department of Public Safety. (2020). *Project investment justification: Arizona biometric information system (PS20003)*. Arizona Strategic Enterprise Technology. https://aset.az.gov/sites/default/files/2022-06/PS20003%20PIJ%20Final%20061522.pdf

[213] Arkansas Department of Finance and Administration. (2019). *Budget manual 2019*. State Police. https://oversight.house.gov/wp-content/uploads/2017/03/Arkansas-MOU.pdf

[214] Delaware Code Online. (n.d.). *Title 11 Crimes and criminal procedure: Law-enforcement administration chapter 86, Delaware criminal justice information system § 8601-8611*. https://delcode.delaware.gov/title11/c086/index.html

[215] Indiana Intelligence Fusion Center. (2019, June 1). *Face recognition policy*. https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf

[216] Michigan State Police. (n.d.). *Statewide network of agency photos (SNAP) acceptable use policy*. https://www.michigan.gov/msp/divisions/bid/dais/statewide-network-of-agency-photos-snap/snap-acceptable-use-policy; Michigan State Police Biometrics & Identification Division. (2022, June). *Facial recognition FAQs*. Michigan State Police Biometrics and Identification Division – Facial Recognition – Frequently Asked Questions. https://www.michigan.gov/msp/divisions/bid/dais/facial-recognition-faqs; List of Michigan police agencies with desktop FRT access as of 1/2022. https://www.documentcloud.org/documents/21217860-agencies-with-desktop-fr-1-19-22

[217] Department of Public Safety Records & Technology Division Records Bureau. (2012, September 19). *NCJIS advisory committee meeting*. https://rccd.nv.gov/uploadedFiles/gsd.nv.gov/content/Resources/AdvisoryCommittee/2013(1)/Exhibit%20A%2015%20June%2015.pdf

[218] U.S. Department of Justice, Office of Justice Programs. (2010, August). *Florida facial recognition system unmasks identity, boosts arrests* (NCJ Number 230005). https://www.ojp.gov/ncjrs/virtual-library/abstracts/florida-facial-recognition-system-unmasks-identity-boosts-arrests; The Perpetual Line-Up. *Florida & Pinellas County Sheriff's Office*. https://www.perpetuallineup.org/jurisdiction/florida; Orlando Police Department. (n.d.). *Policy and procedure 1147.2: Facial recognition*. https://www.orlando.gov/files/sharedassets/public/v/4/documents/opd/policies-and-procedures/police-operations/1147.2-facial-recognition.pdf; Pinellas County. (2022, June 28). *Example of FACES MOU with Winter Springs, FL*. https://weblink.winterspringsfl.org/WebLink/DocView.aspx?id=1483548&dbid=0&repo=WinterSprings&cr=1

[219] New York State Senate. (2021, January). *Assembly Bill A768: Relates to the use of facial recognition and biometric information for determining probable cause*. https://www.nysenate.gov/legislation/bills/2021/A768;

New York State Municipal Training Council. (2019, December 4). *Facial recognition model policy*. New York State Division of Criminal Justice Services. This policy provides guidance to law enforcement agencies in developing written policies and procedures regarding the use of facial recognition technology, emphasizing the importance of civil rights protections and stating that results obtained using facial recognition software are merely a lead and do not constitute probable cause to arrest. *Facial Recognition Model Policy*, Municipal Policy Training Council, New York State Division of Criminal Justice Services (Dec. 4, 2019)

[220] North Dakota Legislative Assembly. (n.d.). *North Dakota Century Code Chapter 12-60: Bureau of Criminal Investigation*. This chapter defines biometric data to include facial recognition technology (FRT) and states that the bureau may establish and maintain an automated biometric data identification system for the state and cooperate with other states for a regional system. https://www.ndlegis.gov/cencode/t12c60.pdf; North Dakota. (2013, May 21). *FBI Memorandum of Understanding*. https://oversight.house.gov/wp-content/uploads/2017/03/North-Dakota-MOU.pdf

[221] South Carolina. (2013, April 4). *FBI Memorandum of Understanding for use of DMV & criminal face database*. https://oversight.house.gov/wp-content/uploads/2017/03/South-Carolina-MOU.pdf; FEMA. (n.d.). *Lessons learned information sharing: SCIIC FRT database*. This document describes the South Carolina Information and Intelligence Center's Facial Recognition Database, which is partnered with the SC DMV to assist state and local law enforcement agencies in investigating identity fraud and other types of criminal activity using its FRT system, funded in part by a DHS grant. https://www.hsdl.org

[222] Tennessee Department of Finance and Administration, Division of Tech Solutions. (2019*). Face recognition: Enhancing data quality and security – A Tennessee FRT system project (September 2018 – June 2019).* This project states that the in-house development of a face recognition system will allow for quick adaptation of the technology to various needs, including driver's licenses, fraud detection, identity verification, and real-time critical infrastructure protection. https://www.nascio.org/wp-content/uploads/2020/09/NASCIO-Submission-7-TN-Facial-Recog-Final.pdf; *Nashville is utilizing face recognition technology. (2021, February 23). Analysis: Nashville should ban facial recognition technology.* Tennessee Lookout. https://tennesseelookout.com/2021/02/23/analysis-nashville-should-ban-facial-recognition-technology/; ACLU of Tennessee. (n.d.). *Police surveillance in Knoxville, Tennessee.* https://www.aclu-tn.org/en/news/police-surveillance-knoxville-tennessee

[223] Turner Lee, N., & Chin-Rothmann, C. (2022, April 12). *Police surveillance and facial recognition: Why data privacy is imperative for communities of color*. Brookings Institution. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

[224] Alabama Senate. (2022, April 6). *Senate Bill 56: Facial recognition technology, use of match as the sole basis of probable cause or arrest, prohibited*. This bill allows law enforcement to use facial recognition technology but prohibits its use as the sole basis for probable cause or arrest. It mandates data limits, privacy protections, training, and audits. https://legiscan.com/AL/text/SB56/2022

[225] Colorado Senate. (2022, June 8). *Senate Bill 22-113: Task force for the consideration of facial recognition services—creation, membership, duties, compensation, staff support, repeal*. This bill applies to all government workers and concerns the use of personal identifying data. It creates a task force for the consideration of facial recognition services, restricts their use by state and local government agencies, temporarily prohibits public schools from executing new contracts for such services, and includes provisions for pre-approval, system testing, trained facial examiners, and prohibits surveillance. SB113.

[226] Illinois General Assembly. (2021). *Public Act 102-0354*. This act amended the Illinois Identification Card Act and the Illinois Vehicle Code, prohibiting the Secretary of State from using facial recognition search services or photographs obtained during the issuance of identification cards or driver's licenses for the purpose of enforcing federal immigration laws, while allowing facial recognition for other law enforcement activities. https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=102-0354; Illinois General Assembly. (n.d.). *Bill status for SB 225*. https://www.ilga.gov/legislation/BillStatus.asp?DocNum=225&GAID=16&DocTypeID=SB&SessionID=110&GA=102; Illinois General Assembly. (n.d.). *HB 3902: Freedom from Drone Surveillance Act*. This bill addresses the ban on the use of facial recognition-enabled drones. https://ilga.gov/legislation/fulltext.asp?DocName=&SessionId=112&GA=103&DocTypeId=HB&DocNum=3902&GAID=17&LegID=149171&SpecSess=&Session=

[227] General Assembly of the Commonwealth of Kentucky. (n.d.). *A new section of KRS Chapter 61 pertaining to facial recognition technology* (July 22). This section permits the use of facial recognition technology under a model use policy, stipulating that it cannot be the sole basis for probable cause, is not permitted for constitutionally protected activities, requires a human examiner, includes data retention measures, mandates training, and must meet minimum accuracy standards using NIST guidelines. https://apps.legislature.ky.gov/recorddocuments/bill/22RS/sb176/orig_bill.pdf

[228] Maine Legislature. (2021). *Maine Title 25: Internal Security and Public Safety, Part 14 Surveillance, Chapter 701: Facial Surveillance*. This law is among the most restrictive, allowing use only when there is probable cause in serious crime investigations, and limits searches to Maine's DMV facial database. Other permissible uses include identifying missing, endangered, or deceased persons. https://legislature.maine.gov/statutes/25/title25sec6001.html; Portland City Council. (n.d.). *Portland City Code 17-131: Ban on facial recognition technology*. This code prohibits the use of facial recognition technology outright.

[229] 193rd General Court of the Commonwealth of Massachusetts. (2021, July 1). *Section 220: Facial recognition searches; requests; valid purposes; documentation; reporting; exceptions*. This law permits the use of facial recognition technology only with a court order in criminal cases, specifically to mitigate substantial risks of harm, to identify deceased persons, or during investigations into DMV fraud. https://malegislature.gov/Laws/GeneralLaws/PartI/TitleII/Chapter6/Section220

[230] New Hampshire Revised Statutes. (n.d.). *N.H. Rev. Stat. § 105-D:2: Use of body worn cameras* (effective January 1, 2017). This statute outlines the regulations surrounding the use of body worn cameras by law enforcement. https://casetext.com/statute/new-hampshire-revised-statutes/title-7-sheriffs-constables-and-police-officers/chapter-105-d-body-worn-cameras/section-105-d2-use-of-body-worn-cameras

[231] Utah State Legislature. (2021, March 16). *S.B. 34: Governmental use of facial recognition technology*. This bill prohibits law enforcement access to the Department of Motor Vehicles' facial recognition database, while allowing its use for felony investigations, violent crimes, at-risk persons, or photo lineups. Utah Code 77-23e-101.

[232] Vermont General Assembly. (2020). *S. 124: Initial complete moratorium on facial recognition technologies, including image analysis regarding "sentiment"*. This act established a moratorium on the use of facial recognition technologies. https://legislature.vermont.gov/Documents/2020/Docs/ACTS/ACT166/ACT166%20As%20Enacted.pdf; Vermont General Assembly. (2022). *H. 195: Public safety, use of facial recognition*. This law amends the previous moratorium to allow facial recognition technologies in cases involving the sexual exploitation of children. https://legislature.vermont.gov/Documents/2022/Docs/BILLS/H-0195/H-0195%20As%20Passed%20by%20Both%20House%20and%20Senate%20Official.pdf

[233] Code of Virginia. (n.d.). *§ 15.2-1723.2: Facial recognition technology; authorized uses* (effective until July 1, 2026). This statute allows law enforcement use of facial recognition technology as long as the "State Police Model FRT Policy" is in place and the algorithm is NIST-evaluated at an accuracy of 98% or above. The technology shall not be used for surveillance or to establish probable cause, but may serve as exculpatory evidence. https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0537; Virginia Code. (n.d.). *§ 52-4.5: Facial recognition technology; authorized uses; Department to establish a State Police Model Facial Recognition Technology Policy; penalty* (effective until July 1, 2026). https://virginia.gov

[234] Washington State Legislature. (2020). *Chapter 43.386 RCW: Facial recognition*. This chapter restricts the use of facial recognition technology for surveillance, real-time identification, or persistent tracking unless a warrant or court order is obtained, or exigent circumstances exist. Additionally, facial recognition services cannot be used as the sole basis for establishing probable cause. https://app.leg.wa.gov/RCW/default.aspx?cite=43.386&full=true#43.386.080

[235] Metropolitan Police Department of the District of Columbia. (n.d.). *CCTV – Systems operations and capabilities*. This document states that the CCTV system does not utilize facial recognition or any other biometric technology, and that both DC regulations and internal MPDC policy prohibit arbitrary monitoring of individuals based on race, gender, or other factors. https://mpdc.dc.gov/page/cctv-system-operations-and-capabilities

[236] California Legislative Information. (2019). *Assembly Bill No. 1215: Law enforcement: facial recognition and other biometric surveillance* (Chapter 579, October 8). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215

[237] Croft, T. (2022, December 14). *Cobb County, Ga., approves facial recognition for police*. GovTech. This article discusses the Cobb Board of Commissioners' approval of a contract with Clearview AI to enable the police department to use facial recognition technology as a crime-fighting tool. https://www.govtech.com/public-safety/cobb-county-ga-approves-facial-recognition-for-police

[238] New Orleans Code of Ordinances. (2020). *§ 147-2: Prohibited surveillance technology*. This ordinance originally banned certain surveillance technologies but was amended in 2022 to allow facial recognition for 18 specific crimes while maintaining the prohibition on its use for surveillance and as probable cause. System audits are still required. https://library.municode.com/la/new_orleans/codes/code_of_ordinances?nodeId=PTIICO_CH147SUTEDAPR_S147-2PRSUTE

[239] New York State Division of Criminal Justice Services. (2019, December 4). *Facial recognition model policy*. Municipal Policy Training Council. This document provides guidelines for the use of facial recognition technology by law enforcement agencies. https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf

[240] Stannard, M. (2023, January 13). *Hartford City Council measure would limit use of facial recognition technology by police: Here's why there are concerns about its accuracy*. Hartford Courant. This article discusses a measure proposed by the Hartford City Council to restrict the use of facial recognition technology by police due to concerns about accuracy. https://www.courant.com/2023/01/13/hartford-city-council-measure-would-limit-use-of-facial-recognition-technology-by-police-heres-why-there-are-concerns-about-its-accuracy/

[241] Hawaii State Legislature. (2021). *S.B. 156/HB 1226: Relating to violation of privacy; facial recognition systems; government officials*. This bill addresses the use of facial recognition systems by government officials in relation to privacy violations.

[242] Legislature of the State of Idaho. (2020). *House Bill 492: An act relating to facial recognition technology*. This bill outlines regulations regarding the use of facial recognition technology. https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2020/legislation/H0492.pdf

[243] Iowa Legislature. (2021, January 12). *Iowa's face recognition restriction: Bill would limit the use of facial recognition with body-worn cameras*. This proposed bill aimed to prohibit the coupling of facial recognition technology with body-worn cameras while requiring their use for certain peace officers, including tribal law

enforcement officers. For bill content and status, see Iowa Legislature bill status. https://www.legis.iowa.gov/legislation/BillBook?ba=HF%2043&ga=89

[244] LegiScan. (2021). *Kansas Senate Bill 198: Amending Kansas open records act provisions regarding access to certain law enforcement audio and video recordings and enacting the police and citizen protection act regarding the use of body cameras by law enforcement officers*. https://legiscan.com/KS/text/SB198/2021

[245] LegiScan. (2021, April 12). *Louisiana House Bill 611: Prohibits the use of facial recognition data under certain circumstances*. This bill aimed to ban law enforcement from using facial recognition technologies in most instances without a court order. https://legiscan.com/LA/research/HB611/2022

[246] Minnesota Legislature, Office of Revisor of Statutes. (2021, February 8). *HF 465: Facial Recognition Technology Warrant Act of 2021*. This bill would have required Minnesota law enforcement to obtain a court order to use facial recognition technologies. https://www.revisor.mn.gov/bills/text.php?number=HF465&version=0&session=ls92&session_year=2021&session_number=0

[247] Legislature of Nebraska. (2020, January 21). *Bill 1091: Face Surveillance Privacy Act*. This bill aimed to ban the use of facial recognition technologies for all government personnel. https://nebraskalegislature.gov/FloorDocs/106/PDF/Intro/LB1091.pdf

[248] Tennessee General Assembly. (2022, February 1). *SB 2286/HB 2834: An act to amend Tennessee Code Annotated, Title 38; Title 39 and Title 40, relative to face recognition*. This bill would have prohibited state or local law enforcement agencies from obtaining, retaining, accessing, or using any facial recognition system or related information, and created a private right of action for individuals unlawfully subjected to facial recognition technology. https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB2286&ga=112; Tennessee Department of Finance and Administration, Division of Tech Solutions. (2019). *Face recognition: Enhancing data quality and security – A Tennessee FRT system project (September 2018 - June 2019)*. This report discusses the in-house development of a facial recognition system with potential applications in areas such as identity verification and fraud detection. https://www.nascio.org/wp-content/uploads/2020/09/NASCIO-Submission-7-TN-Facial-Recog-Final.pdf; Tennessee Lookout. (2021, February 23). *Analysis: Nashville should ban facial recognition technology*. This article addresses the discussion surrounding the use of facial recognition technology in Nashville. https://tennesseelookout.com/2021/02/23/analysis-nashville-should-ban-facial-recognition-technology/; American Civil Liberties Union of Tennessee. (n.d.). *Police surveillance in Knoxville, Tennessee*. This resource explores the use of facial recognition technology by law enforcement in Knoxville. https://www.aclu-tn.org/en/news/police-surveillance-knoxville-tennessee

[249] Ohio Attorney General. (2020, January 26). *Facial recognition task force: Report and recommendations*. This report outlines the findings and recommendations of the task force regarding the use of facial recognition technology in Ohio. https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/AG-Facial-Recognition-Task-Force-Report-FINAL.aspx

[250] Ohio Attorney General. (n.d.). *Facial recognition task force*. Retrieved from https://www.ohioattorneygeneral.gov/Files/Briefing-Room/News-Releases/AG-Facial-Recognition-Task-Force-Report-FINAL.aspx

[251] Pelzer, J. (2023, April 26). Ohio resumes facial-recognition searches using controversial photo-collection firm Clearview AI. *Cleveland.com*. The article discusses the lack of comprehensive regulations on facial recognition technology, noting that federal laws are mostly silent and states like Wisconsin have not established clear parameters for its use. https://www.cleveland.com/news/2023/04/ohio-resumes-facial-recognition-searches-using-controversial-photo-collection-firm-clearview-ai.html

[252] Slaight, J., & LeCloux, R. (2020, March). *Facial recognition technology: Balancing safety and privacy*. Wisconsin Legislative Reference Bureau. This report explores the implications of facial recognition technology on safety and privacy. https://docs.legis.wisconsin.gov/misc/lrb/wisconsin_policy_project/facial_recognition_privacy_3_4.pdf

[253] Delaware Code Online. (n.d.). *Title 11: Crimes and criminal procedure, law-enforcement administration, Chapter 86: Delaware criminal justice information system, § 8601-8611*. This code outlines the provisions related to the Delaware Criminal Justice Information System. https://delcode.delaware.gov/title11/c086/index.html

[254] North Dakota Century Code. (2015). *§ 12-60-07.1: Automated biometric data identification system*. This section allows the bureau to establish and maintain an automated biometric data identification system and cooperate with other states for regional operations. https://casetext.com/statute/north-dakota-century-code/title-12-corrections-parole-and-probation/chapter-12-60-bureau-of-criminal-investigation/section-12-60-071-automated-biometric-data-identification-system

[255] Indiana Intelligence Fusion Center. (2021). *Face recognition policy*. This document outlines the face recognition policy for all operations, covering governance, oversight, use, sharing, data quality, security, retention and destruction, disclosure, and accountability.
https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf

[256] Michigan State Police. (n.d.). *Statewide Network of Agency Photos (SNAP) acceptable use policy*.
https://www.michigan.gov/msp/divisions/bid/dais/statewide-network-of-agency-photos-snap/snap-acceptable-use-policy

[257]West Virginia Intelligence/Fusion Center. (2011, February 25). *Privacy policy*.
https://fusioncenter.wv.gov/Documents/West%20Virginia%20WVIFC%202-25-2011.pdf

[258] Albuquerque Police Department. (2022, December 28). *SOP 2-110: Facial recognition system*.
https://www.cabq.gov/police/documents/2-110-facial-recognition-p-p-draft-12-28-22.pdf. Albuquerque Police Department SOP 2-110, *Facial Recognition System* (12/28/2022) "It is the policy of the Albuquerque Police Department's Investigation Bureau units to use facial recognition software when investigating criminal activity or identifying a person who may be in danger. Furthermore, when the facial recognition software identifies an individual, that information will only be treated as an investigative lead, and further investigation will need to be done to verify an individual's identity."

[259] New York State Division of Criminal Justice Services. (2019, December). *Facial recognition model policy*. Municipal Police Training Council.
https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf

"I. Purpose. The purpose of this policy is to provide guidance to law enforcement agencies in developing written policies and procedures regarding the use of facial recognition technology. The policy promotes public safety and efficiency of law enforcement criminal investigatory activities through the use of facial recognition technologies and protocols, while ensuring the appropriate safeguards are in place to protect the privacy, civil rights and civil liberties of individuals. This policy is intended to allow for the individual needs of police agencies in New York State regardless of size or resource limitations. Law enforcement agencies are encouraged to customize these protocols to meet their agency's needs, while being mindful of the intent of the policy.

II Policy. Facial recognition technology can be used to enhance public safety by assisting law enforcement with identification of unknown subjects. The technology should be used in a manner that protects the civil rights and civil liberties of citizens, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments of the United States Constitution. Results obtained utilizing the facial recognition software are merely a lead and are not probable cause to arrest. A further investigation is needed to develop probable cause to arrest."
https://www.criminaljustice.ny.gov/crimnet/ojsa/standards/MPTC%20Model%20Policy-Facial%20Recognition%20December%202019.pdf

[260] Major Cities Chiefs Association. (2021). *Facial recognition technology in modern policing: Recommendations and considerations*. https://majorcitieschiefs.com/wp-content/uploads/2021/10/MCCA-FRT-in-Modern-Policing-Final.pdf "The widely varying size and scope of MCCA member agencies necessarily requires the key recommendations in this document to be broad in their scope and applicability. Much effort was given to making both the content as a whole and the recommendations below as relevant as possible to all agencies. In general terms, it is the view of the FRT working group that each of the following key recommendations be implemented with the launch of a new FRT program. However, these recommendations are not provided as bright-line requirements for the implementation of FRT at the reader's agency, rather they are meant to serve as important guideposts in any agency's development of a responsible FRT program.

Transparency
• Law enforcement agencies seeking to procure FRT platforms should engage both public and government stakeholders for the purposes of feedback and transparency.
• The documented results of an FRT investigation should be made subject to discovery in the criminal process.
• The eventual outcome of any criminal investigation that utilizes FRT should be captured as part of the agency's data collection process.
Accountability
• Access to an agency's FRT platform should be limited to those members having specialized training in facial identification methods and the application of the technology should be performed by individuals who are not directly involved with a particular investigation.
• Restricting access to an agency's FRT platform to only those members with specialized training in facial identification methods will reduce contextual bias in particular investigations.
• If possible, the application of FRT should be performed by trained individuals who are not directly involved with a particular investigation.
• The identification of a potential lead during an FRT investigation should be documented on a standardized form which requires sufficient detail about the morphological basis of the facial identification process.
• For those agencies wishing to implement the use of FRT, but who are unsure on how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended.
Responsibility
• Careful consideration should be given to the specific and most privacy-conscious approach to what gallery image library is used.
• Agencies should identify an FRT program manager who will be tasked with both the initial deployment and continued oversight and development of the FRT program.
• The results of FRT investigations should be handled as tips/leads only due to the limitations of FRT and the potential consequences of its misuse as outlined in this document.
• FRT examiner training should specifically include familiarization with standardized methods for performing facial identification.
• The initial findings of an FRT investigation should be confirmed by a secondary examiner."

[261] IJIS Institute & International Association of Chiefs of Police. (2019). *Law enforcement facial recognition use case catalog*. https://www.theiacp.org/resources/document/law-enforcement-facial-recognition-use-case-catalog "This Law Enforcement Facial Recognition Use Case Catalog is a joint effort by a Task Force comprised of IJIS Institute and International Association of Chiefs of Police. The document includes a brief description of how facial recognition works, followed by a short explanation of typical system use parameters. The main body of the catalog contains descriptions and examples of known law enforcement facial recognition use cases. A conclusion section completes this catalog, including four recommended actions for law enforcement leaders.

[262] Arkansas State Police. (2017). *Appropriations 345 – AFIS operations maintenance & equipment*. Request to upgrade fingerprint system with Face Detective/Face Expert System. https://www.dfa.arkansas.gov/images/uploads/budgetManuals/0960_state_police2017.pdf

[263] Homeland Security Digital Library. (2009). *Good story: The South Carolina Information and Intelligence Center's facial recognition database: Lessons learned in information sharing*. FEMA.

https://www.hsdl.org/c/abstract/?docid=778945 "The South Carolina Information and Intelligence Center (SCIIC) partnered with the South Carolina Department of Motor Vehicles (DMV) to develop a facial recognition database. The SCIIC uses the database to assist state and local law enforcement agencies in investigating identity fraud and other types of criminal activity." https://www.hsdl.org/c/abstract/?docid=778945

[264] West Virginia Intelligence Fusion Center. (2012). *Real-time face recognition capabilities*. https://www.perpetuallineup.org/sites/default/files/2016-10/26_West%20Virginia.pdf

[265] Baltimore City Council. (2021). *Bill 21-0001, Enactment # 21-038: For the purpose of prohibiting Baltimore City government from purchasing or obtaining certain face surveillance technology*. https://baltimore.legistar.com/LegislationDetail.aspx?ID=4749282&GUID=3605654F-5629-41A1-BD96-89946A2C32FB&Options=&Search= Baltimore allowed the ordinance to expire December 31, 2022.

[266] Anchorage Assembly. (2023). *AO No. 2023-35(S-1): An ordinance of the Anchorage Assembly amending Anchorage Municipal Code Chapter 3.102, Municipal use of surveillance technologies, to ban the acquisition, use, or accessing of facial recognition technology*. https://s3.documentcloud.org/documents/23783222/facial-recognition-technology-ao-2023-35s-1.pdf Note: Only use of face recognition technologies permitted for deceased/missing persons, human trafficking, child abuse. Exceptions for use may be applied for. Not allowed even if obtained lawfully. https://s3.documentcloud.org/documents/23783222/facial-recognition-technology-ao-2023-35s-1.pdf

[267] California local laws prohibiting the use of facial recognition or surveillance technologies: Alameda (2019). *Res. 2019-7553*; Berkeley Municipal Code 2.99.030; Oakland Code of Ordinances 9.64; San Francisco Administrative Code 19B.2; Santa Cruz Municipal Code 9.85.030; Santa Clara Code of Ordinances A40; Davis Municipal Code 26.07; San Diego (2020). *San Diego police DA's office tried out a facial recognition app*. https://www.sandiegouniontribune.com/news/public-safety/story/2020-03-16/san-diego-police-das-office-tried-out-a-facial-recognition-app

[268] Cities in Massachusetts banning facial recognition: Boston (6/20) City of Boston Code 16-62; Brookline (12/19) Brookline Town By-Laws 8.39; Cambridge (1/20) Cambridge Code of Ordinances 2.128.075; Easthampton (7/23) Easthampton City Ordinances 6.22; Northampton (12/19) Northampton Code of Ordinances Ch. 290; Summerville (7/19) Somerville Code of Ordinances 9-25; Springfield (2/20) Springfield Code of Ordinances Ch. 173. Note Worcester is listed in the media having passed a ban as well, but the City's cite does not list any face recognition or biometric ordinance. Lawrence (2018) Lawrence Code of Ordinances 9.25, allows face recognition technologies for criminal investigations or exigent circumstances, for not more than 30 days for any one use.

[269] Minneapolis City Council. (2021). *Ordinance No. 2021-006, Amending Title 2, Chapter 41 of the Minneapolis Code of Ordinances relating to Administration: Information Governance*. Retrieved from https://library.municode.com/mn/minneapolis/ordinances/code_of_ordinances?nodeId=1070288

[270] Crown, K. (2020, August 20). Jackson, Mississippi, bans police use of biometric facial recognition. *Jackson Free Press*. Retrieved from https://www.jacksonfreepress.com/news/2020/aug/20/jackson-mississippi-bans-police-use-biometric-fac/

[271] Yellow Springs, Ohio. (n.d.). *607.03 Use of surveillance technology: Application for surveillance technology funding, acquisition, or use*. Retrieved from https://codelibrary.amlegal.com/codes/yellowsprings/latest/yellowsprings_oh/0-0-0-23917#JD_Chapter607

[272] Pittsburgh Code of Ordinances. (2015). *§116.15, Select surveillance technology*. Retrieved from https://library.municode.com/pa/pittsburgh/codes/code_of_ordinances?nodeId=COOR_TITONEAD_ARTIIIOR_CH116DEPUSA_S116.15SESUTE "Purpose. It is paramount that the City of Pittsburgh provides regulations for the acquisition, retention, access, or use of Facial Recognition and Predictive Policing Technologies to safeguard the right of individuals to privacy, balance the public's right to privacy with the need to promote and ensure safety and security, provide protocols for acquisition, retention, access, or use that include specific steps to mitigate potential impacts on the civil rights and liberties of any individuals, communities, or groups—including communities of color or other marginalized communities—in the City of Pittsburgh, to provide for transparency, oversight, and

accountability, and to minimize the risks posed by use of Select Surveillance Technology in the City of Pittsburgh." https://library.municode.com/pa/pittsburgh/codes/code_of_ordinances?nodeId=COOR_TITONEAD_ARTIIIOR_CH116DEPUSA_S116.15SESUTE

[273] City Council of the City of Austin. (2020). *Resolution No. 20200611-095*. Retrieved from https://services.austintexas.gov/edims/document.cfm?id=342177 "Facial Recognition: It is the stated policy of the City that neither facial recognition technology designed or used to identify members of the public, nor information obtained from such facial recognition technology, shall be used by the City for criminal investigation purposes, law enforcement, or surveillance purposes, nor shall such technology be allowed to be used by private corporations on City property—such a policy applies across City operations. If such information is obtained by the City inadvertently, or if APD determines that the gathering of such information or use of such technology is necessary due to imminent threat or danger, it must be approved by the City Manager and promptly reported to the Council and public with full details about the purpose of such use, how long information will be retained, who information is shared with, and protections for the public. Purchases of such technology must be approved by the Council. As this policy relates to the Austin Airport, the City should comply with all federal rules and requirements, but the City should minimize and eliminate discretionary use of facial recognition technology to the greatest extent possible under those rules and requirements, and update any policies, plans, or procedures to meet this intent to the greatest extent possible." https://services.austintexas.gov/edims/document.cfm?id=342177

[274] King County Council. (2021). *Ordinance File 2021-0091, Enactment # 19296*. Retrieved from https://kingcounty.legistar.com/LegislationDetail.aspx?ID=4793336&GUID=260D1D8E-6553-4583-B75B-92FB4C5886C8 An Ordinance relating to facial recognition, prohibiting the acquisition and use of facial recognition technology by County administrative offices and executive departments, including the department of public safety; and adding a new chapter in K.C.C. Title 2 (6/1/2021). https://kingcounty.legistar.com/LegislationDetail.aspx?ID=4793336&GUID=260D1D8E-6553-4583-B75B-92FB4C5886C8

[275] City of Madison. (2020). *Madison Code of Ordinances 23.64, Banning use of face surveillance technology*. Retrieved from https://library.municode.com/wi/madison/codes/code_of_ordinances?nodeId=COORMAWIVOIICH20--31_CH23OFAGPUPO_23.64BAUSFASUTE