Federal Law Enforcement Use of Facial Recognition Technology

October 27, 2020

Congressional Research Service
https://crsreports.congress.gov
R46586

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

Federal Law Enforcement Use of Facial Recognition Technology

R46586

October 27, 2020

Kristin Finklea, Coordinator
Specialist in Domestic Security

Laurie Harris
Analyst in Science and Technology Policy

Abigail F. Kolker
Analyst in Immigration Policy

Law enforcement agencies' use of facial recognition technology (FRT), while not a new practice, has received increased attention from policymakers and the public. Some of the concerns raised revolve around the accuracy of the technology, including potential race-, gender-, and age-related biases; the process of collecting, retaining, and securing images contained in various facial recognition databases; public notification of the use of facial recognition and other image-capturing technology; and policies or standards governing law enforcement agencies' use of the technology. Some of these concerns have manifested in actions such as federal, state, and city efforts to prohibit or bound law enforcement agencies' use of FRT. In addition, some companies producing facial recognition software have placed new barriers to law enforcement using their technologies.

FRT is one of several biometric technologies employed by law enforcement agencies, which also include fingerprint, palm print, DNA, and iris scans. FRT can be used by law enforcement for a variety of purposes such as generating investigative leads, identifying victims of crimes, helping sort faces in photos that are part of forensic evidence, and helping verify the identity of inmates before they are released from prison. However, the frequency and extent to which FRT is used at various phases of the criminal justice system is unknown. It is most often discussed by law enforcement officials as being used to help identify suspects.

The Federal Bureau of Investigation (FBI) is a leading federal law enforcement agency in the use of FRT. The bureau operates two programs that support the use of the technology: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting state and local law enforcement, and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, supporting FBI investigations. NGI-IPS contains criminal mugshots, and the system allows authorized law enforcement users (primarily state and local) to search the database for potential investigative leads. The FACE Services Unit supports FBI investigations by searching *probe* photos of unknown persons against faces in NGI-IPS and other federal and state facial recognition systems authorized for FBI use. A facial recognition search alone does not provide law enforcement with a positive identification; the results need to be manually reviewed and compared by an officer trained in facial comparison. Further, law enforcement agencies are prohibited from relying solely on the results of a search in NGI-IPS to take a law enforcement action (e.g., making an arrest). The FBI maintains an NGI Policy and Implementation Guide that outlines policies surrounding use of NGI-IPS. Authorized law enforcement users of NGI-IPS are required to follow these policies as well as established standards for performing facial comparison.

While FRT is generally used by law enforcement agencies to help generate potential investigative leads, it is also employed by U.S. border enforcement officials to assist with verifying travelers' identities. The Department of Homeland Security (DHS) and Customs and Border Protection (CBP) use the Traveler Verification Service (TVS). TVS compares the travelers' *live photographs* (taken, for example, by a gate agent) to a gallery of photographs and provides a *match* or *no match* result; a no match results in a manual check by an official to verify a traveler's identity.

Guidelines and recommendations regarding law enforcement use of FRT have been produced by the Facial Identification Scientific Working Group (FISWG). FISWG is one of the various scientific working groups that support the Organization of Scientific Area Committees for Forensic Science (administered by the National Institute of Standards and Technology, which facilitates standards development, including for FRT). FISWG has published a number of FRT-related documents for forensic science practitioners. For instance, they have guidelines and recommendations for establishing and conducting training on facial comparison, guides for capturing facial images that can be used in facial recognition systems, and recommended methods and techniques for using facial recognition systems.

As policymakers consider legislation and oversight on law enforcement agencies' use of FRT, they may evaluate how the accuracy of these systems is defined and assessed by law enforcement; how to support or restrict the technology's use by federal, state, and local law enforcement—and potential implications; and how to balance privacy and security concerns with supporting lawful criminal justice activities.

Contents

Appendixes

Contacts

Law enforcement agencies' use of facial recognition technology (FRT), while not a new practice, has received increased attention from policymakers and the public. In the course of carrying out their duties, federal law enforcement agencies may use FRT for a variety of purposes. For instance, the Federal Bureau of Investigation (FBI) uses the technology to aid its investigations, and the bureau provides facial recognition assistance to federal, state, local, and tribal law enforcement partners. State, local, and tribal law enforcement have also adopted facial recognition software systems to assist in various phases of investigations. In addition, border officials use facial recognition for identity verification purposes.

The use of FRT by law enforcement agencies has spurred questions on a range of topics. Some primary concerns revolve around the accuracy of the technology, including potential race-, gender-, and age-related biases; the collection, retention, and security of images contained in various facial recognition databases; public notification regarding the use of facial recognition and other image capturing technology; and policies or standards governing law enforcement agencies' use of the technology. Some of these concerns have manifested in actions such as federal, state, and city efforts to prohibit or bound law enforcement agencies' use of FRT.[1] In addition, some companies producing facial recognition software, such as Microsoft, IBM, and Amazon, have enacted new barriers to law enforcement using their technologies.[2]

This report provides an overview of federal law enforcement agencies' use of FRT, including the current status of scientific standards for its use. The report includes a discussion of how FRT may be used by law enforcement agencies with traditional policing missions as well as by those charged with securing the U.S. borders. It also discusses considerations for policymakers debating whether or how to influence federal, state, and local law enforcement agencies' use of FRT.

Conceptualizing Facial Recognition Technology

The term *facial recognition technology* can have different meanings for law enforcement agencies, policymakers, and the public, and the process of using facial recognition in a law enforcement context can involve various technologies and actors. Broadly, as technology experts have noted, "[t]here is no one standard system design for facial recognition systems. Not only do organizations build their systems differently, and for different environments, but they also use different terms to describe how their systems work."[3] The following key terms are provided to help in understanding facial recognition technologies and processes in this report.[4]

Face detection technology determines whether a digital image contains a face.

Facial classification algorithms analyze a face image to produce an estimate of age, sex, or some other property, but do not identify the individual. An example application of this would be

[1] See, for example, Dave Lee, "San Francisco is First US City to Ban Facial Recognition," *BBC*, May 15, 2019; and Dustin Gardiner, "California Blocks Police From Using Facial Recognition in Body Cameras," *San Francisco Chronicle*, October 8, 2019.

[2] See, for example, Jay Greene, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM," *The Washington Post*, June 11, 2020.

[3] Partnership on AI, *Understanding Facial Recognition Systems*, February 19, 2020, p. 3, https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf.

[4] These terms are taken or adapted from the Facial Identification Scientific Working Group (FISWG), *FISWG Glossary Version 2.0*, October 25, 2019; FISWG, *Facial Comparison Overview and Methodology Guidelines*, October 25, 2019; and National Institute of Standards and Technology (NIST), *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects (NIST IR8280)*, December 19, 2019, https://doi.org/10.6028/NIST.IR.8280. Some editorial changes have been made.

retail stores using facial classification to gather data on the gender and age ranges of people visiting a store, without identifying each shopper individually.

Facial comparison and **facial identification** are often used in the same context. They involve a human manually examining the differences and similarities between facial images, or between a live subject and facial images, for the purpose of determining if they represent the same person. Facial comparison has three broad categories: assessment, review, and examination. Facial assessment is a quick image-to-image or image-to-person comparison, typically carried out in screening or access control situations, and is the least rigorous form of facial comparison. Facial review (often used in investigative, operational, or intelligence gathering applications) and facial examination (often used in a forensic applications) are increasingly rigorous levels of image comparison and should involve verification by an additional reviewer or examiner. They may involve a formal, systematic examination of facial images.

Facial recognition broadly involves the automated searching of a facial image (a probe) against a known collection or database of photos.

Facial recognition algorithms compare identity information from facial features in two face image samples and produce a measure of similarity (sometimes called a match score) between them; this information can be used to determine whether the same person is in both images. Images that have a similarity score above a defined threshold are presented to the user. There are two ways in which facial recognition algorithms work to compare images:

- One-to-one verification algorithms compare a photo of someone claiming a specific identity with a stored image(s) of that known identity to determine if it is the same person. Uses of these algorithms can include unlocking a smartphone and verifying identities at a security checkpoint.
- One-to-many identification search algorithms compare features of a probe photo with all those in a gallery of images. The algorithms can provide either a fixed number of the most similar candidates, or all candidates with a similarity score above a preset threshold, for human review.[5] These algorithms may be used for purposes such as identifying potential suspect leads from a mugshot database.

Probe refers to the facial image or template searched against a gallery or database of photos in a facial recognition system.

Real-time facial recognition involves facial recognition algorithms that can be used while a video recording is taking place in order to determine in real time whether an individual in a video matches with a list of candidates in a database of photos.

Threshold refers to any real number against which similarity scores are compared to produce a verification decision or gallery of images.

Scientific Standards and Facial Recognition Technology

The National Institute of Standards and Technology's (NIST's) Role in Facial Recognition Technology

NIST is a non-regulatory federal agency within the Department of Commerce charged with promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. Among its key roles, NIST is the lead federal agency for metrology

[5] This process is described in more detail in the "Accuracy and Interpretation of Results" section of this report.

(the science of measurement) and facilitates standards development, two key elements in the development and deployment of FRT.[6]

NIST's work in FRT includes the following:

- **Research** to improve the accuracy, quality, usability, interoperability, and consistency of FRT identity management systems;
- **Testing and Evaluation** to provide tools and support for evaluating the effectiveness of FRT prototypes and products;
- **Technical Guidance and Support** to assist federal law enforcement and other federal government agencies in the use of FRT; and
- **Standards** to facilitate the development of scientifically valid, fit-for-purpose FRT standards and to ensure that U.S. interests are represented in international arenas.

NIST collaborates with other federal agencies, law enforcement agencies, industry, and academic partners in these and related activities. Detailed information on NIST efforts in research, testing and evaluation, technical guidance and support, and standards development related to FRT are included in the **Appendix**.

Facial Identification Scientific Working Group

NIST administers the Organization of Scientific Area Committees (OSAC) for Forensic Science, which is a collaboration of more than 550 forensic scientific practitioners and experts across government, academia, and industry.[7] The OSAC for Forensic Science works to facilitate "the development of technically sound, science-based standards through a formal standard developing organization (SDO) process."[8] It also evaluates existing standards developed by SDOs and may place them on the OSAC Registry,[9] which contains approved scientifically sound forensic science standards for specific disciplines, such as facial identification, digital evidence, or bloodstain pattern analysis. The OSAC also promotes the use of these OSAC Registry-approved standards by the forensic science community.

The OSAC for Forensic Science is supported by a number of scientific working groups, which are collaborations between forensic science laboratories and practitioners "to improve discipline practices and build consensus standards."[10] There are over 20 scientific working groups across a range of disciplines including facial identification, DNA analysis, and latent fingerprint examination. The mission of the Facial Identification Scientific Working Group (FISWG) "is to develop consensus standards, guidelines and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of the science in this field."[11]

FISWG has published a number of guidelines and recommendations for forensic science practitioners. For instance, they have guidelines and recommendations for conducting and establishing training on facial comparison, guides for capturing facial images that can be used in

[6] Facial recognition technology is a subfield of biometrics. Biometrics is the measurement and analysis of unique physical or behavioral characteristics.

[7] For more information, see https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science.

[8] Ibid.

[9] See https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/osac-registry.

[10] See https://fiswg.org/about_swgs.html.

[11] See https://fiswg.org/objectives.html.

facial recognition systems, and recommended methods and techniques for using facial recognition systems.[12]

How FRT May Be Used by Federal Law Enforcement Agencies

Law enforcement agencies' use of FRT has received attention from policymakers and the public over the past several years. There have been heightened concerns following several revelations, including that Clearview AI, a company that developed image-search technology used by law enforcement agencies around the country, had amassed a database of over 3 billion images against which probe photos could be compared.[13]

FRT is one of several biometric technologies employed by law enforcement agencies, which also include fingerprint, palm print, DNA and iris scans. FRT can be used by law enforcement for a variety of purposes such as generating investigative leads, identifying victims of crimes, facilitating the examination of forensic evidence, and helping verify the identity of individuals being released from prison.[14] Press releases and statements from the Department of Justice highlight how the technology has been used in the criminal justice system.

- FRT has been used to help generate suspect leads. In one case, FBI agents used the technology, via the Mississippi Fusion Center, to identify a potential suspect in an interstate stalking case who had allegedly been harassing high school girls through their Twitter accounts.[15] The suspect was later sentenced to 46 months imprisonment and three years of supervised release for this stalking.[16]
- FRT may also be used to help identify victims. For example, officials have noted FRT was used to help identify "an accident victim lying unconscious on the side of the road."[17]
- FRT, along with other pieces of evidence, has been used to support probable cause in affidavits in support of criminal complaints. In one case, an FBI agent cited the use of FRT in a criminal complaint against a bank robbery suspect. The agent noted that images from the bank's surveillance footage were run against facial recognition software, and a photo of the suspect was returned as a possible match. Investigators then interviewed associates of the suspect, who identified him as the man in the bank surveillance footage.[18]

[12] See https://fiswg.org/documents.html.

[13] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, February 10, 2020.

[14] Remarks by an FBI representative at the President's Commission on Law Enforcement and the Administration of Justice, April 21, 2020.

[15] U.S. Attorney's Office, Southern District of Indiana, "Mississippi Man Faces Interstate Stalking Charges for Five-Year-Long Crime Against Evansville Area High Schoolers," press release, June 28, 2018.

[16] U.S. Attorney's Office, Southern District of Indiana, "Mississippi Man Sentenced for Internet Stalking Young Evansville Women," press release, August 5, 2019.

[17] Remarks by an FBI representative at the President's Commission on Law Enforcement and the Administration of Justice, April 21, 2020.

[18] United States of America v. Terrance Maurice Goss, U.S. District Court for the Middle District of Florida, Criminal Complaint, January 18, 2019.

Notably, the frequency and extent to which FRT is used at various phases of the criminal justice system (from generating leads and helping establish probable cause for an arrest or indictment, to serving as evidence in courtrooms) is unknown.[19] It is most often discussed as being employed during investigations by law enforcement officials. Of note, FRT is generally used by law enforcement in one-to-many searches to produce a gallery of potential suspects ranked by similarity and not to provide a single affirmative match. As such, the technology currently might not be relied upon in the same way that other biometric evidence might. Rather, it is the results of an investigator's facial review between a probe face and the gallery of images produced from running a probe face through facial recognition software that might be used as evidence contributing to an arrest and prosecution.

While FRT is used by a number of federal law enforcement agencies, the next section of this report highlights the FBI's use of it, as the bureau has a leading role in federal law enforcement's employment of the technology.

FBI Use of FRT

The FBI's Criminal Justice Information Services (CJIS) Division operates two programs that support the FBI's use of FRT: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting state and local law enforcement, and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, supporting FBI investigations.

Next Generation Identification–Interstate Photo System (NGI-IPS)

NGI-IPS contains criminal mugshots that have associated 10-print fingerprints and criminal history records. This system allows authorized federal, state, local, and tribal law enforcement users to search the database for potential investigative leads. To use NGI-IPS,

> [a] law enforcement agency submits a "probe" photo that is obtained pursuant to an authorized law enforcement investigation, to be searched against the mugshot repository. The NGI-IPS returns a gallery of "candidate" photos of 2-50 individuals (the default is 20). During the second step of the process, the law enforcement agencies then manually review the candidate photos and perform further investigation to determine if any of the candidate photos are the same person as the probe photo.[20]

The FBI notes that a facial recognition search in NGI-IPS cannot alone provide a positive identification; the results need to be manually reviewed by a trained officer.[21] Further, law enforcement agencies that submit a probe photo for a search in NGI-IPS are prohibited from relying solely on the results of this search to take a formal law enforcement action (e.g., making an arrest).[22]

[19] In at least one case, in California, a judge allowed a suspect's criminal defense team to introduce evidence from biometric facial recognition technology. For more information, see "A First: Biometrics Used to Sentence Criminal," *Homeland Security Newswire*, February 1, 2011.

[20] FBI testimony before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2020.

[21] As noted elsewhere, authorized users of NGI-IPS must receive training in the use of facial recognition technology.

[22] See https://www.fbibiospecs.cjis.gov/Face.

Photos in NGI-IPS

NGI-IPS "contains over 93 million civil photos, criminal photos, and scars, marks and tattoo images. Of this number, over 38 million criminal photos are available for facial recognition searching by law enforcement agencies."[23] The photos in NGI-IPS are separated into various groups: a criminal identity group (mugshots pursuant to arrest),[24] a civil identity group (those submitted for criminal background checks for non-criminal justice purposes such as employment and security clearances), and an unsolved photo file (UPF, which contains photos of unknown subjects reasonably suspected of a felony crime against a person). The criminal identity group is automatically available for facial recognition searching. If an individual has photos associated with both the criminal and civil identity groups, all photos become associated with the criminal identity group and are available for searching. A law enforcement agency submitting a probe photo to NGI-IPS for searching can affirmatively request to search against the UPF in addition to the criminal identity group.

Facial Analysis, Comparison, and Evaluation (FACE) Services Unit

While NGI-IPS primarily supports state, local, and tribal law enforcement partners, the FACE Services Unit supports FBI investigations. Specifically, FACE Services supports FBI field offices, operational divisions, and legal attachés (and sometimes federal partners) on open investigations and, in limited circumstances, on closed cases. The FACE Services Unit searches "probe photos that have been collected pursuant to the Attorney General guidelines as part of an authorized FBI investigation, and they are not retained."[25] These probe photos are searched against faces in NGI-IPS as well as other federal and state facial recognition systems authorized for FBI use. The FACE Services Unit then, through facial review, compares the probe photo against the candidate gallery of faces produced from the search to help identify potential investigative leads.

FRT Used by Law Enforcement Agencies at the Border

While FRT is generally used by law enforcement agencies to help generate potential investigative leads, it is also employed by U.S. border enforcement officials to assist with verifying travelers' identities. The Department of Homeland Security (DHS) is developing an automated biometric entry-exit system for foreign nationals traveling into and out of the country.[26] The entry system has been implemented,[27] but the exit system has yet to be fully operationalized.[28] In developing the exit system, DHS and Customs and Border Protection (CBP) have piloted various programs using an array of biometric technologies (e.g., fingerprints, iris scans, and facial recognition) and determined that facial recognition was the optimal approach because of the speed with which it could be used and its relative accuracy. The FRT program they have implemented is the Traveler Verification Service (TVS).[29]

TVS is a public-private partnership between the federal government and private airlines, airports, and cruise lines. It is deployed by CBP and the Transportation Security Administration (TSA). TVS currently operates in 27 airports, 7 seaports, and 5 border locations across the United States, as well as 4 international preclearance locations. TVS currently captures roughly 60% of *in-scope* travelers (i.e., foreign nationals aged 14-79) departing the

[23] FBI, *Privacy Impact Assessment for the Next Generation Identification – Interstate Photo System*, October 29, 2019.

[24] The mugshots taken pursuant to arrest are not indicative of actual criminality or guilt.

[25] FBI testimony before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2020. Department of Justice policies and procedures—including guidelines for investigations—are outlined in the *Justice Manual*, available at https://www.justice.gov/jm/justice-manual.

[26] For more information, see CRS In Focus IF11634, *Biometric Entry-Exit System: Legislative History and Status*.

[27] The entry system, fully implemented in December 2006, utilizes biometrics such as fingerprints and digital photographs.

[28] There have been "various longstanding planning, infrastructure, and staffing challenges" to developing and implementing the biometric exit system, including airports' lack of secure inspection areas for outbound travelers. See U.S. Government Accountability Office (GAO), *DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain*, GAO-17-170, February 17, 2017.

[29] Additional information, including privacy documents, is available at https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

United States via commercial air carriers and 20% of in-scope arriving travelers.[30] CBP's goal is to capture 97% of all in-scope departing commercial air travelers by 2022.[31] TVS compares the travelers' *live photographs* (taken, for example, by a gate agent) to a gallery of photographs. The composition of the galleries depends on the travel context. For air and sea travelers, CBP uses biographic data obtained from flight and ship manifests via the Advance Passenger Information System[32] to gather all associated facial images from DHS holdings (e.g., photographs from U.S. passports, U.S. visas, CBP entry inspections, and any other DHS encounters). For pedestrians and vehicle travelers, the gallery consists of photographs of frequent crossers at that port of entry. TVS provides a *match* or *no match* result within two seconds.[33] In case of the latter result, the traveler's identity is checked manually by a CBP agent.

Federal Law Enforcement FRT Policy Guidance

The FBI maintains an NGI Policy and Implementation Guide that outlines policies surrounding use of NGI-IPS. Authorized law enforcement users of NGI-IPS are required to follow these policies as well as FISWG standards for performing facial comparison.[34] Policies outlined in the guide include information on how to

- submit photos for enrollment in NGI-IPS,
- conduct an investigative photo search,
- retrieve additional biometrics associated with a probable candidate generated from a search of NGI-IPS,
- notify the FBI of a potential match resulting from an investigative photo search,
- request an audit trail for a biometric set that an authorized user enrolled in NGI-IPS, and
- delete a biometric set that an authorized user enrolled in NGI-IPS.[35]

The FBI outlines technical requirements for using NGI-IPS in an Electronic Biometric Transmission Specification document that it provides to system users. In addition, it asks that users of NGI-IPS use its Mugshot Implementation Guide as a reference for submitting proper facial images to the FBI. The guide notes that image quality is affected by the camera, background, lighting, and subject posing.[36]

The FBI requires that users of NGI-IPS complete facial recognition training that meets FISWG guidelines. To facilitate this requirement, the FBI provides facial comparison and identification training, which "is designed to provide the skills and knowledge to professionals from the law enforcement and intelligence communities working in the fields of face recognition and face comparison. It also provides students with awareness and understanding of the face comparison

[30] Based on CRS discussions with CBP officials on January 30, 2020, and CRS email communication with CBP officials on August 12, 2020.

[31] Department of Homeland Security (DHS), *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies*, Report to Congress, August 30, 2019, p. 5.

[32] APIS collects biographic data such as gender, date of birth, travel document type and number, and nationality, Ibid. p. 30.

[33] U.S. Customs and Border Control, *Traveler Verification Service for Simplified Travel*, August 2018.

[34] FISWG has Guidelines and Recommendations for Facial Comparison Training to Competency, available at https://fiswg.org/FISWG_Training_Guidelines_Recommendations_v1.1_2010_11_18.pdf.

[35] FBI, *Next Generation Identification (NGI) Interstate Photo System (IPS) Policy and Implementation Guide: Version 1.3*, April 23, 2015.

[36] FBI, *Mugshot Implementation Guide: Photographic Considerations Related to Facial Recognition Software and Booking Station Mug Shots*, April 25, 2013.

discipline. This training is consistent with the guidelines and recommendations outlined by [FISWG]."[37] FISWG notes that "[t]he level of training necessary to conduct facial comparison is dependent upon the source, quality, quantity, and complexity of the images that are being analyzed and the purpose of the analysis."[38] As outlined by FISWG, basic level training for facial comparison includes, among other things, an understanding of the principles of facial comparison, including

- assessing the quality of a facial image to determine the value for examination;
- using a process of "Analysis, Comparison, Evaluation, and Verification (ACE-V)";
- understanding the methods of comparison, such as one-to-one facial examination;
- understanding the levels of conclusion;
- having the ability to render proper conclusions;
- understanding the concept and effects of cognitive bias, including confirmation bias; and
- understanding the benefits of verification by another qualified reviewer or examiner.[39]

The FBI has also conducted audits to evaluate whether users of its facial recognition systems are in compliance with the policies surrounding their use. In congressional testimony, the FBI indicated that as of May 2019, nine FBI audits of NGI-IPS revealed no findings of non-compliance and no observations of unauthorized requests or misuse of NGI-IPS; in addition, a 2018 FBI audit of the FACE Services Unit indicated that the unit is operating in accordance with FBI policies and relevant privacy laws.[40]

Policy Considerations Surrounding Federal Law Enforcement Use of FRT

Accuracy and Interpretation of Results

The accuracy of FRT has come under scrutiny, independent of law enforcement's use of the technology including an officer's review of potential matches. When considering accuracy, there are a number of possible outcomes in both one-to-many identification searches (such as those used by the FBI's NGI-IPS) and one-to-one verifications (such as those used by the CBP's TVS). Facial recognition systems may return an accurate match (i.e., a true positive result, or hit),[41] an

[37] FBI, *Biometric and Criminal History Record Training*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-and-criminal-history-record-training.

[38] FISWG, *Guide for Role-Based Training in Facial Comparison*, July 17, 2020, pp. 1-2.

[39] FISWG, *Guidelines and Recommendations for Facial Comparison Training to Competency*, November 18, 2010, pp. 1-2.

[40] Statement for the Record of Kimberly Del Greco, Federal Bureau of Investigation, before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology: Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2019.

[41] In a one-to-many identification search, this occurs when the probe face matches a face in the database and is one of the faces returned in the gallery of potential matches. In a one-to-one identity verification, this occurs when the probe face submitted matches a photo of the same individual in a database, and a match is confirmed.

accurate non-match (i.e., a true negative, or correct rejection),[42] an inaccurate match (i.e., a false positive, or false alarm),[43] or an inaccurate non-match (i.e., a false negative, or miss).[44] It is the two types of errors—inaccurate matches and inaccurate non-matches—that have been of particular interest to policymakers.

- An inaccurate match, or *false positive*, result occurs when there is an erroneous association between images from two different people, which can occur when the digitized faces of two different people are highly similar.
- An inaccurate non-match, or *false negative*, result occurs when there is a failure to match images of the same person in two different photos. This could occur due to factors such as a change in the person's appearance or discrepancies in the quality of the images. Variations in pose, illumination, and expression may contribute to false negatives.[45]

Notably, there are both technical and human factors that contribute to the overall accuracy of facial recognition searches as performed by law enforcement officers.

Matching a probe to a gallery of images or a reference image depends on the threshold set for the similarity scores generated by the facial recognition algorithm. Similarity scores indicate the similarity between the probe and reference or gallery images.[46] For example, if using a zero-to-one scale, a similarity score of one would indicate that the two images are most similar (not necessarily that the two face images belong to the same person) in that system. Further, similarity scores are system specific (i.e., a similarity score from a system developed by company A is not necessarily comparable to a similarity score from a system from company B).[47]

When trying to decide whether a probe image matches any images in a given database, setting a higher threshold will return fewer potential results and setting a lower threshold will return a greater number of potential results. Generally, the threshold is initially set by the algorithm developer. Depending on the system, the user can choose to keep or change this threshold. As with similarity scores, thresholds do not indicate accuracy of a system (i.e., adjusting a threshold to a higher value does not mean the results returned are more accurate); rather, the decision of where to set a threshold is based on how the system is being used and what the developer or user wants to optimize (e.g., reducing the chance of false positives or false negatives).[48] Notably, when considering where to set the threshold, there is also consideration of the inherent trade-off in error

[42] In a one-to-many identification search, this occurs when the probe face does not match a face in the database and a gallery of potential matches is not returned. In a one-to-one identity verification, this occurs when the probe face does not match any faces in a database, and a match is not confirmed.

[43] In a one-to-many identification search, this occurs when the probe face does not match a face in the database, but a gallery of potential matches is returned. In a one-to-one identity verification, this occurs when the probe face does not match a face in the database, but a match is confirmed.

[44] In a one-to-many identification search, this occurs when the probe face submitted matches a face in the database, but a gallery of potential matches is not returned. In a one-to-one identity verification, this occurs when the probe face matches a face in the database, but a match is not confirmed.

[45] See NIST, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects (NIST IR8280)*, December 19, 2019, https://doi.org/10.6028/NIST.IR.8280.

[46] Similarity scores are sometimes referred to as *confidence scores*, but they do not represent a degree of certainty or confidence in the matches returned to the user or the accuracy of the system.

[47] For additional explanations of match scores and thresholds, see Partnership on AI, *Understanding Facial Recognition Systems*, February 19, 2020, pp. 6-7.

[48] Ibid.

rates—one can minimize the false positive rate or the false negative rate by resetting the threshold, but not both at the same time.[49]

There is also a range of possible accurate and inaccurate outcomes when the probe face and any gallery of potential matches are subject to facial review by a human. For instance, in one-to-many searches a reviewer can correctly match the probe face to the same individual's photo returned in the gallery of potential matches, or a reviewer can correctly reject the probe face as a match to faces in the gallery if the FRT software has returned a gallery that does not contain a match. In addition, a reviewer can incorrectly identify the probe face as a match to a face in a returned gallery (in a gallery that either correctly contains or incorrectly does not contain a match); alternatively, a reviewer could fail to identify the probe face as a match when a gallery contains the correct match. In one-to-one identity verifications, such as those used to confirm a traveler's identity, there may be follow-up facial comparison by an official in the instance of a no-match returned by the technology. In this case, the comparison can result in one of the same outcomes as one-to-many searches subject to follow-up review by a human.

Effects of Errors

False positives and negatives returned by FRT have come under scrutiny because of their potential implications. In one-to-many identification searches used by law enforcement, false positives could potentially contribute to errant investigative leads and false accusations. False negatives could potentially result in loss of evidence that could support a case. In one-to-one verifications used by border officials, false positives pose potential security risks because they may not flag a traveler using an assumed identity. False negatives could result in enhanced questioning, surveillance, or disrupted travel of individuals for whom it was not necessary.[50] According to CBP internal analysis, the estimated false positive rate of TVS is .0103%.[51] (It did not report the false negative rate.) Further, in September 2020, the Government Accountability Office (GAO) reported that CBP "met or exceeded" its facial recognition accuracy requirements for its air exit system.[52]

A December 2019 NIST study of both one-to-many identification search algorithms and one-to-one verification algorithms found that FRT algorithms' accuracy rates can vary by demographic factors such as age, sex, and race.[53] For example, false positive rates tended to be higher for Asian and African American faces compared to those of Caucasians, which may be due to the data used

[49] This trade-off is demonstrated by plots that incorporate false negative and false positive identification rates with a threshold value; these plots are called detection error trade-off (DET) characteristic or receiver operating characteristic (ROC) curves. For additional information see the 2019 NIST FRVT Part 3: Demographic Effects report, p. 23; and for further discussion, see Lucas D. Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, The Center for Catastrophe Preparedness and Response, New York University, 2009, pp. 14-15.

[50] As a 2019 NIST study notes, "in a one-to-one access control, false negatives inconvenience legitimate users; false positives undermine a system owner's security goals. On the other hand, in a one-to-many deportee detection application, a false negative would present a security problem, and a false positive would flag legitimate visitors." Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Science and Technology, December 2019.

[51] DHS, *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies*, Report to Congress, August 30, 2019, p. 30. CBP does not provide the methodology for calculating the false positive rate.

[52] GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568, September 2020, p. 50.

[53] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Science and Technology, December 2019.

to train the algorithm; an explanation that the NIST study did not explore. However, NIST noted that there is wide variation among algorithms, with some producing significantly fewer errors, and errors of different types, than others.[54] Policymakers may wish to exercise oversight over the *specific* FRT algorithms employed by federal law enforcement agencies, and the data on which those systems are trained, as they evaluate the accuracy and use of facial recognition. They may also debate whether or how to provide legislative direction aimed at maximizing the accuracy of FRT algorithms used by federal law enforcement entities. In attempting to maximize accuracy, developers and users of FRT must weigh the consequences of errors (false positives and false negatives) for different communities and decide which error measure is of higher priority to minimize, depending on how the threshold is set.

NIST researchers and collaborators have also studied the facial recognition accuracy of forensic examiners, *superrecognizers*, and face recognition algorithms.[55] They found that while the "best machine performed in the range of the best-performing humans, who were professional facial examiners … optimal face identification was achieved only when humans and machines collaborated."[56] Policymakers may consider this as they evaluate the accuracy of law enforcement use of FRT—such as the FBI's NGI-IPS, which requires manual review of the gallery of faces produced by submitting a probe face to the FRT algorithm.

Potential Restrictions on Law Enforcement Use of FRT

Recent policy debates surrounding law enforcement agencies' use of FRT have included discussions about potential prohibitions, restrictions, or moratoriums on the technology's use. In these discussions, policymakers may consider issues such as the following:

How is law enforcement conceptualized in this context? As noted, law enforcement agencies with various missions—from those like the FBI's to investigate violations of federal criminal law to those like CBP's to support border enforcement—have employed FRT. Policymakers may consider whether proposals to specify whether or how law enforcement agencies may use FRT have also factored in which type of law enforcement activities might be affected.[57]

How might restrictions on the use of FRT affect emergencies or cases involving threats to national security? Policymakers debating bounds on law enforcement agencies' use of FRT may consider whether restrictions should apply equally in all circumstances. For example, while many tools and technologies used by law enforcement agencies to aid investigations have not been specifically permitted or prohibited by law, Congress has legislated on and conducted oversight of certain technologies that could affect individual privacy. With electronic surveillance, for instance, investigators must generally obtain a warrant to conduct wiretaps;[58] however, exceptions

[54] Ibid. Also, testimony by Charles H. Romine, NIST Director, before U.S. Congress, House Committee on Homeland Security, *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies: Part II*, 116th Cong., 2nd sess., February 6, 2020.

[55] P. Jonathon Phillips et al., "Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms," *Proceedings of the National Academy of Sciences, USA*, vol. 115, no. 24 (2018), pp. 6171-6176, https://doi.org/10.1073/pnas.1721355115. Researchers note that superrecognizers are "untrained people with strong skills in face recognition."

[56] Testimony by Charles H. Romine, NIST, before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology: Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2019.

[57] The Bureau of Justice Statistics' Census of Federal Law Enforcement Officers may help inform this discussion. The most recent survey provides data from 2016. Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016-Statistical Tables*, October 2019.

[58] 18 U.S.C. §2510 et seq. See also Department of Justice, *Justice Manual, Title 9, 9.7000: Electronic Surveillance.*

exist for emergency situations that may involve death or serious injury, threaten national security, or involve conspiracies of organized crime.[59]

How might policymakers influence law enforcement use of FRT at the federal level as well as state and local levels? Policymakers can legislate directly on federal law enforcement agencies' ability to utilize facial recognition and other biometric technologies, as well as specify under which circumstances federal law enforcement may use these tools. They can also direct federal departments and agencies to develop or rely on established guidelines surrounding the technologies, require them to use technology and FRT algorithms that meet specified standards, and conduct broad oversight of agencies' use of FRT.

Congress could also influence state, local, and tribal use of these technologies through the provision or withholding of grant funding. Programs such as the Edward Byrne Memorial Justice Assistance Grant (JAG) program[60] and the Community Oriented Policing Services (COPS) program[61] have been used to incentivize activities of state and local law enforcement and may be leveraged to support or restrict agencies' use of FRT. For instance, Pinellas County, FL, law enforcement has used COPS funding to develop a facial recognition system.[62]

Another way the federal government can affect state, local, and tribal policies, without the provision or withholding of grant funding, is through the transfer of knowledge and expertise—via training, research and guiding documents, and model legislation. For instance, the Bureau of Justice Assistance published a guidance document for state, local, and tribal criminal intelligence and investigative entities to aid in developing policies around the use of FRT.[63]

Privacy and Security

In a September 2019 survey by the Pew Research Center, 56% of surveyed Americans indicated that they trust law enforcement agencies to use FRT responsibly, and 59% indicated it is acceptable for law enforcement agencies to use these technologies to assess security threats in public.[64] Further, the American public generally has more trust in law enforcement agencies using FRT responsibly than it does in technology companies or advertisers. This trust, however, has some notable demographic variances. Older Americans indicated they had more trust in law enforcement using FRT responsibly than did younger Americans. Further, White respondents (61%) reported more trust in law enforcement using the technology responsibly than did Hispanic respondents (56%), who in turn reported more trust than Black respondents (43%). Nonetheless, policymakers, advocates, and the public have raised questions about how these technologies might affect privacy as well as the security of facial recognition systems' data.[65] Questions for policymakers to consider include the following:

---

[59] 18 U.S.C. §2518.

[60] For more information, see CRS In Focus IF10691, *The Edward Byrne Memorial Justice Assistance Grant (JAG) Program.*

[61] For more information, see CRS In Focus IF10922, *Community Oriented Policing Services (COPS) Program*.

[62] National Law Enforcement and Corrections Technology Center, *Florida Facial Recognition System Unmasks Identity, Boosts Arrests*, August 2010. Pinellas County, FL, law enforcement agencies had previously received, through the FY2001 appropriations, $3.5 million in funding for a demonstration grant "to demonstrate with the Florida Department of Motor Vehicles how facial recognition technology may be used by police." See H.Rept. 106-1005.

[63] Bureau of Justice Assistance, *Face Recognition Policy Development Template*, December 2017.

[64] Aaron Smith, Pew Research Center, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, September 5, 2019.

[65] The issues discussed in this section are focused on FRT as used by law enforcement to generate potential (continued...)

Is there public awareness and notification surrounding federal law enforcement use of FRT? Some have questioned whether or how individuals might know that their faces are included in databases searched by FRT for law enforcement purposes. For example, federal law enforcement agencies may rely on FRT to search against a number of databases to help identify suspects.[66] The FBI's FACE Services Unit can search probe photos against faces in NGI-IPS as well as other federal and state facial recognition systems authorized for FBI use. Some states allow FBI access to driver's license/identification photos, mugshot photos, and state department of corrections photos; some allow access to some portion or subset of those photos; and some prohibit access.[67] The FBI is required to provide information to the public on its facial recognition systems through Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).[68] Policymakers may question whether these are sufficient measures to notify the public about federal law enforcement agencies use of FRT to search against databases in which individuals' photos are held. In addition, they may conduct oversight over the timeliness with which federal law enforcement agencies publish and update relevant PIAs and SORNs.

There are also concerns about CBP's use of FRT. U.S. citizens are allowed to opt out of TVS biometric exit participation and can instead undergo manual review of travel documents. CBP notifies travelers of this alternative through its website, physical signs and verbal announcements at the ports of entry, and an FAQ sheet upon request.[69] However, a September 2020 GAO report found that "notices to inform the public of facial recognition contained limited privacy information and were not consistently available."[70] Policymakers may examine whether CBP provides U.S. citizens with adequate notice about TVS and explains its opt-out procedures clearly.[71]

How might the use of FRT affect police-community relations? In the national debate about police-community relations,[72] there have been concerns about whether race, gender, and age biases in some FRT algorithms could contribute to tensions between the police and the communities they serve. Further, in the midst of these discussions, some companies producing

investigative leads and by border enforcement for identity verification. There are other potential uses of FRT in the criminal justice system, not discussed here, such as compelling an individual to use the facial recognition feature to unlock a mobile device such as an iPhone. Of note, "at least one court has upheld compelled use of a facial recognition unlock feature." See Joey L. Blanch and Stephanie S. Christensen, "Biometric Basics: Options to Gather Data from Digital Devices Locked by a Biometric "Key"," *Emerging Issues in Federal Prosecutions*, vol. 66, no. 1 (January 2018), p. 6.

[66] The same may be true for state and local law enforcement, but this varies by jurisdiction.

[67] GAO, *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains*, GAO-2019-579T, June 4, 2019.

[68] Ibid. This requirement is not specific to the FBI. Federal agencies are subject to requirements under Section 208 of the E-Government Act of 2002 (P.L. 107-347) regarding the protection of personal information collected, maintained or disseminated using information technology. For more information, see Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22, September 26, 2003. In this guidance, a PIA is defined as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." In addition, SORN is required to be published for any newly created or revised system of records.

[69] DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS/CBP/PIA-056, November 14, 2018, p. 19.

[70] GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568, September 2020, p. 39.

[71] Letter from 23 Members of Congress to Kevin McAleenan, former Acting Secretary of Homeland Security, June 13, 2019, https://wild.house.gov/sites/wild.house.gov/files/CBP%20Facial%20Recognition%20Ltr.%20final.%20.pdf.

[72] For more information, see CRS Report R43904, *Public Trust and Law Enforcement—A Discussion for Policymakers*.

facial recognition software have decided to cease production or have enacted new barriers to law enforcement use of their technologies.[73] Some have been less concerned with potential errors produced by the technology and more apprehensive with how the technology may be *used* by law enforcement; specifically, the concern is whether law enforcement agencies' use of the technology can "strip individuals of their privacy and enable mass surveillance."[74]

Policymakers may continue to question whether federal law enforcement agencies have assessed—or have policies for ongoing assessments of—potential biases in the specific facial recognition technologies (and associated algorithms) that they use. This could include policies for ongoing assessments by NIST. Policymakers may also look into whether federal grants for state, local, and tribal law enforcement use of FRT include requirements that grantees are using facial recognition technologies that have been assessed for biases. In addition, they could continue to examine how federal law enforcement agencies, as well as state, local, and tribal recipients of federal grants, utilize the technology in their policing.

How do federal law enforcement agencies employing FRT retain and secure the data? The security of data held by federal agencies and their contractors is of ongoing interest to Congress. For instance, in June 2019, CBP revealed that images of faces and license plates were compromised in a cyberattack on one of its subcontractors that provides automated license plate recognition technology to the agency.[75] This breach reportedly exposed confidential agreements, hardware schematics, and other records related to border security.[76] Breaches like this highlight the vulnerability of data, including face image data captured and held by governmental agencies. In evaluating the security of federal law enforcement data systems, policymakers may pay particular attention to the security of facial recognition and other biometric data.

For example, the FBI's NGI-IPS contains mugshot photos against which probe photos are compared. The FBI notes that "after the facial recognition search is performed, the probe photo is not retained in the NGI-IPS. This ensures that the Criminal Identity Group of the NGI-IPS remains a repository of mugshots collected pursuant to arrest."[77] While NGI-IPS is often used by state, local, and tribal law enforcement agencies, the FACE Services Unit supports FBI investigations. The FACE Services Unit submits probe photos to NGI-IPS (which does not retain probe photos) as well as other federal, state, and local systems (which may have different policies on photo retention); when the FBI submits probe photos to entities outside the bureau, it is the other agency that is responsible for conducting the search. The FBI notes that "to accommodate certain states that have auditing and/or logging requirements that necessitate retention of probe photos and candidate galleries, the FBI constructs [memoranda of understanding] in compliance with these requirements while also requiring state maintenance of only the minimum information

[73] See, for example, Jay Greene, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM," *The Washington Post*, June 11, 2020. See also Dustin Gardiner, "California Blocks Police From Using Facial Recognition in Body Cameras," *San Francisco Chronicle*, October 8, 2019.

[74] Osonde A. Osoba and Douglas Yeung, *Bans on Facial Recognition Are Naive. Hold Law Enforcement Accountable for Its Abuse*, RAND, June 17, 2020.

[75] For more information, see CRS Insight IN11143, *Exposed Data Highlights Law Enforcement Use of Selected Technologies*.

[76] Drew Harwell, "Surveillance Contractor That Violated Rules by Copying Traveler Images, License Plates Can Continue to Work with CBP," *The Washington Post*, October 10, 2019.

[77] FBI, *Privacy Impact Assessment for the Next Generation Identification – Interstate Photo System*, October 29, 2019, p. 2.

necessary, for the shortest time period necessary, and notification to the FBI of any potential or actual breach of that information."[78]

CBP stores photographs of foreign nationals and U.S. citizens differently. All photographs are purged from the TVS cloud after 12 hours, regardless of citizenship status.[79] However, CBP stores photographs of foreign nationals for 14 days in the Automated Targeting System (ATS) Unified Passenger Module (UPAX).[80] These photographs are then transmitted to the Automated Biometric Identification System (IDENT), where they are retained for up to 75 years.[81] In contrast, photographs of U.S. citizens are immediately deleted after the matching process.[82] While CBP requires its commercial partners to follow these data retention requirements, a September 2020 GAO report found that CBP does not adequately audit its airline partners.[83]

Going Forward

There are currently no federal laws specifically governing law enforcement agencies' use of FRT,[84] and law enforcement agencies around the country may rely on a patchwork of technology platforms and algorithms for their facial recognition systems. As such, policymakers may question how federal law enforcement agencies assess and ensure the accuracy and security of their FRT systems as well as the policies governing their use. They may also examine the oversight of federal grants used to support or restrict the use of FRT by state, local, and tribal law enforcement. Policymakers may further consider how FRT is used more broadly in various phases of the criminal justice system, from generating leads and helping establish probable cause for an arrest or indictment, to serving as evidence in courtrooms and confirming prisoners' identities before release; this may help inform oversight and legislative efforts to enhance or bound aspects of how law enforcement uses the technology. In addition, policymakers may question whether or how recommendations from FISWG are adopted by federal law enforcement agencies; their state, local, and tribal partners; and law enforcement grant recipients.

[78] FBI, *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System*, July 9, 2018, p. 8.

[79] Ibid., p. 9.

[80] DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS/CBP/PIA-056, November 14, 2018, pp. 9, 21.

[81] Ibid., pp. 8, 21.

[82] Ibid., p. 10.

[83] GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568, September 2020, p. 46.

[84] For a discussion of relevant constitutional considerations surrounding law enforcement use of FRT, see CRS Report R46541, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*.

Appendix. NIST Efforts on Facial Recognition Technology

NIST work on FRT includes research, testing and evaluation, technical guidance and support, and standards.[85]

Research

NIST work in biometrics dates back to the 1960s. The agency's efforts span a wide range of activities to help improve the ability to establish or verify the identity of humans based upon one or more physical (e.g., face, fingerprint, iris images) or behavioral (e.g., signature analysis) characteristics.

The Information Technology Laboratory (ITL), one of six NIST research laboratories, is a measurement and testing facility that develops and deploys standards, tests, and metrics to make information systems more secure, usable, interoperable, and reliable. Among its functions, ITL conducts research on issues related to biometric measurement and testing and facilitates standards development, including those related to FRT. According to NIST, ITL has measured the core algorithmic capability of biometric recognition technologies and reported on the accuracy, throughput, reliability, and sensitivity of biometric algorithms with respect to data characteristics and subject characteristics.

NIST states that its biometric evaluations advance measurement science by providing a scientific basis for what to measure and how to measure it. These evaluations also help facilitate development of consensus-based standards by providing quantitative data for development of scientifically sound, fit-for-purpose standards. In addition, these evaluations help federal agencies determine how best to deploy FRT.

NIST's FRT research includes a wide span of activities as illustrated by the following examples:

In 2018, the National Academies published research conducted by NIST and three universities testing facial forensic examiners ability to match identities across different photographs.[86] The intent of the study was to find better ways to increase the accuracy of forensic facial comparisons. The study concluded that

> [e]xaminers and other human face "specialists," including forensically trained facial reviewers and untrained super-recognizers, were more accurate than the control groups on a challenging test of face identification. It also presented data comparing state-of-the-art facial recognition algorithms with the best human face identifiers. The best machine performed in the range of the best-performing humans, who were professional facial examiners. However, optimal face identification was achieved only when humans and machines collaborated.[87]

[85] Much of the information in this appendix is drawn from testimony given on February 6, 2020, by Charles H. Romine, Director of the National Institute of Standards and Technology's Information Technology Laboratory before the House Committee on Homeland Security.

[86] P. Jonathon Phillips et al., "Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms," *Proceedings of the National Academy of Sciences, USA*, vol. 115, no. 24 (2018), pp. 6171-6176, https://doi.org/10.1073/pnas.1721355115.

[87] Testimony of Charles H. Romine, Director, NIST Information Technology Laboratory, before U.S. Congress, House Committee on Homeland Security, *Facial Recognition Technology (FRT)*, 116th Cong., 2nd sess., February 6, 2020, https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0 (hereinafter, Romine FRT testimony).

In addition, NIST conducted the Face in Video Evaluation (FIVE) program to assess the capability of facial recognition algorithms to identify individuals appearing in video sequences. NIST documented the outcomes of FIVE in its report, *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects (NIST IR8173)*, which discusses the accuracy and speed of FRT algorithms applied to the identification of individuals appearing in video sequences drawn from six video datasets.[88] NIST completed this program in 2017. The report found that

> [h]igh accuracy recognition of passively-imaged subjects is only achievable with: a) a small minority of the algorithms tested [under this program]; b) a dedicated and deliberate design effort that must embed optical, architectural, human factors, operations-research, and face recognition expertise; c) galleries limited to small numbers of actively curated images; and d) field tests with empirical quantitative calibration and optimization.[89]

Further, the report states that with "better cameras, better design, and the latest algorithm developments, recognition accuracy can advance even further," but notes that "even with perfect design, some proportion of a non-cooperative population will not be recognized" due to failure to acquire cases where subjects never look toward the camera or because their faces were occluded.[90]

The report concluded, in part, that

> [d]eployment should proceed only after quantitative assessment of objectives, alternatives, ease of evasion or circumvention, enrolled population sizes, search volumes, the proportion of searches expected to have an enrolled mate, accuracy requirements, consequences and procedures for resolution of errors, and speed and hardware cost constraints. In particular, deployers must weight their tolerance for misses and their risk appetite. In addition, when non-cooperative face recognition is used to identify individuals nominated to a watchlist, human reviewers must be employed to adjudicate whether candidate matches are true or false positives … [and that] overall error rates of the hybrid machine-human system must be understood and planned for.[91]

NIST has also conducted a number of FRT-related "Grand Challenge" competitions—including the Face Recognition Grand Challenge (2004-2006) and the Multiple Biometric Grand Challenge (2008-2010) programs—to encourage the FRT community to break new ground in solving biometric research problems.

Testing and Evaluation

Since 2000, NIST has operated a Face Recognition Vendor Testing (FRVT) program to assess the capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. The voluntary program is open to any organization worldwide, and participants may submit their algorithms on a continuous basis for evaluation. Users include corporate research and development laboratories and universities. Submitted algorithms include commercially available products and prototypes that are not necessarily available as final products ready for integration in

[88] NIST, Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects (NIST IR8173), March 2017, https://doi.org/10.6028/NIST.IR.8173.

[89] Ibid.

[90] Ibid.

[91] Ibid.

FRT systems. NIST posts performance results for evaluated algorithms on its FRVT website along with the name of the organization that developed the algorithm.[92]

According to NIST, the FRVT program does not train face recognition algorithms.[93] NIST does not provide training data to the software under test, and the software is prohibited from adapting to any data that is passed to the algorithms during a test.[94]

With respect to its 2019 FRVT activities, NIST reported that

> [t]he 2019 FRVT quantified the accuracy of face recognition algorithms for demographic groups defined by sex, age, and race or country of birth, for both one-to-one verification algorithms and one-to-many identification search algorithms. NIST conducted tests to quantify demographic differences for 189 face recognition algorithms from 99 developers, using four collections of photographs with 18.27 million images of 8.49 million people. These images came from operational databases provided by the State Department, the Department of Homeland Security and the FBI. Previous FRVT reports documented the accuracy of these algorithms and showed a wide range in accuracy across algorithms. The more accurate algorithms produce fewer errors and can therefore be anticipated to have smaller demographic differentials.
>
> NIST Interagency Report 8280,[95] released on December 19, 2019, quantifies the effect of age, race, and sex on face recognition performance. It found empirical evidence for the existence of demographic differentials in face recognition algorithms that NIST evaluated. The report distinguishes between false positive and false negative errors, and notes that the impacts of errors are application dependent.[96]

In interpreting the results of the 2019 FRVT report on demographic effects, one should note that the study used high-quality, standards-compliant images, not image data from the Internet nor from video surveillance. Thus, demographic differentials from images in such everyday scenarios were not evaluated. Some stakeholders have criticized such limitations in analyzing face recognition algorithms and called for more testing "in the field under real-life conditions."[97]

With respect to its 2018 FRVT, NIST reported that

> [t]he 2018 FRVT tested 127 facial recognition algorithms from the research laboratories of 39 commercial developers and one university, using 26 million mugshot images of 12 million individuals provided by the FBI. The 2018 FRVT measured the accuracy and speed of one-to-many facial recognition identification algorithms. The evaluation also contrasted

[92] NIST, "FRVT 1:1 Leaderboard," https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt. The FRVT 1:1 Leaderboard shows the top performing 1:1 algorithms measured on false non-match rate across several different datasets.

[93] According to NIST, "The process of training a face recognition algorithm (or any machine learning algorithm) involves providing a machine learning algorithm with training data to learn from. The training data shall contain the correct answer, which is known as ground-truth label, or a target. The learning algorithm finds patterns in the training data that map the input data attributes to the target and builds a machine-learning model that captures these patterns. This model can then be used to get predictions on new data for which the target is unknown." See Romine FRT testimony.

[94] Romine FRT testimony.

[95] NIST, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects (NIST IR8280)*, December 19, 2019, https://doi.org/10.6028/NIST.IR.8280. This is the third in a series of reports on the 2019 FRVT activities that extends the evaluations from parts 1 and 2—which covered the performance of one-to-one and one-to-many face recognition algorithms, respectively—to document accuracy variations across demographic groups.

[96] Romine FRT testimony.

[97] Darrell M. West, "10 Actions That Will Protect People From Facial Recognition Software," Brookings Institution, October 31, 2019, https://www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/.

> mugshot accuracy with that from lower quality images. The findings, reported in *NIST Interagency Report 8238*,[98] showed that massive gains in accuracy have been achieved since the FRVT in 2013, which far exceed improvements made in the prior period (2010-2013).
>
> The accuracy gains observed in the 2018 FVRT study stem from the integration, or complete replacement, of older facial recognition techniques with those based on deep convolutional neural networks. While the industry gains are broad, there remains a wide range of capabilities, with some developers providing much more accurate algorithms than others do. Using FBI mugshots, the most accurate algorithms fail only in about one quarter of one percent of searches, and these failures are associated with images of injured persons and those with long time lapse since the first photograph. The success of mugshot searches stems from the new generation of facial recognition algorithms, and from the adoption of portrait photography standards first developed at NIST in the late 1990s.[99]

Technical Guidance and Scientific Support

NIST provides technical guidance and scientific support to various U.S. government and law enforcement agencies for the use of FRT. For example, NIST's research supported DHS's transition from a 2-fingerprint to a 10-fingerprint collection standard for visa application and entry into the United States to prevent terrorism and identity fraud as well as to prevent criminals and immigration violators from crossing U.S. borders. In addition, NIST is working with CBP to analyze performance effects of image quality and traveler demographics, and to provide recommendations regarding match algorithms, optimal thresholds, and match gallery creation for TVS. NIST's work also supports the FBI and the Office of the Director of National Intelligence's Intelligence Advanced Research Projects Activity (IARPA).[100]

[98] NIST, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification (NIST IR8238)*, November 2018, https://doi.org/10.6028/NIST.IR.8238. This report was subsequently updated and extended by NIST as *Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST Interagency Report 8271*, September 2019, https://doi.org/10.6028/NIST.IR.8271.

[99] Romine FRT testimony.

[100] Romine FRT testimony.

Standards

The United States has a voluntary, consensus-based standards development system.[101] Under the National Technology Transfer and Advancement Act of 1995 (P.L. 104-113)[102] and OMB Circular A-119,[103] NIST is charged with promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities, encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government-unique standards, and coordinating federal agency participation in the development of relevant standards.

NIST leads national and international consensus standards activities in biometrics, such as FRT, to ensure that they are interoperable, reliable, secure, and usable.

The following examples of NIST consensus standards development activities illustrate NIST's role in this arena:

Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (ANSI/NIST-ITL 1-2011 Update: 2015), published by the American National Standards Institute and NIST, is a biometric standard used in 160 countries to facilitate the exchange of biometric data across jurisdictional lines and between dissimilar systems. This standard allows accurate and interoperable exchange of biometrics information by law enforcement agencies globally, assisting in the identification of criminals and terrorists. The standard continues to evolve to support government applications, including law enforcement, homeland security, and other identity management applications. According to NIST, the standard is used for nearly all law enforcement biometric collections worldwide.[104]

---

[101] According to the American National Standards Institute (ANSI),

> The U.S. standardization system reflects a market-driven and highly diversified society. It is a decentralized system that is naturally partitioned into industrial sectors and supported by independent, private sector standards developing organizations (SDOs). It is a demand-driven system in which standards are developed in response to specific concerns and needs expressed by industry, government, and consumers. And it is a voluntary system in which both standards development and implementation are driven by stakeholder needs…. Voluntary standards serve as the cornerstone of the distinctive U.S. infrastructure. These documents arise from a formal, coordinated, consensus-based and open process. Their development depends upon data gathering, a vigorous discussion of all viewpoints, and agreement among a diverse range of stakeholders…. Voluntary refers only to the manner in which the standard was developed; it does not necessarily refer to whether compliance to a consensus standard is optional or whether a government entity or market sector has endorsed the document for mandatory use. Most other countries adhere to a "top-down" approach to standardization where the government or groups closely coupled to government either serve as the standards setter or mandate what standards will be developed.

(American National Standards Institute, "Overview of the U.S. Standardization System," https://www.standardsportal.org/usa_en/standards_system.aspx.) ANSI was founded in 1918 by five engineering societies and three federal agencies (the Departments of War, Navy, and Commerce). ANSI is the sole U.S. representative and dues-paying member of the two major non-treaty international standards organizations, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[102] Codified at 15 U.S.C. §272(b), which directs the Secretary of Commerce, through the NIST director, "to facilitate standards-related information sharing and cooperation between Federal agencies and to coordinate the use by Federal agencies of private sector standards, emphasizing where possible the use of standards developed by private, consensus organizations" and "to coordinate technical standards activities and conformity assessment activities of Federal, State, and local governments with private sector technical standards activities and conformity assessment activities, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures."

[103] Executive Office of the President, Office of Management and Budget, Circulars, https://www.whitehouse.gov/omb/information-for-agencies/circulars/.

[104] Romine FRT testimony.

NIST has also led and provided technical expertise for the development of international biometric standards in ISO/IEC Joint Technical Committee 1, Subcommittee 37 (JTC1/SC37) – Biometrics.[105] The standards developed by the subcommittee, which was established in 2002, are broadly used nationally and internationally. Since 2006, the subcommittee has published standards on biometric performance testing and reporting (including guidance on principles and framework, testing methodologies, modality-specific testing, interoperability performance testing, and access control scenarios), drawing upon NIST technical contributions.

Author Information

Kristin Finklea, Coordinator
Specialist in Domestic Security

Abigail F. Kolker
Analyst in Immigration Policy

Laurie Harris
Analyst in Science and Technology Policy

Disclaimer

[105] ISO is the International Organization for Standards. IEC is the International Electrotechnical Commission.