United States Government Accountability Office

Testimony

Before the Committee on Oversight and Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, June 4, 2019

FACE RECOGNITION TECHNOLOGY

DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains

Statement of Gretta L. Goodwin, Director
Homeland Security and Justice

June 4, 2019

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 Highlights

Highlights of GAO-19-579T, a testimony before the Committee on Oversight and Reform, House of Representatives

Why GAO Did This Study

Technology advancements have increased the overall accuracy of automated face recognition over the past few decades. This technology has helped law enforcement agencies identify criminals in their investigations. However, there are questions about the accuracy of the technology and the protection of privacy and civil liberties when face recognition technologies are used to identify people for investigations.

This statement describes the extent to which the FBI (1) ensures adherence to laws and policies related to privacy regarding its use of face recognition technology, and (2) ensures its face recognition capabilities are sufficiently accurate. This statement is based on GAO's May 2016 report regarding the FBI's use of face recognition technology (GAO-16-267) and includes agency updates to GAO's recommendations. To conduct its prior work, GAO reviewed federal privacy laws, and DOJ and FBI policies and operating manuals. GAO interviewed officials from the FBI and the departments of Defense and State, which coordinate with the FBI on face recognition. GAO also interviewed two state agencies that partner with the FBI to use multiple face recognition capabilities. For updates, GAO reviewed FBI data, as well as materials provided by DOJ and the FBI on the status of GAO's recommendations.

What GAO Recommends

In its May 2016 report, GAO made three recommendations related to privacy, one of which has been implemented. GAO also made three recommendations related to accuracy that the FBI is still working to address.

View GAO-19-579T. For more information, contact Gretta L. Goodwin at 202-512-8777 or goodwing@gao.gov.

What GAO Found

In May 2016, GAO found that the the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) could improve transparency and oversight to better safeguard privacy and had limited information on accuracy of its face recognition technology. GAO made six recommendations to address these issues. As of May 2019, DOJ and the FBI had taken some actions to address three recommendations—one of which the FBI has fully implemented—but has not taken any actions on the other three.

Privacy. In its May 2016 report, GAO found that DOJ did not complete or publish key privacy documents for FBI's face recognition systems in a timely manner and made two recommendations to DOJ regarding its processes for developing these documents. These included privacy impact assessments (PIA), which analyze how personal information is collected, stored, shared, and managed in federal systems, and system of records notices, which inform the public about, among other things, the existence of the systems and the types of data collected. DOJ has taken actions to expedite the development process of the PIA. However, DOJ has yet to take action with respect to the development process for SORNs. GAO continues to believe both recommendations are valid and, if implemented, would help keep the public informed about how personal information is being collected, used and protected by DOJ components. GAO also recommended the FBI conduct audits to determine if users of FBI's face recognition systems are conducting face image searches in accordance with DOJ policy requirements, which the FBI has done.

Accuracy. GAO also made three recommendations to help the FBI better ensure the accuracy of its face recognition capabilities. First, GAO found that the FBI conducted limited assessments of the accuracy of face recognition searches prior to accepting and deploying its face recognition system. The face recognition system automatically generates a list of photos containing the requested number of best matched photos. The FBI assessed accuracy when users requested a list of 50 possible matches, but did not test other list sizes. GAO recommended accuracy testing on different list sizes. Second, GAO found that FBI had not assessed the accuracy of face recognition systems operated by external partners, such as state or federal agencies, and recommended it take steps to determine whether external partner systems are sufficiently accurate for FBI's use. The FBI has not taken action to address these recommendations. GAO continues to believe that by verifying the accuracy of both systems—its system, and the systems of external partners—the FBI could help ensure that the systems provide leads that enhance criminal investigations. Third, GAO found that the FBI did not conduct an annual review to determine if the accuracy of face recognition searches was meeting user needs, and recommended it do so. In 2016 and 2017 the FBI submitted a paper to solicit feedback from system users. However, this did not result in formal responses from users and did not constitute a review of the system. GAO continues to believe that conducting such a review would help provide important information about potential factors affecting accuracy of the system.

Chairman Cummings, Ranking Member Jordan, and Members of the Committee:

I am pleased to be here today to discuss our prior work on the Federal Bureau of Investigation's (FBI) use of face recognition technology. Over the past few decades, technological advancements have increased the overall accuracy of automated face recognition technology that is now used for wide-ranging applications from accessing a smart phone to banking and identifying friends in photos. Face recognition can also help law enforcement agencies identify criminals in federal, state, and local investigations, according to the FBI. For example, the FBI used face recognition in August 2017 to assist in the identification and arrest of an FBI Ten Most Wanted Fugitive. However, some academics and privacy advocates have questioned whether the technology is sufficiently accurate for this use. In addition, the use of face recognition technology raises questions regarding the protection of privacy and individual civil liberties.

This statement summarizes key findings from our prior work which addressed the extent to which the FBI (1) ensures adherence to laws and policies related to privacy regarding its use of face recognition technology, and (2) ensures its face recognition capabilities are sufficiently accurate. Specifically, this statement is based on our May 2016 report and our testimony before this Committee in March 2017 regarding the FBI's use of face recognition technology as well as actions the FBI has taken, as of May 2019, to address our recommendations from this work.[1] These recommendations are also included in our April 2019 letter to the Department of Justice regarding priority open recommendations.[2] More information on our scope and methodology can be found in our May 2016 report.[3] This statement also provides updates

[1]GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* GAO-16-267 (Washington, D.C.: May 16, 2016); *Face Recognition Technology: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy,* GAO-17-489T (Washington, D.C.: March 22, 2017).

[2]GAO, *Priority Open Recommendations: Department of Justice*, GAO-19-361P (Washington, D.C.: Apr. 10, 2019). We highlight priority recommendations because, upon implementation, they may significantly improve government operation, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk area or duplication. Since 2015, we have sent letters to selected agencies to highlight the importance of implementing such recommendations.

[3]GAO-16-267.

to FBI data we reported in May 2016. Specifically, we reviewed data that the FBI provided in May 2019 regarding summary statistics on the number of photos in the FBI's face recognition system, the number of face searches conducted, and the information available to the FBI unit that conducts face recognition searches. We also reviewed materials provided by DOJ and the FBI on the status of our recommendations.

The work upon which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

FBI's Use of Face Recognition Technology

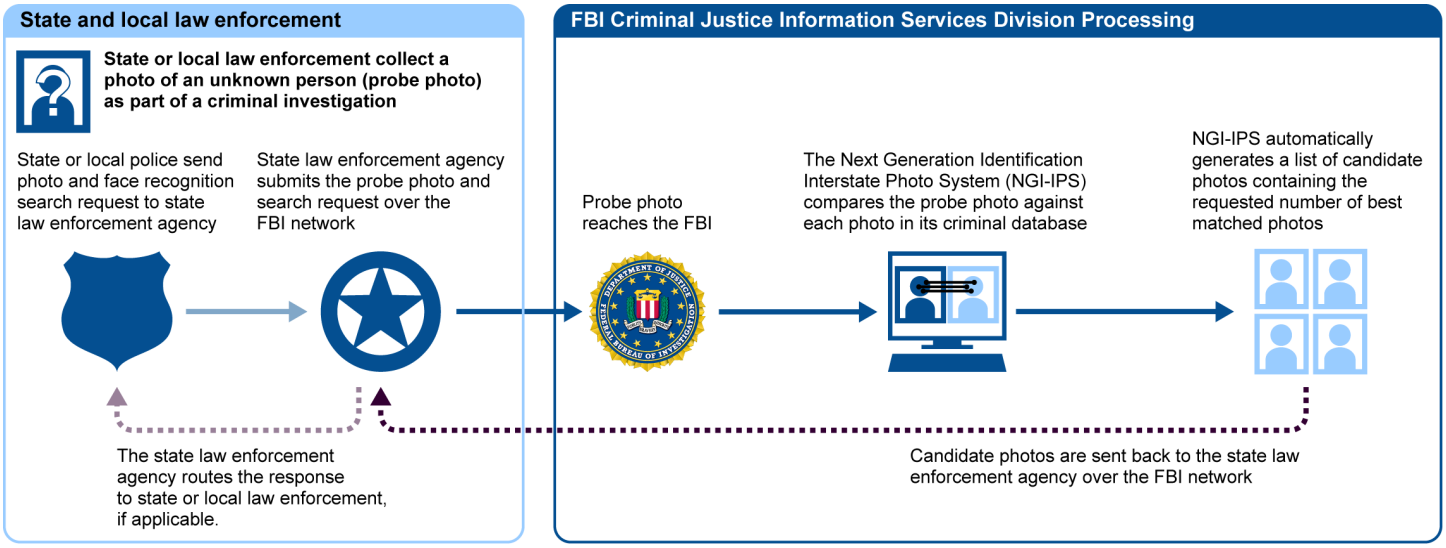
For decades, fingerprint analysis was the most widely used biometric technology for positively identifying arrestees and linking them with any previous criminal record. However, beginning in 2010, the FBI began incrementally replacing the Integrated Automated Fingerprint Identification System (IAFIS) with Next Generation Identification (NGI).[4] NGI was not only to include fingerprint data from IAFIS and biographic data, but also to provide new functionality and improve existing capabilities by incorporating advancements in biometrics, such as face recognition technology. As part of the fourth of six NGI increments, the FBI updated the Interstate Photo System (IPS) to provide a face recognition service that allows law enforcement agencies to search a database of criminal photos that accompanied fingerprint submissions using a photo of an unknown person—called a probe photo.[5] The FBI began a pilot of NGI-IPS in December 2011, and NGI-IPS became fully operational in April 2015.

[4]IAFIS was a national, computerized system for storing, comparing, and exchanging fingerprint data in a digital format.

[5]When the FBI implemented IAFIS in 1999, the Criminal Justice Information Service (CJIS) began storing mugshot photos submitted with fingerprints in a photo database and also digitized all previously submitted hardcopy mugshots. However, until the implementation of NGI, users could only search for photos using the person's name or unique FBI number.

NGI-IPS users include the FBI and selected state and local law enforcement agencies, which can submit search requests to help identify an unknown person using, for example, a photo from a surveillance camera. When a state or local agency submits such a photo, NGI-IPS uses an automated process to return a list of candidate photos from the database. The number of photos returned ranges from 2 to 50 possible candidate photos from the database, depending on the user's specification. According to the FBI, in fiscal year 2018, NGI-IPS returned about 50,000 face recognition search results to law enforcement agency users, a decrease from about 90,000 search results in fiscal year 2017. Figure 1 describes the process for a search requested by state or local law enforcement.

Figure 1: Description of the Federal Bureau of Investigation's (FBI) Face Recognition System Request and Response Process for State and Local Law Enforcement as of May 2016.



Source: GAO analysis of FBI documentation. | GAO-19-579T

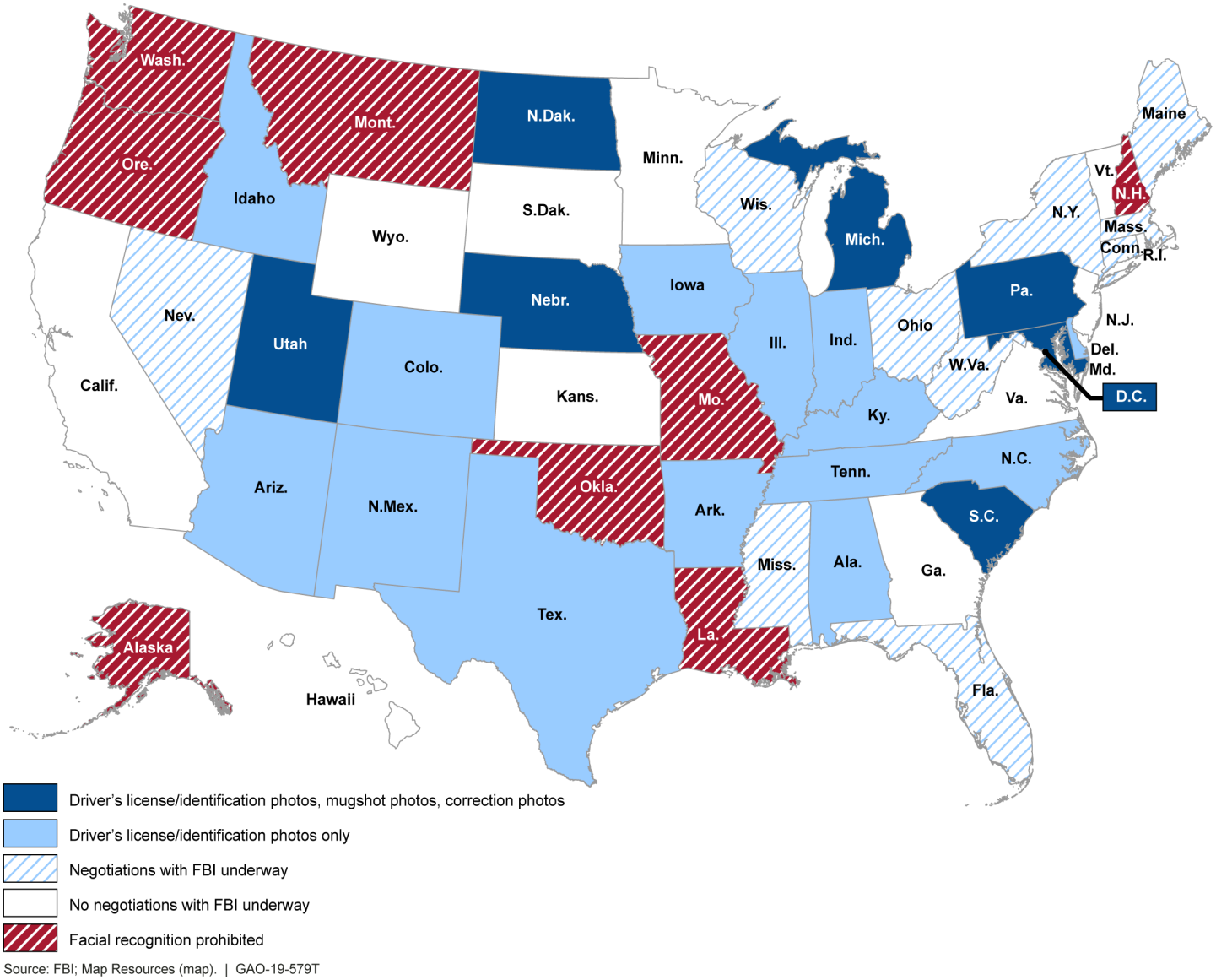
In addition to the NGI-IPS, the FBI has an internal unit called Facial Analysis, Comparison and Evaluation (FACE) Services that provides face recognition capabilities, among other things, to support active FBI investigations.[6] FACE Services has access to NGI-IPS, and can also search or request to search databases owned by the departments of State and Defense and 21 states, which use their own face recognition

[6]FACE Services began supporting FBI investigations in August 2011.

systems.[7] Figure 2 shows which states partnered with the FBI for FACE Services requests, as of May 2019, according to the FBI.

[7]We reported in May 2016 that, according to FBI officials, the external photo databases do not contain privately obtained photos or photos from social media, and the FBI does not maintain these photos. Also, according to FBI officials, legal authority exists for the face recognition searching of all of these photo databases. For example, FBI officials stated that states are authorized to use the law enforcement exception of the Driver's Privacy Protection Act—a federal law that regulates and restricts access to a state's department of motor vehicle records— to permit sharing photos with the FBI. Further, the FBI also has memoranda of understanding with their partner agencies that describe the legal authorities that allow the FBI to search the partner agencies' photos.

Figure 2: Status of Reported Partnerships for Photo Searches between States and the Federal Bureau of Investigation (FBI) Facial Analysis, Comparison, and Evaluation (FACE) Services, as of May 2019



Source: FBI; Map Resources (map). | GAO-19-579T

Unlike NGI-IPS, which primarily contains photos obtained from criminal justice sources, these external systems primarily contain photos from state and federal government databases, such as driver's license photos and visa applicant photos. According to the FBI, the total number of face

photos available in all searchable repositories for FACE Services is over 641 million.[8] Biometric images specialists for FACE Services manually review any photos received from their external partners before returning a photo as an investigative lead to the requesting FBI agents. No more than two photos are returned as a lead after the specialist for FACE Services completes the review. However, according to FACE Services officials we met with during our May 2016 review, if biometric images specialists determine that none of the databases returned a likely match, they do not return any photos to the agents. According to the FBI, from August 2011 (when searches began) through April 2019, FACE Services received 153,636 photos of unknown persons (often called probe photos) from FBI headquarters, field offices, and overseas offices, which resulted in 390,186 searches of various databases in attempt to find photo matches of known individuals in these databases.

Privacy Laws and Responsibilities at DOJ

Federal agency collection and use of personal information, including face images, is governed primarily by two laws: the Privacy Act of 1974[9] and the privacy provisions of the E-Government Act of 2002.[10]

- The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice (SORN) in the Federal Register.[11] According to Office of Management and Budget (OMB) guidance, the purposes of the notice are to inform the public of the existence of systems of records; the kinds of information maintained; the kinds of individuals on whom information is maintained; the purposes for which they are

[8]The over 641 million refers to photos, not the total number of identities, and reflects data as of April 2019.

[9]Pub. L. No. 93-579, 88 Stat. 1896 (1974), as amended; 5 U.S.C. § 552a.

[10]Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002); 44 U.S.C. § 3501 note.

[11]A system of record is defined by the Privacy Act of 1974 as a group of records containing personal information under the control of any agency from which information is retrieved by the name of an individual or by an individual identifier. See 5 U.S.C. § 552a(a)(4), (5).

used; and how individuals can exercise their rights under the Privacy Act.[12]

- The E-Government Act of 2002 requires that agencies conduct Privacy Impact Assessments (PIAs) before developing or procuring information technology (or initiating a new collection of information) that collects, maintains, or disseminates personal information. The assessment helps agencies examine the risks and effects on individual privacy and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. OMB guidance also requires agencies to perform and update PIAs as necessary where a system change creates new privacy risks, for example, when the adoption or alteration of business processes results in personal information in government databases being merged, centralized, matched with other databases or otherwise significantly manipulated.[13]

Within DOJ, preserving civil liberties and protecting privacy is a responsibility shared by departments and component agencies. As such, DOJ and the FBI have established oversight structures to help protect privacy and oversee compliance with statutory and policy requirements. For example, the FBI drafts privacy documentation for its face recognition capabilities, and DOJ offices review and approve key documents developed by the FBI—such as PIAs and SORNs.

[12]OMB, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,962 (July 9, 1975).

[13]See M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).

DOJ and FBI Have Taken Steps Since May 2016 to Better Ensure Privacy but Work Remains to Fully Address Prior Recommendations

DOJ Has Taken Steps to More Quickly Publish Privacy Impact Assessments but Has Not Fully Implemented Its Revised Process

We reported in May 2016 that the FBI did not (1) update the NGI-IPS PIA in a timely manner when the system underwent significant changes, or (2) develop and publish a PIA for FACE Services before that unit began supporting FBI agents. However, DOJ and the FBI have since taken steps to review and publish PIAs more quickly.

As discussed in our 2016 report, consistent with the E-Government Act and OMB guidance, DOJ developed guidance that requires initial PIAs to be completed at the beginning of development of information systems and any time there is a significant change to the information system in order to determine whether there are any resulting privacy issues. In accordance with this guidance, FBI published a PIA at the beginning of the development of NGI-IPS in 2008, as required.[14] However, the FBI did not publish a new PIA or update the 2008 PIA before beginning to pilot NGI-IPS in December 2011 or as significant changes were made to the system through September 2015.[15] During the pilot, the FBI used NGI-IPS to conduct over 20,000 searches to assist in investigations.

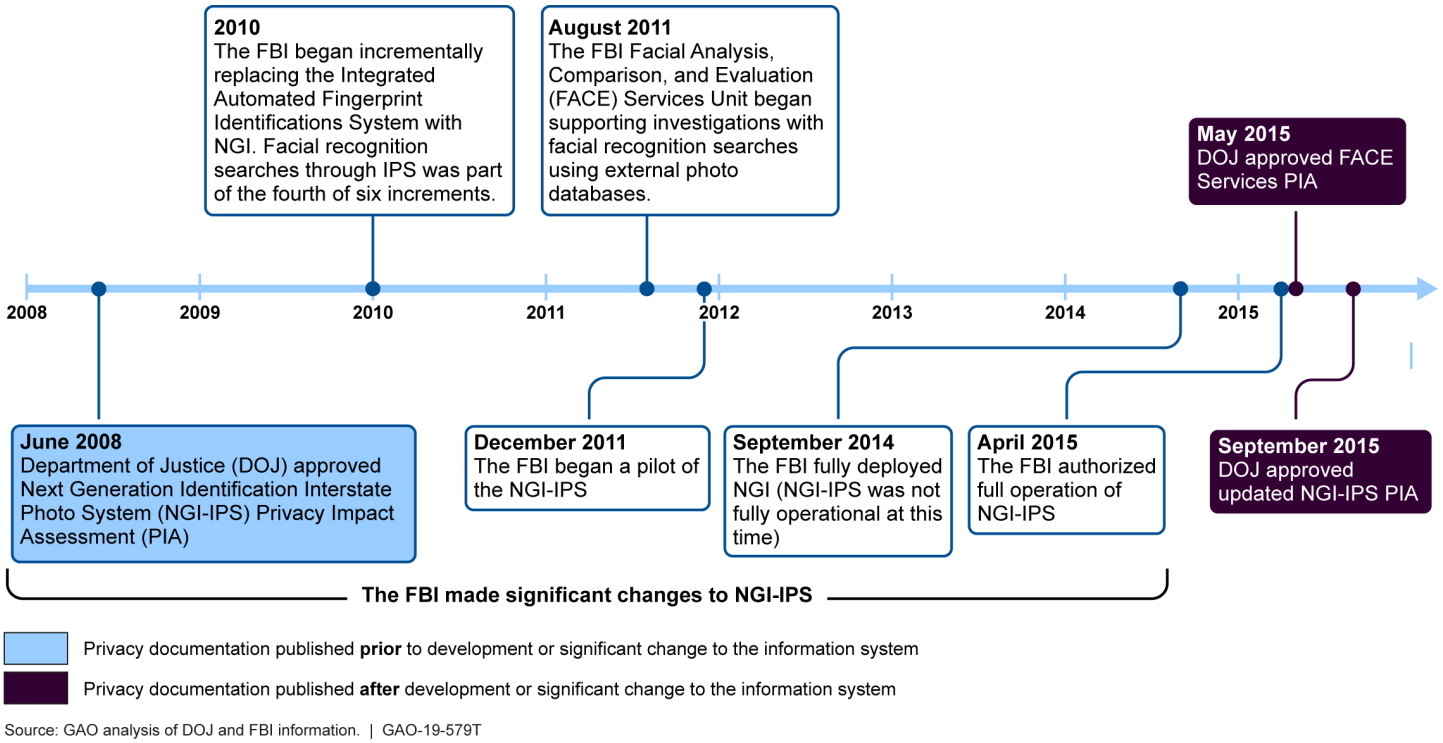
Similarly, DOJ did not approve a PIA for FACE Services when it began supporting investigations in August 2011. As a new use of information technology involving the handling of personal information, it too required a PIA, according to the E-Government Act, as well as OMB and DOJ

[14]Specifically, in June 2008 the FBI published a PIA of its plans for NGI-IPS and indicated it was in the study phase, which included development of functional and system requirements.

[15]In December 2011, as part of a pilot program, the FBI began incrementally allowing a limited number of states to submit face recognition searches against a subset of criminal images in the FBI's database. Beginning in April 2015, states started transitioning from the pilot to full operational capability.

guidance.[16] Figure 3 provides key dates in the implementation of these face recognition capabilities and the associated PIAs.

Figure 3: Key Dates in the Implementation of the Federal Bureau of Investigation's (FBI) Face Recognition Capabilities and Associated Privacy Impact Assessments



Source: GAO analysis of DOJ and FBI information. | GAO-19-579T

DOJ approved the NGI-IPS PIA in September 2015 and the FACE Services PIA in May 2015—over 3 years after the NGI-IPS pilot began and FACE Services began supporting FBI agents with face recognition services. Among other factors, implementation of the NGI-IPS pilot constituted a significant change in the FBI's use of the technology that, consistent with the E-Government Act and OMB guidance required DOJ/FBI to update the PIA. Similarly, DOJ/FBI acknowledged that FACE Services began supporting FBI investigations in 2011, which involved storing photos in a new work log and also performing automated searches instead of manual searches. As a new use of information technology involving the handling of personal information, it too required a

[16]The FBI conducted a privacy threshold assessment of FACE Services in 2012 that determined a PIA was necessary for the worklog used to store personal information.

PIA. While DOJ and the FBI updated the internal drafts of these PIAs, the public remained unaware of the department's consideration for how the FBI uses personal information in the face recognition search process.[17] Given the issues we identified, we recommended that DOJ assess the PIA development process to determine why PIAs were not published prior to using or updating face recognition capabilities.

Although DOJ officials did not concur with this recommendation, they did agree that all DOJ processes may be reviewed for improvements and efficiencies. In November 2018, DOJ officials told us that they had reviewed the PIA development process and determined that one reason the FBI's face recognition PIAs were not completed more quickly was because the FBI and DOJ engaged in an extensive PIA revision process. As a result, DOJ reported that it implemented a pilot in 2018 to expedite the PIA approval process, which included developing a PIA approval template, conducting DOJ's review earlier in the process, and focusing the review solely on legal sufficiency instead of a more comprehensive review that included less significant editorial changes. According to DOJ, this new process has significantly reduced the time required between the completion of the PIA process by the FBI and the review by DOJ. Further, DOJ reported that it has applied the same process to other DOJ components since December 2018, and that the pilot is evolving into an operational process. We will continue to monitor DOJ's implementation of its review process changes.

[17]FBI officials stated that they drafted an updated PIA for NGI-IPS in January 2015 and submitted it to DOJ for review, which was before NGI-IPS became fully operational in April 2015.

DOJ Did Not Complete a SORN Addressing FBI's Face Recognition Capabilities in a Timely Manner and Has Not Implemented Corrective Actions

We reported in May 2016 that DOJ did not publish a SORN, as required by the Privacy Act, that addresses the collection and maintenance of photos accessed and used through the FBI's face recognition capabilities, in a timely manner. The DOJ published the SORN on May 5, 2016—after completion of our review—even though those capabilities were in place since 2011.[18] According to OMB guidance then in effect, the SORN "must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information."[19] However, from 2011 through May 2016, the agency collected and maintained personal information for these capabilities without the required explanation of what information it was collecting or how it was used. For example, at the time of our review, the existing version of the SORN that covered FBI's face recognition capabilities was dated September 1999. According to DOJ officials, it did not address the collection and maintenance of photos accessed and used through NGI for the FBI's face recognition capabilities but rather discussed fingerprint searches. Given that DOJ did not publish the SORN in a timely manner, we recommended DOJ develop a process to determine why a SORN was not published for the FBI's face recognition capabilities prior to using NGI-IPS, and implement corrective actions to ensure SORNs are published before systems become operational. DOJ agreed, in part, with our recommendation and submitted the SORN for publication after we provided our draft report for comment.

According to DOJ, it continues to review and update its pre-existing SORNs on an ongoing basis and is continually improving the scope and efficiency of its privacy processes. However, as of May 2019, DOJ had not taken actions to address our recommendation. Further, in April 2019, DOJ stated that with respect to transparency, a published PIA will provide much the same information that would be contained in a SORN and may provide it in a timelier manner. However, according to OMB guidance, the purpose of the SORN is to inform the public of the existence of systems of records; the kinds of information maintained; the kinds of individuals on

[18]The SORN published by DOJ modified the existing Fingerprint Identification Records System and renamed it the Next Generation Identification (NGI) System. See 81 Fed. Reg. 27,284 (May 5, 2016). According to DOJ officials, the FBI initially waited to complete the NGI SORN until all of NGI's capabilities were identified in order to provide a comprehensive explanation of NGI and limit the number of necessary SORN revisions.

[19]OMB Circular A-130, App. I, § 5.a(2)(a) (2000). OMB subsequently relocated Appendix I to OMB Circular A-130 to OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, as reissued. See 81 Fed. Reg. 94,424 (Dec. 23, 2016).

whom information is maintained; the purposes for which they are used; and how individuals can exercise their rights under the Privacy Act. Further, PIAs and SORNs both contain information key to providing the public with information about the collection of their personal information, among other things. We continue to believe that by assessing the SORN development process and taking corrective actions to ensure timely development of future SORNs, DOJ would be better positioned to provide the public with a better understanding of how personal information is being used and protected by DOJ components.

FBI Has Conducted Audits to Oversee the Use of NGI-IPS and FACE Services

The Criminal Justice Information Services Division (CJIS), which operates FBI's face recognition capabilities, has an audit program to evaluate compliance with restrictions on access to CJIS systems and information by its users, such as the use of fingerprint records. However, at the time of our May 2016 review, it had not completed audits of the use of NGI-IPS or FACE Services searches of external databases. We reported that state and local users had been accessing NGI-IPS since December 2011 and had generated IPS transaction records since then that would enable CJIS to assess user compliance.[20] In addition, we found that the FACE Services Unit had used external databases that included primarily civil photos to support FBI investigations since August 2011, but the FBI had not audited its use of those databases.[21] *Standards for Internal Control in the Federal Government* calls for federal agencies to design and implement control activities to enforce management's directives and to monitor the effectiveness of those controls.[22] In May 2016, we recommended that the FBI conduct audits to determine the extent to which users of NGI-IPS and biometric images specialists in FACE Services are conducting face image searches in accordance with CJIS policy requirements.

[20]Transaction records are a log of communications between CJIS and CJIS system users. NGI-IPS transaction records would include, among other things, tenprint submissions transactions (submission of all ten fingerprints), images submissions for an existing identity, face recognition search requests, and face image search results.

[21]Unlike NGI-IPS, which primarily contains criminal photos, these external systems primarily contain civil photos from state and federal government databases, such as visa applicant photos and selected states' driver's license photos.

[22]GAO, *Internal Control: Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999).

DOJ partially concurred with our recommendation. Specifically, DOJ concurred with the portion of our recommendation related to the use of NGI-IPS. In March 2017, DOJ reported that the FBI began assessing NGI-IPS requirements in participating states in conjunction with its triennial National Identity Services audit, and by February 2018 had conducted eight NGI-IPS audits, which found no significant findings of noncompliance. In February 2018, DOJ provided us with copies of the final audit results for one state and its NGI-IPS audit reference guide.

The FBI reported that it conducted an audit of FACE Services in September 2018. According to FBI documentation, the purpose of the audit was to determine the extent to which specialists in FACE Services conducted face image searches in accordance with FBI privacy laws and policies. The scope of the audit focused on determining adherence to policies which govern the appropriate use of NGI-IPS, including those for policy development as well as authorized requests and responses. The FBI reported that it finalized the audit report in April 2019, which concluded that the Face Services Unit is operating in accordance with privacy laws and policies. Further, the FBI stated in May 2019 that audits of FACE Services will continue on a triennial basis and that it conducts triennial audits of states that use NGI-IPS. As a result, DOJ has fully implemented our recommendation.

FBI Has Taken Limited Actions to Address Our Recommendations for Ensuring the Accuracy of Its Face Recognition Capabilities

FBI Has Conducted Limited Assessments of the Accuracy of NGI-IPS Face Recognition Searches

In May 2016, we reported that prior to accepting and deploying NGI-IPS, the FBI conducted testing to evaluate how accurately face recognition searches returned matches to persons in the database. However, we found that the tests were limited because they did not include all possible candidate list sizes and did not specify how often incorrect matches were returned.[23] According to the National Science and Technology Council and the National Institute of Standards and Technology at the time, the detection rate (how often the technology generates a match when the person is in the database) and the false positive rate (how often the technology incorrectly generates a match to a person in the database) are both necessary to assess the accuracy of a face recognition system.[24] The FBI's detection rate requirement for face recognition searches at the time stated that when the person exists in the database, NGI-IPS shall return a match of this person at least 85 percent of the time. However, we found that the FBI only tested this requirement with a candidate list of 50 potential matches. In these tests, 86 percent of the time, a match to a person in the database was correctly returned. The FBI had not assessed accuracy when users requested a list of 2 to 49 matches.

According to FBI, a smaller list would likely lower the accuracy of the searches as the smaller list may not contain the likely match that would be present in the larger list. Further, FBI officials stated during our May 2016 review that they had not assessed how often NGI-IPS face recognition searches erroneously match a person to the database (the false positive rate). If false positives are returned at a higher than acceptable rate, law enforcement users may waste time and resources pursuing unnecessary investigative leads. In addition, we concluded that by conducting this assessment the FBI would help ensure that it is sufficiently protecting the privacy and civil liberties of U.S. citizens enrolled in the database. Therefore, we recommended that the FBI conduct tests of NGI-IPS to verify that the system is sufficiently accurate for all allowable candidate list sizes and ensure that both the detection rate and the false positive rate are identified for such tests.

In comments on our draft report in 2016, and reiterated during recommendation follow-up in May 2019, DOJ did not concur with this

[23]NGI-IPS automatically generates a list of candidate photos containing the requested number of best matched photos.

[24]National Science and Technology Council, *Biometrics Frequently Asked Questions* (Sept. 7, 2006) and National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

recommendation. DOJ officials stated that the FBI has performed accuracy testing to validate that the system meets the requirements for the detection rate, which fully satisfies requirements for the investigative lead service provided by NGI-IPS. As of May 2019, DOJ has not taken action to address the recommendation.

We continue to believe that the recommended action is needed. Such action would allow the FBI to have more reasonable assurance that NGI-IPS provides leads that help enhance, rather than hinder, criminal investigations and that helps protect the privacy of citizens. As noted above, a key focus of our recommendation is the need to ensure that NGI-IPS is sufficiently accurate for all allowable candidate list sizes. As we reported, although the FBI tested the detection rate for a candidate list of 50 photos, they did not do such tests when NGI-IPS users request smaller candidate lists—specifically between 2 and 50 photos. Further, according to the FBI Information Technology Life Cycle Management Directive, testing needs to confirm the system meets all user requirements. Because the accuracy of NGI-IPS's face recognition searches when returning fewer than 50 photos in a candidate list is unknown, the FBI is limited in understanding whether the results are accurate enough to meet NGI-IPS users' needs.

In comments on our May 2016 report, DOJ officials also stated that searches of NGI-IPS produce a gallery of likely candidates to be used as investigative leads, not for positive identification.[25] As a result, according to DOJ officials, NGI-IPS cannot produce false positives and there is no false positive rate for the system. We disagree with DOJ. According to the National Institute of Standards and Technology, the detection rate and the false positive rate are both necessary to assess the accuracy of a face recognition system. Generally, face recognition systems can be configured to allow for a greater or lesser number of matches. A greater number of matches would generally increase the detection rate, but would also increase the false positive rate. Similarly, a lesser number of matches would decrease the false positive rate, but would also decrease the detection rate. Reporting a detection rate of 86 percent without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy.

[25]The term "positive identification" means a determination, based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record. See 34 U.S.C. § 40316.

FBI Agreed to Conduct Annual Operational Reviews of NGI-IPS but Implementation Is Incomplete

We reported in May 2016 that FBI, DOJ, and OMB guidance all required annual reviews of operational information technology systems to assess their abilities to continue to meet cost and performance goals.[26] For example, the FBI's Information Technology Life Cycle Management Directive required an annual operational review to ensure that the fielded system is continuing to support its intended mission, among other things.

In May 2016, we reported that the FBI had not assessed the accuracy of face recognition searches of NGI-IPS in its operational setting—the setting in which enrolled photos, rather than a test database of photos are used to conduct a search for investigative leads. According to FBI officials, at the time of our May 2016 review, the database of photos used in its tests was representative of the photos in NGI-IPS, and ongoing testing in a simulated environment was adequate. However, according to the National Institute of Standards and Technology, as the size of a photo database increases, the accuracy of face recognition searches performed on that database can decrease due to lookalike faces.[27] At the time of our review, FBI's test database contained 926,000 photos while NGI-IPS contained about 30 million photos. We concluded that by conducting an operational review of these systems, FBI officials would obtain information regarding what factors affect the accuracy of the face recognition searches, such as the quality of the photos in the database, and if NGI-IPS is meeting federal, state, and local law enforcement needs. As a result, we recommended the FBI conduct an operational review of NGI-IPS, at least annually, that includes an assessment of the accuracy of face recognition searches and take actions, as necessary, to improve the system.

In May 2016, DOJ concurred with this recommendation and has taken steps to seek input from its users. For example, the FBI submitted a staff paper through the fall 2016 Advisory Policy Board Process to solicit feedback from its users. Specifically, officials said the paper requested feedback on whether the face recognition searches of the NGI-IPS are

[26]See FBI, *FBI Information Technology Life Cycle Management Directive*, version 3.0 (August 19, 2005); DOJ, *Systems Development Life Cycle Guidance* (Jan. 2003); and OMB, *Circular No. A-11, Planning, Budgeting, and Acquisition of Capital Assets*, V 3.0 (2015).

[27]National Institute of Standards and Technology, *Face Recognition Vendor Test: NIST Interagency Report 8009* (May 26, 2014).

meeting their needs, and input regarding search accuracy.[28] According to FBI officials, no users expressed concern with any aspect of the NGI-IPS meeting their needs, including accuracy. DOJ reported that it repeated this process in the fall of 2017.

Although FBI's action of providing working groups with a paper presenting our recommendation is a positive step, FBI's actions do not fully meet the recommendation. FBI's paper was presented as informational, and did not result in any formal responses from users. We disagree with FBI's conclusion that receiving no responses on the informational paper fulfills the operational review recommendation, which includes determining that NGI-IPS is meeting user's needs. In addition, in May 2019, the FBI stated that it will be working with the National Institute of Standards and Technology on annual operational testing and that such testing meets the intention of this recommendation. However, the proposed testing, while promising, will not occur in an operational environment. As such, we continue to believe the FBI should conduct an operational review of NGI-IPS at least annually, as we recommended.

FBI Has Not Assessed the Accuracy of External Partners' Face Recognition Systems Used by FACE Services

In May 2016 we reported that FBI officials had not assessed the accuracy of face recognition systems operated by external partners. Specifically, before agreeing to conduct searches on, or receive search results from, these systems, the FBI did not ensure the accuracy of these systems was sufficient for use by FACE Services. *Standards for Internal Control in the Federal Government* calls for agencies to design and implement components of operations to ensure they meet the agencies mission, goals, and objectives, which, in this case, is to identify missing persons, wanted persons, suspects, or criminals for active FBI investigations. As a result, we recommended the FBI take steps to determine whether each external face recognition system used by FACE Services is sufficiently accurate for the FBI's use and whether results from those systems should be used to support FBI investigations.

In comments on our draft report in 2016, and reiterated during subsequent recommendation follow-up, DOJ officials did not concur with this recommendation. DOJ officials stated that the FBI has no authority to set or enforce accuracy standards of face recognition technology

[28]The FBI's Advisory Policy Board is responsible for reviewing appropriate policy, technical, and operational issues related to the FBI's CJIS programs.

operated by external agencies. In addition, DOJ officials stated that the FBI has implemented multiple layers of manual review that mitigate risks associated with the use of automated face recognition technology. Further, DOJ officials stated there is value in searching all available external databases, regardless of their level of accuracy.

We acknowledge that the FBI cannot and should not set accuracy standards for the face recognition systems used by external partners. We also agree that the use of external face recognition systems by the FACE Services Unit could add value to FBI investigations. However, we disagree with DOJ and continue to believe that the FBI should assess the quality of the data it is using from state and federal partners. We also disagree with the DOJ assertion that manual review of automated search results is sufficient. Even with a manual review process, the FBI could miss investigative leads if a partner does not have a sufficiently accurate system. The FBI has entered into agreements with state and federal partners to conduct face recognition searches using hundreds of millions of photos. Without assessments of the results from its state and federal partners, the FBI is making decisions to enter into agreements based on assumptions that the search results may provide valuable investigative leads. For example, the FBI's accuracy requirements for criminal investigative purposes may be different than a state's accuracy requirements for preventing driver's license fraud.[29] By relying on its external partners' face recognition systems, the FBI is using these systems as a component of its routine operations and is therefore responsible for ensuring the systems will help meet the FBI's mission, goals and objectives. Until FBI officials can assure themselves that the data they receive from external partners are reasonably accurate and reliable, it is unclear whether such agreements are beneficial to the FBI, whether the investment of public resources is justified, and whether photos of innocent people are unnecessarily included as investigative leads.

[29]We reported in 2012 that 41 states and the District of Columbia use face recognition technology to detect fraud in driver's license applications by ensuring an applicant does not obtain a license by using the identity of another individual and has not previously obtained licenses using a different identity or identities. See GAO, *Driver's License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*, GAO-12-893 (Washington, D.C.: Sept. 21, 2012).

Chairman Cummings, Ranking Member Jordan, and Members of the Committee, this concludes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Gretta Goodwin at (202) 512-8777 or GoodwinG@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Dawn Locke (Assistant Director), Jason Jackson (Analyst-In-Charge), Jennifer Beddor, Ann Halbert-Brooks, Eric Hauswirth, Paul Hobart, Richard Hung, Susanna Kuebler, Kay Kuhlman, Tom Lombardi, and Dina Shorafa. Key contributors for the previous work that this testimony is based on are listed in the previously issued product.