United States Government Accountability Office

Testimony

Before the Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 11:00 a.m. ET
Wednesday, June 29, 2022

FACIAL RECOGNITION TECHNOLOGY

Federal Agencies' Use and Related Privacy Protections

Statement of Candice N. Wright

Accessible Version

GAO-22-106100

GAO Highlights

Highlights of GAO-22-106100, a testimony before the Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives

June 29, 2022

FACIAL RECOGNITION TECHNOLOGY

Federal Agencies' Use and Related Privacy Protections

Why GAO Did This Study

Use of FRT has become increasingly common across the government and private sector. As the use of FRT continues to expand, advocacy organizations and others have highlighted the importance of understanding FRT uses in federal agencies and related privacy risks.

This statement describes (1) use of FRT at federal agencies and (2) privacy protections present in FRT systems used by federal agencies.

This statement is based on recent GAO reports on the use of FRT, including (1) an August 2021 report on current and planned use of FRT across federal agencies that included a survey of the 24 largest agencies, (2) a June 2021 report on federal law enforcement agencies' use of FRT that included a survey administered to 42 agencies that employ law enforcement officers, and (3) a 2020 report on use of FRT for airport and port security. To conduct this prior work, GAO reviewed relevant documents and interviewed agency officials.

What GAO Recommends

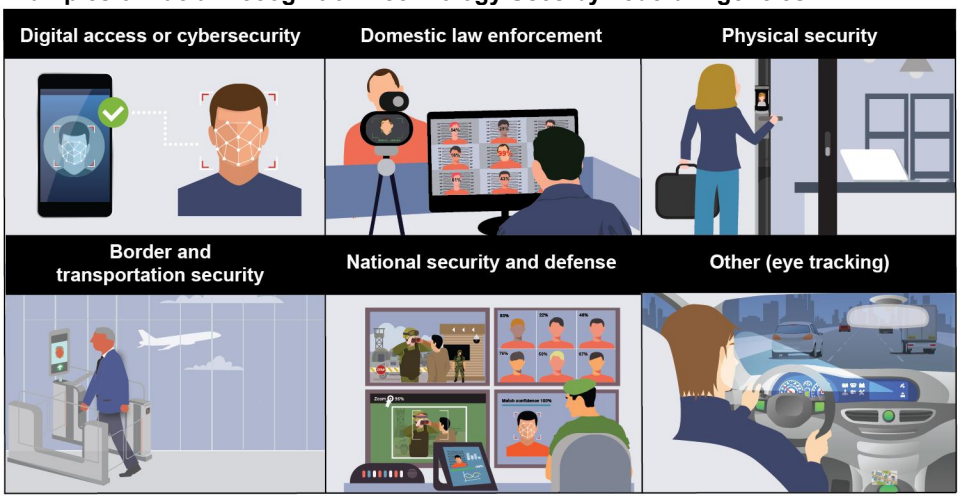
In prior reports, GAO made recommendations to 13 agencies to implement a mechanism to track use of non-federal systems by employees and assess the risks of these systems and to CBP to develop and implement a plan to conduct privacy audits of its partners, among others. Agencies generally concurred with the recommendations. Three agencies have implemented mechanisms to track non-federal systems, but have not yet assessed the risks of using such systems. CBP has conducted some, but not all, privacy audits of its partners.

View GAO-22-106100. For more information, contact Candice N. Wright at (202) 512-6888 or wrightc@gao.gov

What GAO Found

In August 2021, GAO reported its survey results on facial recognition technology (FRT) activities, which found that 18 of 24 agencies reported using FRT for one or more purposes, with digital access and domestic law enforcement as the most common. For example, two agencies reported testing FRT to verify identities of persons accessing government websites and other agencies used FRT to generate leads in criminal investigations. Agencies also reported accessing FRT systems of other entities, such as those owned by other federal agencies, state and local governments, and the private sector. In addition, ten agencies reported conducting or supporting FRT-related research and development. For example, the Department of Justice reported conducting applied research on the relationship between skin tone and false match rates in facial recognition algorithms, among other efforts.

Examples of Facial Recognition Technology Uses by Federal Agencies



Source: GAO analysis of survey results and GoldenSikora/metamorworks/Cipta/stock.adobe.com. | GAO-22-106100

In June 2021, GAO reported the results of another survey of 42 federal agencies that employ law enforcement officers. Fourteen agencies reported using FRT to support criminal investigations; however, GAO found that 13 of these agencies did not track employee use of non-federal (e.g., state and commercial) FRT systems. For example, one agency conducted a poll and learned that its employees had used a non-federal system to conduct more than 1,000 facial recognition searches. The lack of awareness about employees' use of non-federal FRT systems can have privacy implications—including a risk of not adhering to privacy laws or that system owners may share sensitive information used for searches. In September 2020, GAO also found that U.S. Customs and Border Protection's (CBP) Biometric Entry-Exit Program incorporated some privacy protections, but the implementation of privacy notices and audits were inconsistent. For example, CBP had audited only one of its more than 20 commercial airline partners and did not have a plan to audit all its partners for compliance with the program's privacy requirements.

Chairman Foster, Ranking Member Obernolte, and members of the Subcommittee:

I am pleased to be here today to discuss the federal government's use of facial recognition technology (FRT). Use of this technology has become increasingly common across the government and private sector. As the use of FRT continues to expand, Members of Congress, academics, and advocacy organizations have highlighted the importance of developing a comprehensive understanding of how it is used by federal agencies. In addition, use of the technology has raised concerns about its accuracy and the privacy implications.

My statement today will focus on (1) use of FRT at federal agencies and (2) privacy protections present in FRT systems used by federal agencies. This statement is based on findings from a series of recent reports we have issued on FRT.[1] In August 2021, we reported on current and planned uses of FRT systems within the federal government, which included a survey of 24 Chief Financial Officers Act agencies.[2] In June 2021, we reported on the use of FRT systems by federal law enforcement agencies, which included a survey to 42 federal agencies that employ law enforcement officers. In September 2020, we reported on use of FRT for airport and port security. For each of these reports, we reviewed program documents and interviewed relevant officials. These reports provide detailed descriptions of our scope and methodology.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. These 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.

[1]GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526 (Washington, D.C.: Aug. 24, 2021); GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington, D.C.: Jun. 3, 2021); GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, D.C.: Sep. 2, 2020).

[2]The 24 agencies are those identified in the Chief Financial Officers Act of 1990, as amended (31 U.S.C. § 901(b)) (2018).

Background

How Facial Recognition Technology Works

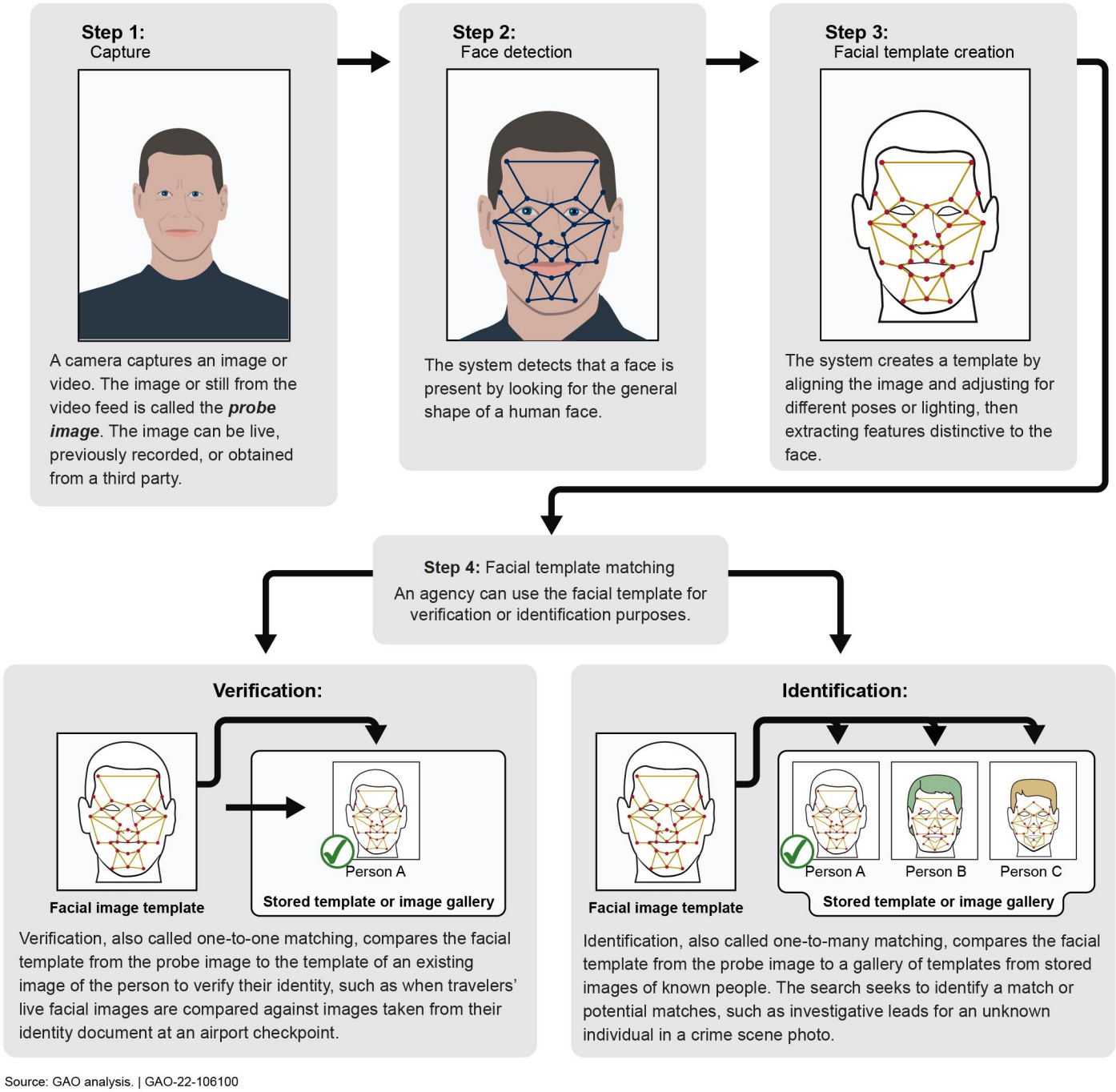
Facial recognition is one of several biometric technologies that identify individuals by measuring and analyzing physical and behavioral characteristics.[3] FRT uses a photo or a still from a video feed of a person—often called a probe or live photo—and converts it into a template, or a mathematical representation of the photo. A matching algorithm can then compare the template to one from another photo and calculate their similarity.

Facial recognition searches or comparisons generally fall into two categories: verification and identification (see figure 1). Verification (or one-to-one searches) compares a stored photo of an individual to another photo purportedly of the same individual to determine whether they are the same person. Identification (or one-to-many searches) compares a photo from a single individual against a gallery of stored photos from a number of individuals to determine if there is a potential match.[4]

[3]Other biometric technologies can identify individuals by measuring and analyzing physical and behavioral characteristics, which include fingerprints, eye irises, voice, and gait.

[4]Two technologies, facial detection and facial analysis, are related to, but distinct from, facial recognition. Facial detection determines if a photo or video contains a face in the image. Facial analysis (sometimes referred to as facial classification or characterization) uses a facial image to estimate or classify personal characteristics such as age, race, or sex. We use the term “facial recognition technology” to include facial recognition, facial detection, or facial analysis technologies.

Figure 1: Process Used in Facial Recognition Technology



Source: GAO analysis. | GAO-22-106100

Text of Figure 1: Process Used in Facial Recognition Technology

1) Step 1 Capture:
   A camera captures an image or video. The image or still from the video feed is called the probe image. The image can be live, previously recorded, or obtained from a third party.

2) Step 2 Facial Recognition:
   The system detects that a face is present by looking for the general shape of a human face.

3) Step 3 Facial template creation:
   The system creates a template by aligning the image and adjusting for different poses or lighting, then extracting features distinctive to the face.

4) Step 4 Facial template matching:
   An agency can use the facial template for verification or identification purposes.

   a) Verification
      Verification, also called one-to-one matching, compares the facial template from the probe image to the template of an existing image of the person to verify their identity, such as when travelers' live facial images are compared against images taken from their identity document at an airport checkpoint.

   b) Identification
      Identification, also called one-to-many matching, compares the facial template from the probe image to a gallery of templates from stored images of known people. The search seeks to identify a match or potential matches, such as investigative leads for an unknown individual in a crime scene photo.

Privacy Principles and Requirements

Federal agency collection and use of personal information, including facial images, is governed primarily by the Privacy Act of 1974[5] and the

[5]See Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2018)). The act generally prohibits (with a number of exceptions) the disclosure by federal entities of records about an individual without the individual's written consent and provides U.S. persons with a means to seek access to and amend their records.

privacy provisions of the E-Government Act of 2002.[6] The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[7] The Privacy Act requires that when agencies establish or make changes to a system of records, they must publish a notice—known as a System of Records Notice—in the Federal Register. The notice is to identify, among other things, the types of data collected, the types of individuals about whom information was collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information.

Further, the E-Government Act requires agencies to conduct, where applicable, privacy impact assessments (PIA) that analyze how personal information is collected, stored, shared, and managed in a federal system. Agencies are required to make their PIAs publicly available, if practicable. Further according to Office of Management and Budget (OMB) officials, the Privacy Act and OMB Circular A-130 generally provide that agencies must ensure that privacy requirements apply to systems operated by contractors or other entities on behalf of the Federal Government, which could include facial recognition service providers.[8] Agencies also have their own privacy policies that govern use of FRT. For example, the Department of Homeland Security privacy policies require adherence to the Fair Information Practice Principles (FIPP), which provides a framework for balancing the need for privacy with other public policy interests, such as national security and law enforcement.[9]

[6]Pub. L. No. 107-347, title II, § 208, 116 Stat. 2899, 2921-23 (2002) (codified at 44 U.S.C. § 3501 note (2018)).

[7]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).

[8]Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130 (July 28, 2016).

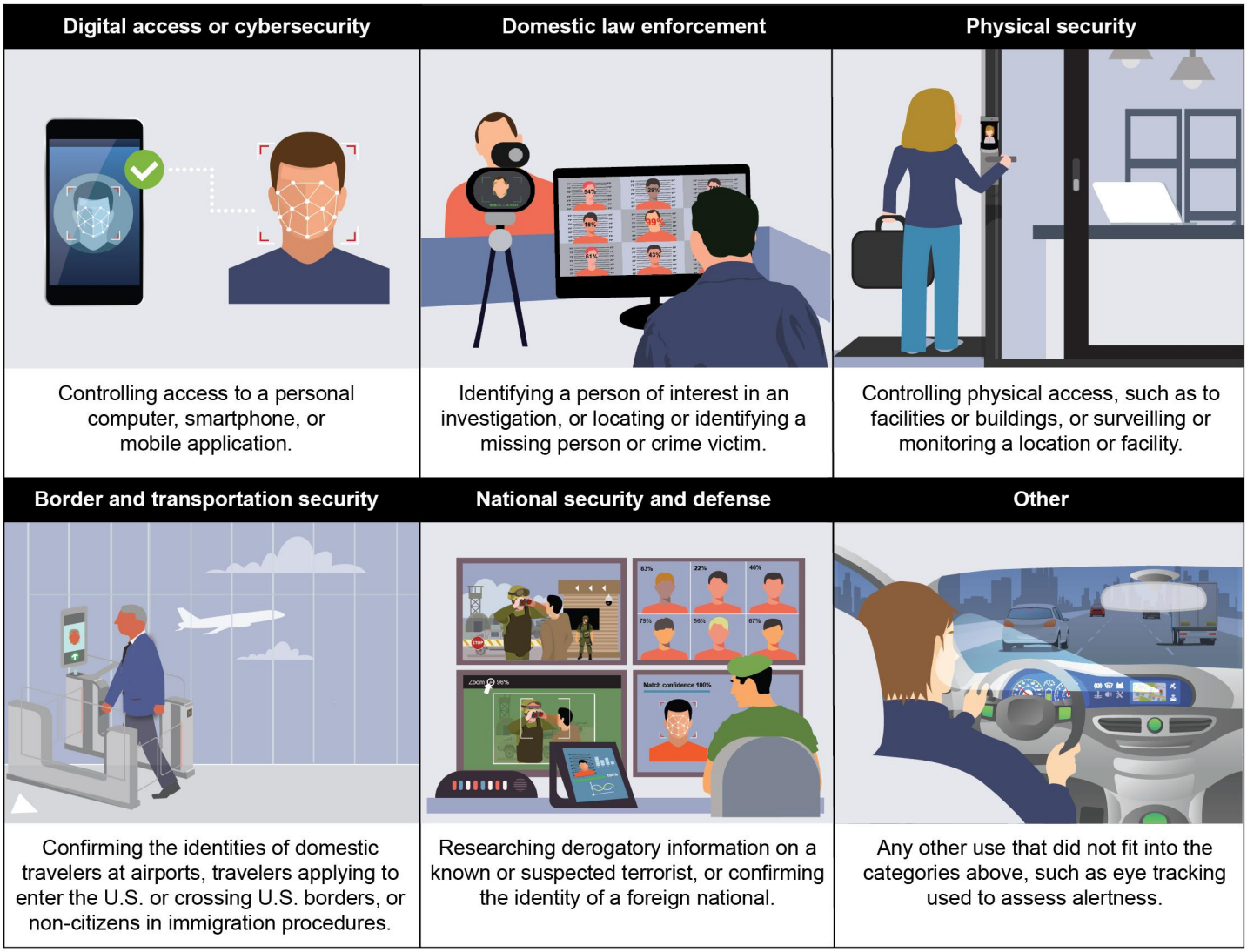
[9]The Fair Information Practice Principles include the following nine principles: access and amendment, accountability, authority, minimization, quality and integrity, individual participation, purpose specification and use limitation, security, and transparency.

Agencies Reported Using FRT for Multiple Purposes and Have Plans to Expand Its Use

Agencies Reported Various Uses of FRT

FRT systems are used for a variety of purposes across the federal government. These purposes can be grouped into several different categories. Figure 2 provides illustrative examples of these purposes.

Figure 2: Purposes and Examples of Federal Agencies' Use of Facial Recognition Technology



Source: GAO analysis of survey results and GoldenSikora/metamorworks/Cipta/stock.adobe.com. | GAO-22-106100

Text of Figure 2: Purposes and Examples of Federal Agencies' Use of Facial Recognition Technology

- Digital access or cybersecurity:
  Controlling access to a personal computer, smartphone, or mobile application.

- Domestic law enforcement
  Identifying a person of interest in an investigation, or locating or identifying a missing person or crime victim.
- Physical security
  Controlling physical access, such as to facilities or buildings, or surveilling or monitoring a location or facility.
- Border and transportation security
  Confirming the identities of domestic travelers at airports, travelers applying to enter the U.S. or crossing U.S. borders, or non-citizens in immigration procedures.
- National security and defense
  Researching derogatory information on a known or suspected terrorist, or confirming the identity of a foreign national.
- Other
  Any other use that did not fit into the categories above, such as eye tracking used to assess alertness.

Eighteen of the 24 agencies we surveyed reported using FRT in fiscal year 2020 for one or more of these purposes, with digital access and domestic law enforcement as the most common (see table 1).

Table 1: Reported Purposes of Facial Recognition Technology Systems Used by Federal Agencies in Fiscal Year 2020

Federal Agency	Digital access	Domestic law enforcement	Physical security	Border and transportation security	National security and defense	Other
Department of Agriculture	Yes	No	No	No	No	No
Department of Commerce	Yes	No	Yes	No	No	No
Department of Defense	No	Yes	Yes	No	Yes	Yes
Department of Energy	Yes	No	Yes	No	No	No
Department of Health and Human Services	Yes	Yes	Yes	No	No	No
Department of Homeland Security	Yes	Yes	No	Yes	Yes	No
Department of the Interior	Yes	Yes	No	No	No	No
Department of Justice	Yes	Yes	Yes	No	Yes	Yes
Department of State	No	No	No	Yes	Yes	No
Department of the Treasury	Yes	Yes	No	No	No	No
Department of Veterans Affairs	Yes	No	No	No	No	No
Agency for International Development	Yes	No	No	No	No	No
Environmental Protection Agency	Yes	No	No	No	No	No
General Services Administration	Yes	No	No	No	No	No
National Aeronautics and Space Administration	Yes	No	No	No	No	Yes
National Science Foundation	Yes	No	No	No	No	No
Office of Personnel Management	Yes	No	No	No	No	No
Social Security Administration	Yes	No	No	No	No	No

Source: GAO analysis of survey results. | GAO-22-106100

Examples of how agencies used FRT for selected purpose categories are described below.

- **Digital access or cybersecurity.** Sixteen agencies reported using FRT for digital access or cybersecurity purposes.[10] Of these, 14 agencies authorized personnel to use FRT to unlock their agency-issued smartphones—the most common purpose of FRT reported. Two agencies—General Services Administration and Social Security Administration—also reported testing FRT to verify identities of persons accessing government websites.
- **Domestic law enforcement.** Six agencies reported using FRT to generate leads in criminal investigations, such as identifying a person of interest, by comparing their image against mugshots. In some

[10]The Department of the Treasury did not disclose in its survey responses an additional digital access use of a commercial FRT system and was not included in our analysis.

cases, agencies identify crime victims, such as exploited children, by using commercial systems that compare against publicly available images, such as from social media.

- **Physical security.** Five agencies reported using FRT to monitor or surveil locations to determine if an individual is present, such as someone on a watchlist, or to control access to a building or facility. For example, one agency used it to monitor live video for persons on watchlists and to alert security personnel to these persons without needing to memorize them.

Eighteen Agencies Reported Owning or Accessing FRT

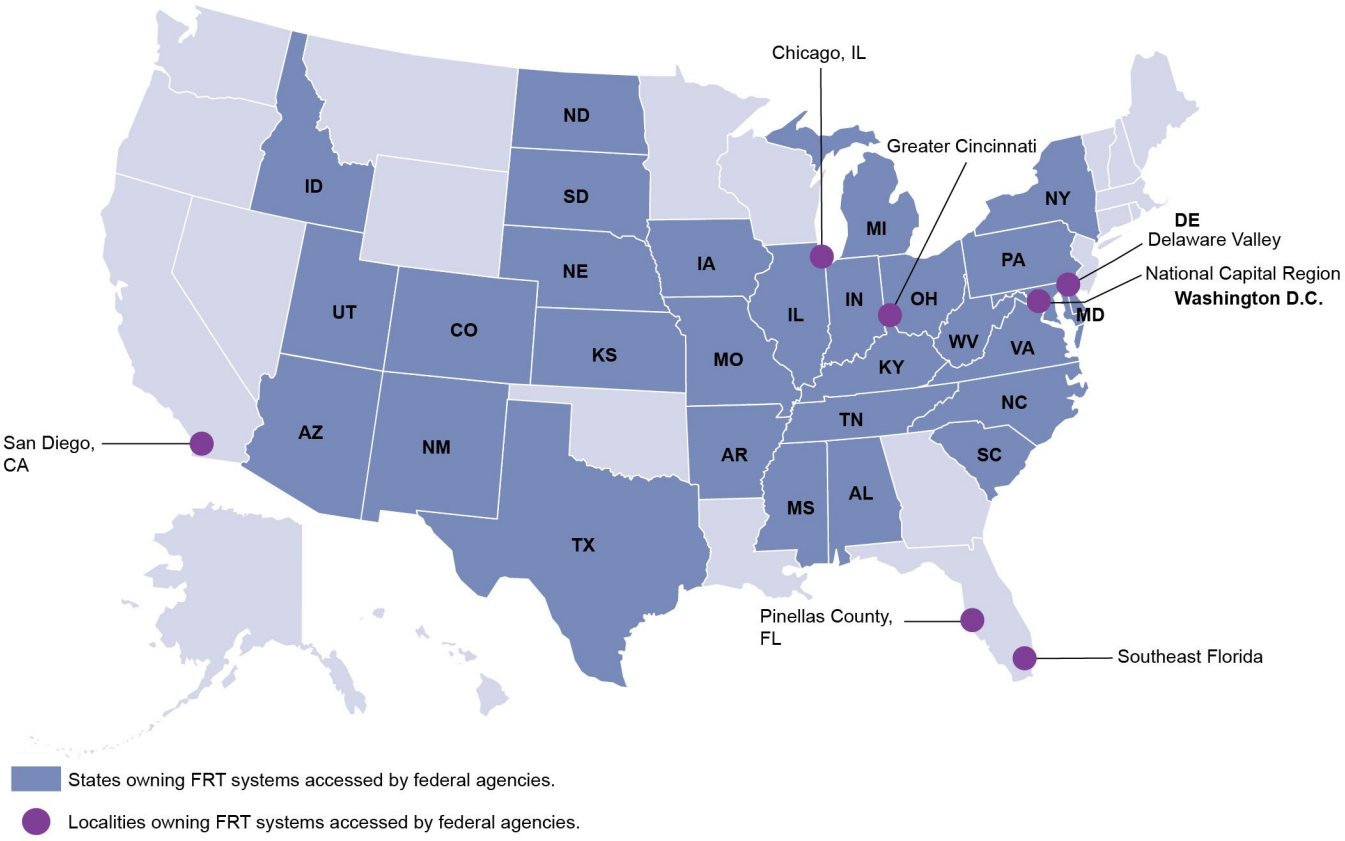
Federal agencies can own their FRT systems or access the FRT systems of other government entities, including federal, state, local, tribal, and territorial governments and commercial facial recognition service providers. Agencies can have direct access to an FRT system or indirect access through requesting a third party run a facial recognition search on behalf of the federal agency.

- **Federal FRT systems.** Seventeen agencies reported that they owned or accessed 27 federal FRT systems. Fourteen of these agencies owned smartphones that can be unlocked with facial recognition and nine of these agencies reported owning FRT systems other than smartphones for physical security and domestic law enforcement purposes, among others.[11] One agency did not own an FRT system, but accessed federal and commercially owned systems.[12]
- **State and local FRT systems.** Three agencies reported accessing one or more FRT systems owned by 29 states and seven localities for law enforcement purposes. Figure 3 shows the states and localities that own FRT systems accessed by these federal agencies.

[11]For summaries of selected federal agencies' FRT activities, see our August 2021 report, GAO-21-526.

[12]The Department of the Treasury reported it accessed the General Services Administration's login.gov during testing of the FRT capability. Login.gov is a single sign-on mechanism that uses FRT to match applicants to their identification documents to access accounts on agency websites. Treasury also reported a third-party vendor performed facial recognition searches on its behalf in April 2020.

Figure 3: States and Localities that Own Facial Recognition Technology (FRT) Systems Accessed by Federal Agencies in Fiscal Year 2020



Source: GAO analysis of survey responses. | GAO-22-106100

- **Commercial FRT systems.** Six agencies reported accessing eight FRT systems owned by commercial vendors, mostly for domestic law enforcement purposes. Four agencies accessed Clearview AI, which conducts facial recognition searches using publicly available images. For example, the Office of the Inspector General within the Department of Health and Human Services reported it began a pilot of Clearview AI in September 2020 to assist with identifying subjects of a criminal investigation.

Agencies Reported Conducting or Supporting FRT-related Research and Development

Based on our analysis, 10 of the 24 agencies surveyed conducted or supported research and development (R&D) for FRT in fiscal year 2020. These agencies include the Departments of Commerce, Defense, Homeland Security, Health and Human Services, Justice, State, Transportation, and Veterans Affairs, the National Aeronautics and Space Administration (NASA), and the National Science Foundation (NSF).

R&D to Address Agency Specific Needs

Four agencies—the Departments of Defense, Homeland Security, Justice, and State—generally focused their R&D on agency-specific needs, such as to develop new applications or improve existing capabilities. Examples from some of these agencies include:

- The Department of Homeland Security reported sponsoring Biometric Technology Rallies, which are ongoing events that challenge industry to develop innovative solutions for biometric collection and matching, including facial recognition. For example, the 2020 Rally focused on the ability of FRT systems to reliably collect or match images of individuals wearing masks.
- The Department of Justice reported conducting applied research on the relationship between skin tone and false match rates in facial recognition algorithms, the capabilities and limitations of current synthetic face detection, such as deepfakes, and the development of software to detect synthetic faces.[13] It also explored the potential benefits of combining FRT systems with trained forensic examiners to achieve better matching performance than by the technology or by humans alone.

R&D to Support Broad Research Goals and Other Efforts

Two agencies—Commerce and NSF—conducted or supported FRT-related research more broadly, including for commercial vendors and other agencies. For example, Commerce reported that its National Institute of Standards and Technology (NIST) conducted research

[13]For more information on deepfakes, see GAO, *Science & Tech Spotlight: Deepfakes*, GAO-20-379SP (Washington, D.C.: Feb. 20, 2020).

through its Face Recognition Vendor Test program. NIST most recently released reports from this program quantifying facial recognition accuracy across demographic characteristics and the use of face masks.[14] NSF reported that it awards grants to universities and others to conduct research on facial recognition. Specifically, NSF's Directorate for Computer and Information Science and Engineering supported FRT-related research, including a project assessing how to prevent identifying an individual from facial images used in research, such as recordings of a driver's face during driver behavior studies.

Further, four agencies—the Departments of Health and Human Services, Transportation, and Veterans Affairs, and NASA—reported using FRT as a tool to conduct other research. For example, Transportation reported that the Federal Railroad Administration used eye tracking to study alertness in train operators. Similarly, NASA also reported that it used eye tracking to conduct human factors research. In addition, the Department of Veterans Affairs reported it used eye tracking as part of a clinical research program that treats post-traumatic stress disorder in veterans.

Ten Agencies Plan to Expand Use of FRT, Mostly through Use of New FRT Systems

According to our analysis of survey responses, 10 of the 24 agencies surveyed plan to expand their use of FRT systems in one or more ways through fiscal year 2023. These agencies include the Departments of Agriculture, Commerce, Defense, Health and Human Services, Homeland Security, the Interior, Justice, State, the Treasury, and Veterans Affairs. We categorized plans to expand FRT use in three ways: (1) using new FRT systems, (2) evaluating existing FRT systems (e.g., pilot testing), and (3) upgrading existing FRT systems (see table 2). New FRT systems refers to systems that are new to federal agencies and new access to existing FRT systems that agencies did not report using in fiscal year 2020. Three agencies—the Departments of Defense, Homeland Security, and the Treasury—reported plans to conduct new pilot tests or continue evaluating existing FRT systems. One agency, the Department of Homeland Security, reported plans to upgrade an existing FRT system by replacing IDENT, which is its current system for processing and storing

[14]The Department of Homeland Security and the Department of Justice have interagency agreements with the National Institute of Standards and Technology for related FRT research and evaluation.

biometric data, with the Homeland Advanced Recognition Technology system.

Table 2: Federal Agencies That Reported Plans to Expand Their Use of Facial Recognition Technology (FRT) Systems, through Fiscal Year 2023

Federal Agency	Plan to use new FRT systems	Plan to evaluate FRT systems	Plan to upgrade FRT systems or capabilities
Department of Agriculture	Yes	No	No
Department of Commerce	Yes	No	No
Department of Defense	Yes	Yes	No
Department of Health and Human Services	Yes	No	No
Department of Homeland Security	Yes	Yes	Yes
Department of the Interior	Yes	No	No
Department of Justice	Yes	No	No
Department of State	Yes	No	No
Department of the Treasury	Yes	Yes	No
Department of Veterans Affairs	Yes	No	No

Source: GAO analysis of survey results. | GAO-22-106100

Federal Efforts to Assess and Mitigate Privacy Risks of FRT

Most Agencies Accessing Non-Federal Systems Did Not Track Use or Assess Related Privacy Risks

In 2021, we reported the results of another survey on FRT, and found that 14 of the 42 federal agencies we surveyed had used non-federal systems to support criminal investigations.[15] Most federal agencies that reported using non-federal systems did not own systems. Thus, employees were relying on systems owned by other entities, including non-federal entities, to support their operations.

Thirteen of the 14 agencies that reported use of non-federal FRT systems did not have complete, up-to-date information on what non-federal systems were used by employees because they did not track this

[15]GAO-21-518. We surveyed 42 federal agencies that employed law enforcement officers. We defined law enforcement officers as full-time employees with federal arrest authority and who are authorized to carry firearms while on duty.

information.[16] These agencies had therefore not fully assessed the potential risks of using these systems, such as risks related to privacy. These agencies reported not having a mechanism to track what non-federal systems were used by employees. For example, when we requested information from one agency about its use of non-federal systems, agency officials told us they had to poll field division personnel because the information was not maintained by the agency. These agency officials also told us that the field division personnel had to work from their memory about their past use of non-federal systems, and that they could not ensure we were provided comprehensive information about the agency's use of non-federal systems. Officials from another agency initially told us that employees did not use non-federal systems; however, after conducting a poll, the agency learned that its employees had used a non-federal system to conduct more than 1,000 facial recognition searches.

One agency–the U.S. Immigration and Customs Enforcement–reported that it was in the process of implementing a mechanism to track what non-federal systems are used by employees (see table 3).[17] According to U.S. Immigration and Customs Enforcement officials, in November 2020 they were in the process of developing a list of approved facial recognition technologies that employees can use.

[16]By complete, up-to-date information, we mean that an agency has ongoing knowledge of what non-federal systems with FRT are used by employees. By non-federal systems, we are referring to systems owned by state, local, tribal, territorial, and non-government entities.

[17]According to U.S. Immigration and Customs Enforcement officials, they had only planned to subject employees within its Homeland Security Investigations to the procedures, as only employees within this component of the agency were using FRT.

Table 3: Federal Agency Tracking of Employee Use of Non-Federal Systems with Facial Recognition Technology, as of June 2021

Federal agency	Have mechanism to track what non-federal systems are used by employees
U.S. Immigration and Customs Enforcement	Yes
Bureau of Alcohol, Tobacco, Firearms, and Explosives	No
Bureau of Diplomatic Security	No
U.S. Capitol Police	No
U.S. Customs and Border Protection	No
Drug Enforcement Administration	No
Federal Bureau of Investigation	No
U.S. Fish and Wildlife Service	No
Food and Drug Administration, Office of Criminal Investigations	No
Internal Revenue Service, Criminal Investigation Division	No
U.S. Marshals Service	No
U.S. Park Police	No
U.S. Postal Inspection Service	No
U.S. Secret Service	No

Source: GAO analysis of agency information. | GAO-22-106100

Notes: Federal agencies marked “No” may have known that employees used certain systems, but they do not have a mechanism to provide complete, up-to-date information of what systems are used by employees. This information is from June 2021, and since then, three agencies have implemented mechanisms to track employee use of non-federal systems.

Numerous privacy risks to federal agencies and the public can accompany the use of FRT. When agencies use FRT without first assessing the privacy implications and applicability of privacy requirements, there is a risk that they will not adhere to privacy-related laws, regulations, and policies. There is also a risk that non-federal system owners will share sensitive information (e.g. photo of a suspect) about an ongoing investigation with the public or others. In addition, privacy advocacy organizations, government agencies, academics, and some industry representatives have raised privacy and security concerns. For example, there is a risk that data sets with personal information could be subject to breaches, resulting in sensitive biometric data being revealed to unauthorized entities. Because a person’s face is distinctive, permanent, and therefore irrevocable, a breach involving data derived from a face may have more serious consequences than the breach of other information, such as passwords, which can be changed.

However, as of June 2021, 13 federal agencies could not fully assess the risks of using non-federal systems because they did not have complete,

up-to-date information on what systems are actually used by employees.[18] Therefore, we recommended that these 13 agencies: (1) implement a mechanism to track what non-federal systems with FRT are used by employees to support investigative activities; and (2) after implementing a mechanism to track non-federal systems, assess the risks of using such systems, including privacy and accuracy-related risks.

These agencies generally concurred with our recommendations.[19] As of April 2022, three of 13 agencies implemented at least one of our two recommendations.[20] By implementing a mechanism to track what non-federal systems are used by employees, agencies will have better visibility into the technologies they rely upon to conduct criminal investigations. In addition, by assessing the risks of these systems, including privacy and accuracy-related risks, agencies will be better positioned to mitigate any risks to themselves and the public.

TSA Incorporated Privacy Protections for its FRT Pilot Tests, While CBP Had Inconsistencies in its Approach

In 2020, we reported on steps that the Transportation Security Administration (TSA) and U.S. Customs and Border Protection (CBP) took to implement privacy protections in its programs.[21] TSA conducted a series of pilot tests that began in 2017 to assess the feasibility of using FRT for traveler identity verification at airport security checkpoints. CBP's Biometric Entry-Exit Program integrates biographic and biometric records of foreign nationals entering and exiting the country and identifies overstays. While we found that TSA's facial recognition pilot tests incorporated privacy protections consistent with the FIPPs, we identified limitations in CBP's privacy notices to inform the public of facial

[18]We asked agencies whether they had a mechanism to track *what systems* were used by employees, not whether agencies track *each individual use of a system* by employees.

[19]We made recommendations to 13 of the 42 federal agencies that we surveyed. These 13 agencies are located within eight federal department and entities (i.e. entities), and these eight entities generally concurred with our recommendations.

[20]The U.S. Secret Service, U.S. Fish and Wildlife Service, and the Food and Drug Administration each implemented the recommendation to implement a mechanism to track what non-federal systems with FRT are used by employees to support investigative activities.

[21]GAO-20-568.

recognition use and inconsistency in audits conducted on commercial airline partners to determine compliance with privacy requirements.[22]

In our September 2020 report, we found that CBP's Biometric Entry-Exit Program incorporated some privacy protection principles, but privacy notices and audits were inconsistent. The FIPPs of transparency and individual participation state that individuals should be provided with clear, readable, and comprehensive notices about how their personally identifiable information will be used and have the opportunity to decline to participate if appropriate. However, we found that CBP's notices were not always current or complete, provided limited information on how to request to opt out of facial recognition, and were not always available. In addition, CBP required its commercial partners, as well as contractors and vendors, to follow CBP's data collection and privacy requirements, such as restrictions on retaining or using traveler photos. CBP can conduct audits to assess compliance with these requirements. However, as of May 2020, CBP had audited only one of its more than 20 commercial airline partners and did not have a plan to ensure that all partners are audited for compliance with the program's privacy requirements.

Therefore in September 2020 we recommended that CBP: (1) ensure that the Biometric Entry-Exit Program's privacy notices contain complete and current information, including all of the locations where facial recognition is used and how travelers can request to opt out as appropriate; (2) ensure that the Biometric Entry-Exit Program's privacy signage is consistently available at all locations where CBP is using facial recognition; (3) direct the Biometric Entry-Exit Program to develop and implement a plan to conduct privacy audits of its commercial partners', contractors', and vendors' use of personally identifiable information.

The Department of Homeland Security concurred with our recommendations. As of February 2022, CBP has implemented the recommendation on ensuring that the Biometric Entry-Exit Program's privacy notices contain complete and current information. CBP has taken steps to address the remaining two recommendations but has not fully implemented them. CBP reported that it developed a plan to ensure privacy signage for the Biometric Entry-Exit program is consistently available at all locations where FRT is used. Fully implementing our

[22]GAO-20-568. In September 2020, we reported that given the limited nature of these pilot tests, it was too early to conduct a full assessment of TSA's compliance with privacy protection principles.

recommendation would help give travelers the opportunity to decline to participate, if appropriate, and help CBP improve transparency with the travelling public about how it uses personally identifiable information. Further, CBP has conducted some assessments of its commercial partners at two ports of entry to ensure that they are adhering to CBP's requirements to protect travelers' privacy. CBP would be better positioned to protect travelers' information if it developed and implemented a plan for auditing all partners who have access to personally identifiable information.

Chairman Foster, Ranking Member Obernolte, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgements

If you or your staff have any questions about this testimony, please contact Candice Wright, Director, Science, Technology Assessment, and Analytics at (202) 512-6888 or WrightC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Richard Hung (Assistant Director), Sean Manzano (Analyst-In-Charge), Jehan Chase, Jeffrey Fiore, Gretta Goodwin, Ryan Han, Mark Kuykendall, Grace Kwon, and Monica Perez-Nelson. Key contributors for the previous work that this testimony is based on are listed in the previously issued products.

Related GAO Products

Facial Recognition Technology: Current and Planned Uses by Federal Agencies. GAO-21-526. Washington, D.C.: August 24, 2021.

Forensic Technology: Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcome. GAO-21-435SP. Washington, D.C.: July 6, 2021.

Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks. GAO-21-518. Washington, D.C.: June 3, 2021.

Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues. GAO-20-568. Washington, D.C.: September 2, 2020.

Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses. GAO-20-522. Washington, D.C.: July 13, 2020.

Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy. GAO-16-267. Washington, D.C.: May 16, 2016.

Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law. GAO-15-621. Washington, D.C.: July 30, 2015.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548