United States Government Accountability Office

Testimony

Before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, July 13, 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees

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

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-105309

GAO Highlights

Highlights of GAO-21-105309, a testimony before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, House of Representatives

July 13, 2021

FACIAL RECOGNITION TECHNOLOGY

Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees

Why GAO Did This Study

Federal agencies that employ law enforcement officers use facial recognition technology to assist criminal investigations, among other activities. For example, the technology can help identify an unknown individual in a photo or video surveillance.

This statement describes (1) the ownership and use of facial recognition technology by federal agencies that employ law enforcement officers, (2) the types of activities these agencies use the technology to support, and (3) the extent that these agencies track employee use of facial recognition technology owned by non-federal entities, including the potential privacy and accuracy implications.

This statement is based on GAO's June 2021 report on federal law enforcement's use of facial recognition technology (GAO-21-518). To conduct that prior work, GAO administered a survey questionnaire to 42 federal agencies that employ law enforcement officers regarding their use of the technology. GAO also reviewed relevant documents and interviewed agency officials. The June 2021 report was a public version of a sensitive report that GAO issued in April 2021. Information that agencies deemed sensitive was omitted from the June 2021 report and this statement.

What GAO Recommends

In June 2021, GAO made two recommendations to each of 13 federal agencies to implement a mechanism to track what non-federal systems are used by employees, and assess the risks of using these systems. Agencies generally concurred with the recommendations.

View GAO-21-105309. For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.

What GAO Found

In June 2021, GAO reported the results of its survey of 42 federal agencies that employ law enforcement officers about their use of facial recognition technology. Twenty reported owning systems with the technology or using systems owned by other entities, such as state, local, and non-government entities (see figure).

Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers

Source: GAO analysis of survey data. | GAO-21-105309

Note: For more details, see figure 1 in GAO-21-105309.

Agencies reported using the technology to support several activities (e.g., criminal investigations) and in response to COVID-19 (e.g., verify an individual's identity remotely). Six agencies reported using the technology on images of the unrest, riots, or protests following the killing of Mr. George Floyd in May 2020. Three agencies reported using it on images of the U.S. Capitol attack on January 6, 2021. Agencies said the searches used images of suspected criminal activity.

Fourteen of the 42 agencies reported using the technology to support criminal investigations. However, only one had a mechanism to track what non-federal systems were used by employees. By having a mechanism to track use of these

systems and assessing the related risks (e.g., privacy and accuracy-related risks), agencies can better mitigate risks to themselves and the public.

Chair Jackson Lee, Ranking Member Biggs, and Members of the Subcommittee:

I am pleased to be here to discuss federal law enforcement's use of facial recognition technology. Use of this technology has expanded in recent years, raising concerns about privacy and the accuracy of facial recognition systems. Members of Congress and academics have highlighted the importance of understanding what technologies are owned and how they are used by federal law enforcement.

My statement today will focus on (1) the ownership and use of facial recognition technology by federal agencies that employ law enforcement officers, (2) the types of activities these agencies use the technology to support, and (3) the extent that these agencies track employee use of facial recognition technology owned by non-federal entities, including the potential privacy and accuracy implications. This statement is based on findings from our June 2021 report, which included the results of our survey questionnaire to 42 federal agencies that employ law enforcement officers about their use of the technology.[1] The report provides a detailed description of our scope and methodology.

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.

[1]GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO-21-518 (Washington D.C.: June 3, 2021). Our June 2021 report was a public version of a sensitive report that we issued in April 2021 (GAO-21-243SU). Some federal agencies deemed information in our April 2021 report to be sensitive, which must be protected from public disclosure. Therefore, the June 2021 report and this statement omit sensitive information about federal agency ownership and use of facial recognition technology.

Background

Federal and Non-Federal Systems with Facial Recognition Technology

Federal law enforcement may use systems with facial recognition technology owned by their respective agencies. They may also use systems owned by other government entities, including federal, state, local, tribal, and territorial government entities. Moreover, federal law enforcement may use non-government facial recognition service providers, such as Vigilant Solutions and Clearview AI. For example, law enforcement officers with a Clearview AI account may use a computer or smartphone to upload a photo of an unknown individual to Clearview AI's facial recognition system. The system can return search results that show potential photos of the unknown individual, as well as links to the site where the photos were obtained (e.g., Facebook).

In some cases, law enforcement officers can access another entity's system and conduct a facial recognition search. Alternatively, law enforcement officers can request that another entity use its system to conduct facial recognition searches on their behalf. For example, federal law enforcement officers may ask a state police department to conduct facial recognition searches on their behalf.

Privacy Laws and Rules

Several statutory requirements govern the protection of personal information by federal agencies, including federal law enforcement's use of facial images. The Privacy Act of 1974 places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records (e.g. photos). 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.

Accuracy of Facial Recognition Technology

The accuracy of facial recognition technology can be characterized in a number of ways. For example, a false positive rate is how often the

technology incorrectly declares two images to be a match when they are actually from two different people. In addition, a false negative rate is how often the technology fails to declare two images to be a match when they are actually from the same person. Matching errors can be caused not only by the quality of the facial recognition technology, but also by the quality of the photos used in the matching process and other factors. The National Institute of Standards and Technology has conducted research into the accuracy of facial recognition algorithms. It has evaluated hundreds of commercial facial matching algorithms for accuracy and speed since 2000.

Twenty Federal Agencies Reported Owning or Using Systems with Facial Recognition Technology

We surveyed 42 federal agencies that employ law enforcement officers, 20 of which reported that they owned a system with facial recognition technology or used another entity's system.[2] As shown in figure 1, three agencies only owned a system, 12 agencies only used another entity's system, and five agencies both owned a system and used another entity's system. According to these agencies, some systems can include hundreds of millions or billions of photos.

[2]Specifically, we asked agencies whether at any point from January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned/operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf. See the complete list of 42 federal agencies that received our questionnaire in appendix I.

We defined facial recognition technology as a type of automated or semi-automated biometric technology that uses images for verification, identification, and/or investigative purposes. In addition, we stated that a system with facial recognition technology may include a facial recognition algorithm, hardware, software, and a photo database. We asked agencies to include all uses of facial recognition technology in their response except for facial recognition technology that was solely used to authenticate the identity of the agency's employees and contractors to log into computers and phones.

Figure 1: Ownership and Use of Facial Recognition Technology Reported by Federal Agencies that Employ Law Enforcement Officers

Source: GAO analysis of survey data. | GAO-21-105309

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. We asked agencies whether at any point during January 2015 through March 2020, they owned a system with facial recognition technology, including systems in the process of being developed. In addition, we asked agencies whether at any point from April 2018 through March 2020, they used facial recognition technology—that is, their offices, employees, or contractors (1) accessed a system owned or operated by another entity, or (2) requested that another entity use its system to conduct a facial recognition search on their behalf.

The owned system columns include systems in the process of being developed. The National Aeronautics and Space Administration's Office of Protective Services reported that it did not purchase facial recognition technology. However, we included the agency in the owned column because it used a commercial-off-the-shelf product with facial recognition technology to conduct a proof of concept test to determine whether the technology was suitable for its purposes.

Eight Agencies Reported Owning Systems with Facial Recognition Technology

Eight of the 42 federal agencies reported owning 17 systems with facial recognition technology, from January 2015 through March 2020.[3] Of these systems, four were in operation as of March 31, 2020, and were owned by three agencies: the Federal Bureau of Investigation, Federal Bureau of Prisons, and U.S. Customs and Border Protection. In addition, one of the eight agencies reported that it was in the process of procuring two systems during this time period, but had not finalized the purchase as of March 2020. Detailed descriptions of the 19 systems (17 owned and two in procurement) and their status as of March 31, 2020 can be found in our June 2021 report.

Seventeen Federal Agencies Reported Using Systems Owned by Other Entities

Seventeen of the 42 federal agencies reported using another entity's system with facial recognition technology from April 2018 through March 2020. Of the 17 agencies, 15 reported using systems owned by another federal entity; 14 reported using systems owned by state, local, tribal, or territorial entities; and 11 reported using systems owned by non-government entities. Furthermore, nine of the 17 agencies reported using systems owned by all three types of entities. See table 1 for additional information.

[3]This statement omits some information about systems owned by agencies we surveyed, as the relevant agencies deemed the information sensitive.

Table 1: Reported Use of Other Entities' Facial Recognition Technology by Federal Agencies that Employ Law Enforcement Officers

Federal Agency That Used System	Type of Entity That Owned System				
	Other Federal	State, Local, Tribal, Territorial	Non-Government[a]		
			Clearview AI	Vigilant Solutions	Other Non-Government[b]
Bureau of Diplomatic Security	Yes	Yes	Yes	Yes	Yes
U.S. Customs and Border Protection	Yes	Yes	Yes	Yes	Yes
U.S. Marshals Service	Yes	Yes	Yes	Yes	Yes
Bureau of Alcohol, Tobacco, Firearms and Explosives	Yes	Yes	Yes	Yes	No
U.S. Immigration and Customs Enforcement	Yes	Yes	Yes	No	Yes
U.S. Postal Inspection Service	Yes	Yes	Yes	Yes	No
Drug Enforcement Administration	Yes	Yes	Yes	No	No
Federal Bureau of Investigation	Yes	Yes	Yes	No	No
U.S. Secret Service	Yes	Yes	Yes	No	No
U.S. Capitol Police	Yes	Yes	No	No	No
U.S. Fish and Wildlife Service	Yes	Yes	No	No	No
Food and Drug Administration, Office of Criminal Investigations	Yes	Yes	No	No	No
Internal Revenue Service, Criminal Investigation Division	Yes	Yes	No	No	No
U.S. Park Police	No	Yes	Yes	No	No
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	No	No	No	No	Yes
Pentagon Force Protection Agency	Yes	No	No	No	No
Transportation Security Administration	Yes	No	No	No	No
Total	**15**	**14**	**10**	**5**	**5**

Legend:

✓ Agency used a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020. For federal, state, local, tribal, and territorial entities, the term "used" includes an agency's offices, employees, or contractors (1) accessing a system owned/operated by the respective entity type, or (2) requesting that the respective entity type use its system to conduct a facial recognition search on the agency's behalf. For non-government entities, the term "used" means the agency's offices, employees, or contractors submitted photos to the respective non-government service provider for the purpose of conducting a facial recognition search.

— Agency did not use a system owned by the respective entity (or entity type) at any point from April 2018 through March 2020.

Source: GAO analysis of survey data. I GAO-21-105309

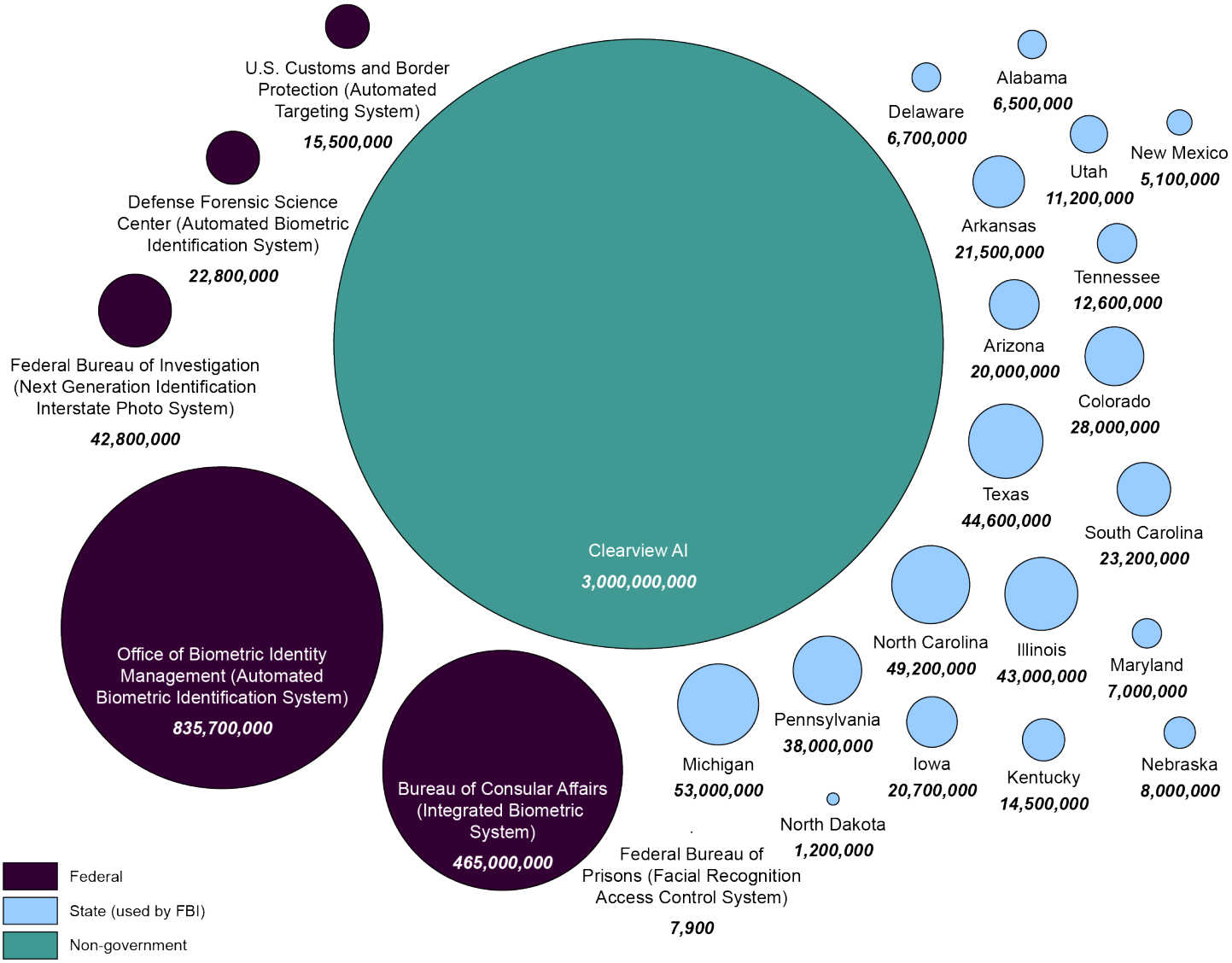
[a]Some agencies reported that they only used Clearview AI or Vigilant Solutions on a free trial basis, and thus, did not enter into a formal contract with the service provider.

[b]Other non-government entities that agencies reported using included Amazon Rekognition, BI SmartLink, and Giant Oak Social Technology, among others.

Agencies Reported Using Systems that Varied in the Number and Type of Photos

Federal agencies reported using numerous systems with facial recognition technology, and sometimes these systems included stored photos. The number and types of photos within these systems can vary, based on information reported by agencies and system owners. Reported photo types included: mug shot photos, driver's license photos, passport photos, publicly available photos on the internet, and images from video/Closed Circuit Television. Figure 2 below shows examples of federal, state, and non-government systems with facial recognition technology that federal agencies reported using, and the number of photos in them.

Figure 2: Selected Federal, State, and Non-government Systems with Facial Recognition Technology Used by Federal Agencies that Employ Law Enforcement Officers, and the Number of Photos in Them



Source: GAO analysis of information provided by system users or owners. | GAO-21-105309

Note: We sent a survey questionnaire to 42 federal agencies that employ law enforcement officers. This figure includes examples of systems used by one or more federal agencies we surveyed. It does not include all systems used by these agencies. The figure includes the number of photos stored in the respective entity's system with facial recognition technology, as of March 31, 2020.

The same individual may be included in multiple photos within one photo database or across multiple databases, and the same photo can exist within multiple databases. Some entities providing these numbers indicated they were estimates. The number of photos for federal and non-government entities were reported by the respective system owner. The number of photos for state entities were all reported by the Federal Bureau of Investigation (FBI). Specifically, the FBI's Facial Analysis,

Comparison, and Evaluation Services has memorandums of understanding with several state agencies, allowing it to leverage the state-owned systems for facial recognition searches. The FBI provided the number of photos they can access via these memorandums of understanding.

Federal Agencies Reported Using Systems with Facial Recognition Technology to Support Various Activities

Federal agencies reported using facial recognition technology to support various activities, such as criminal investigations and surveillance, and also in response to the Coronavirus Disease 2019 (e.g., verify an individual's identity remotely). Of the 20 agencies that owned or used facial recognition technology, 14 reported using the technology to support criminal investigations. For example, the FBI's Next Generation Identification Interstate Photo System allows users to search a database of over 40 million photos. The system returns a list of potential candidates that law enforcement can use to generate investigative leads. According to the FBI, the system has been used for investigations of violent crimes, credit card and identity fraud, missing persons, and bank robberies, among others.

Six agencies reported using facial recognition technology during May through August 2020 to support criminal investigations related to civil unrest, riots, or protests.[4] Following the killing of Mr. George Floyd while in the custody of the Minneapolis, Minnesota police department on May 25, 2020, nationwide civil unrest, riots, and protests occurred. Six agencies told us that they used images from these events to conduct facial recognition searches during May through August 2020 in order to assist with criminal investigations (see table 2). All six agencies reported that these searches were on images of individuals suspected of violating the law.

[4]We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system.

Table 2: Federal Agency Reported Use of Facial Recognition Technology on Images of Individuals Suspected of Violating the Law during Civil Unrest, Riots, or Protests, May through August 2020

Federal Agency	How Agency Reported Using Facial Recognition Technology
Bureau of Alcohol, Tobacco, Firearms and Explosives	In a single instance, used facial recognition technology owned by another law enforcement entity. The search was conducted to help identify an individual suspected of violating the law during the period of civil unrest, riots, or protests.
U.S. Capitol Police	Requested that the Montgomery County Department of Police (Montgomery County, Maryland) conduct facial recognition searches to assist with a criminal investigation. The purpose of the searches was to help identify individuals that confronted and made threats to a member of Congress and the member's spouse outside the White House during the period of civil unrest, riots, or protests.
Federal Bureau of Investigation	Created a digital media tip line and solicited images of people involved in criminal activity during the period of civil unrest, riots, or protests. The agency sought to identify or locate criminal suspects seen in images and video depicting criminal behavior by conducting facial recognition searches using its Next Generation Identification Interstate Photo System.
U.S. Marshals Service	Used a non-government facial recognition service provider to conduct facial recognition searches related to criminal investigations on images from the period of civil unrest, riots, or protests.
U.S. Park Police	Requested that the Maryland National Capital Park Police conduct a facial recognition search using an image from Twitter to identify an individual who allegedly assaulted an officer during the period of civil unrest, riots, or protests. The search was conducted on the National Capital Region Facial Recognition Investigative Leads System. The subject was ultimately charged with Felony Civil Disorder and two counts of Assault on a Police Officer.
U.S. Postal Inspection Service	Used Clearview AI to help identify individuals suspected of criminal activity that took place in conjunction with the period of civil unrest, riots, or protests. This criminal activity included damaging U.S. Postal Service property, stealing mail, opening mail, burglarizing U.S. Postal Service buildings, and committing arson.

Source: GAO analysis of survey data | GAO-21-105309

Three agencies reported using facial recognition technology on images from the U.S. Capitol attack on January 6, 2021.[5] The three agencies reported using the technology to generate investigative leads for criminal investigations as follows:

- U.S. Capitol Police used Clearview AI to help generate investigative leads. The agency also requested that another federal agency use its system to conduct facial recognition searches on behalf of the U.S. Capitol Police.

[5]We asked agencies whether they used facial recognition on images of the civil unrest, riots, or protests at the U.S. Capitol complex on January 6, 2021. We requested this information from 17 agencies that indicated in their questionnaire response as (1) having a system with facial recognition technology that was in operation, or (2) using another entity's system. See more information on our methodology in appendix I in GAO-21-518. Twelve agencies reported that they did not use the technology for these purposes, three agencies reported using the technology, and two agencies told us they could not answer our questions because the information pertains to ongoing investigations.

- U.S. Customs and Border Protection used its Automated Targeting System to conduct searches at the request of another federal agency.
- Bureau of Diplomatic Security used the Department of State's Integrated Biometric System to conduct searches at the request of another federal agency.

Agencies also reported using facial recognition technology to support other activities, such as surveillance, traveler verification, area access, and research and education. For example, the U.S. Secret Service piloted a system with facial recognition technology to determine whether it could be incorporated into the agency's White House Complex security operations. Specifically, the Secret Service stored photos of 23 volunteer employees within the system. As volunteers moved throughout the White House Complex, their images were captured by closed-circuit television cameras. In real time, the system compared the stored photos to images from the video footage to determine whether they represented the same individual. Secret Service told us it did not plan to implement the system based on the results of the pilot.

Most Agencies Do Not Track Non-Federal Systems in Use or Related Risks

Thirteen agencies do not have complete, up-to-date information on what non-federal systems are used by employees.[6] These 13 agencies have therefore not fully assessed the potential risks of using these systems, such as risks related to privacy and accuracy. 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.

Specifically, we found that 13 of 14 agencies that reported using non-federal systems do not have a mechanism to track what non-federal systems are used by employees (see table 3).[7] For example, when we

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

[7]Fifteen agencies reported using non-federal systems; however, we excluded U.S. Probation and Pretrial Services because it does not use facial recognition technology to support criminal investigations. All 14 agencies discussed in this section reported using the technology to support criminal investigations.

requested information from one of the agencies 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 its 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.

Table 3: Tracking of Employee Use of Non-Federal Systems with Facial Recognition Technology among Selected Federal Agencies

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. I GAO-21-105309

Note: 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.

Numerous risks to federal agencies and the public can accompany the use of facial recognition technology. In particular, these risks can relate to privacy and the accuracy of a system. For example, when agencies use facial recognition technology without first assessing the privacy implications, there is a risk that the agencies 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.

Although the accuracy of facial recognition technology has increased dramatically in recent years, risks still exist that searches will provide inaccurate results. For example, if a system is not sufficiently accurate, it could unnecessarily identify innocent people as investigative leads. The system could also miss investigative leads that could otherwise have been revealed. In December 2019, the National Institute of Standards and Technology reported that facial recognition algorithms it tested differed in accuracy widely by race, ethnicity, or country of origin, as well as by gender and age.[8] Some members of Congress, privacy groups, and others have expressed concerns that facial recognition technology's higher error rates for certain demographics could result in disparate treatment, profiling, or other adverse consequences for members of these populations.

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. 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. In addition, log-in sheets will be made available to employees, allowing supervisors to monitor employee use of the technologies. The agency also assessed privacy and accuracy risks associated with its use of facial recognition technology, including non-federal systems.[9]

However, 13 federal agencies cannot fully assess the risks of using non-federal systems because they do not have complete, up-to-date information on what systems are actually used by employees. Therefore, in June 2021 we recommended that these 13 agencies: (1) implement a

[8]National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST Interagency or Internal Report 8280 (Dec. 19, 2019). The National Institute of Standards and Technology reported that it tested 189 mostly commercial algorithms from 99 developers and that performance differences varied by the algorithms tested, with some performing better than others. For a small number of the one-to-many algorithms, differences in false positives across demographic groups were undetectable. The extent of performance differences varied by the developer, type of error, and quality of the facial images.

[9]Department of Homeland Security, Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (May 13, 2020).

mechanism to track what non-federal systems with facial recognition technology 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.[10]

These agencies generally concurred with our recommendations.[11] We believe that expeditious implementation of our recommendations is essential. 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 using these systems, including privacy and accuracy-related risks, agencies will be better positioned to mitigate any risks to themselves and the public.

Chair Jackson Lee, Ranking Member Biggs, 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 Gretta L. Goodwin, Director, Homeland Security and Justice, 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. GAO staff who made key contributions to this testimony are Jeffrey Fiore (Assistant Director), Andrea Bivens (Analyst-In-Charge), Jennifer Beddor, Emily Flores, Richard Hung, Jason Jackson, Heidi Nielson, Erin Pineda, and Adam Schrier. Key contributors for the previous work that this testimony is based on are listed in the previously issued product.

[10]We made these recommendations to all 13 agencies that reported “No” in table 3 above.

[11]As of June 2021, the 13 federal agencies have not implemented these recommendations.

Appendix I: Federal Agencies That Participated in GAO's Survey Questionnaire on Facial Recognition Technology

Our June 2021 report included the results of a survey questionnaire we sent to 42 federal agencies that employed law enforcement officers.[1] The survey focused on agency ownership and use of facial recognition technology. See the list of 42 federal agencies in table 4 below.

Table 4: Federal Agencies That Participated in GAO's Survey Questionnaire on Facial Recognition Technology

Federal Agency	Department
Forest Service	Agriculture
Bureau of Industry and Security	Commerce
National Oceanic and Atmospheric Administration, Office of Law Enforcement	Commerce
Office of Security	Commerce
Secretary's Protective Detail	Commerce
Pentagon Force Protection Agency	Defense
National Nuclear Security Administration	Energy
Food and Drug Administration, Office of Criminal Investigations	Health and Human Services
National Institutes of Health, Division of Police	Health and Human Services
U.S. Customs and Border Protection	Homeland Security
Federal Emergency Management Agency, Mount Weather Police	Homeland Security
Federal Protective Service	Homeland Security
U.S. Immigration and Customs Enforcement	Homeland Security
Office of the Chief Security Officer	Homeland Security
U.S. Secret Service	Homeland Security
Transportation Security Administration	Homeland Security
Bureau of Indian Affairs, Office of Justice Services	Interior

[1]*GAO, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO-21-518 (Washington D.C.: June 3, 2021). In our June 2021 report, we defined federal law enforcement officers as full-time employees with federal arrest authority and who are authorized to carry firearms while on duty. See more information on our scope and methodology in our June 2021 report.

Federal Agency	Department
Bureau of Land Management	Interior
Bureau of Reclamation	Interior
U.S. Fish and Wildlife Service	Interior
U.S. Park Police	Interior
National Park Service Rangers	Interior
Bureau of Alcohol, Tobacco, Firearms, and Explosives	Justice
Drug Enforcement Administration	Justice
Federal Bureau of Investigation	Justice
Federal Bureau of Prisons	Justice
U.S. Marshals Service	Justice
Division of Protective Operations	Labor
Bureau of Diplomatic Security	State
Bureau of Engraving and Printing Police	Treasury
Internal Revenue Service, Criminal Investigation Division	Treasury
U.S. Mint Police	Treasury
Police Service	Veterans Affairs
Amtrak Police Department	–
Environmental Protection Agency, Criminal Investigation Division	–
National Aeronautics and Space Administration, Office of Protective Services	–
U.S. Postal Inspection Service	–
Smithsonian Institution, Office of Protection Services	–
Tennessee Valley Authority Police	–
Administrative Office of the U.S. Courts, U.S. Probation and Pretrial Services	–
U.S. Capitol Police	–
Government Publishing Office, Uniform Police Branch	–

Legend: – Not Applicable

Source: GAO information. I GAO-21-105309

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

Orice Williams Brown, Managing Director, WilliamsO@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