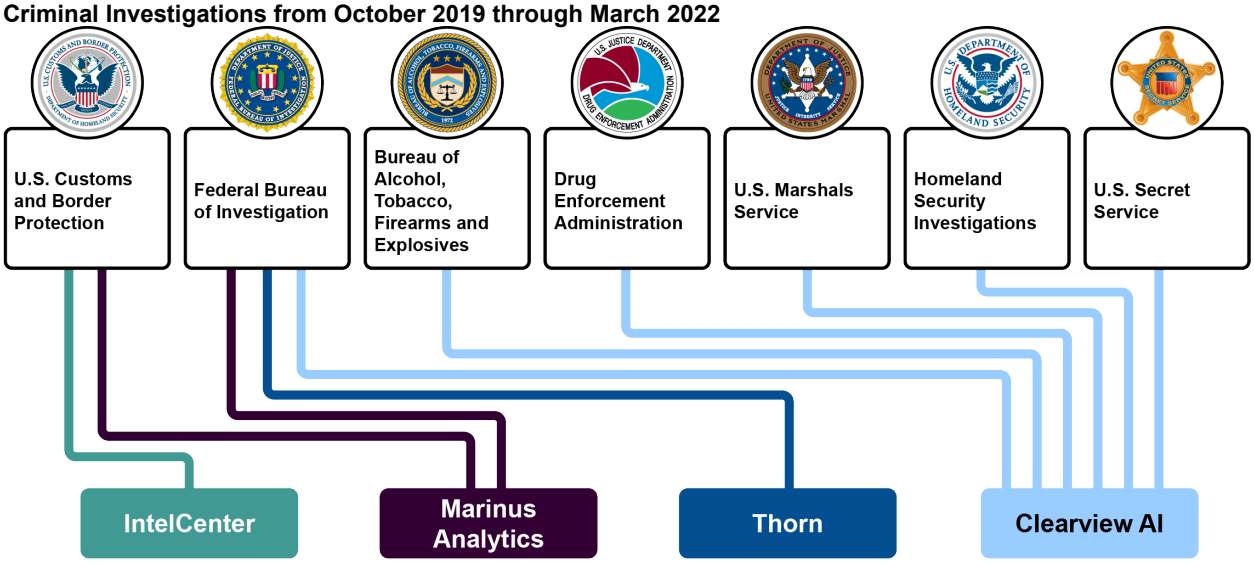
Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, GAO-21-518 (Washington, D.C.: June 3, 2021).

For "owned systems," we asked agencies whether at any point during January 2015 through March 2020 they owned a system with facial recognition technology, including systems that were procured or developed, or in the process of being developed, by the agency. For "other federal" and "state, local, tribal, and territorial systems," 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. For "nongovernment systems," we asked if the agency's offices, employees, or contractors submitted photos to a nongovernment service provider for the purpose of conducting a facial recognition search, which could include using the service as part of a free trial.

In September 2023, we further analyzed the use of nongovernment facial recognition services by the seven DHS and DOJ agencies.[7] The seven agencies reported using four different facial recognition services in total—Clearview AI, IntelCenter, Marinus Analytics, and Thorn—to support criminal investigations from October 2019 through March 2022 (see figure 1). These services gather photos from various sources, such as public social media pages and mugshot websites.

Figure 1: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022



IntelCenter's Terrorist Facial Recognition is a web-based service. The service allows users to search photos against a gallery of over 2.4 million faces extracted from open-source terrorist data, according to service representatives and website materials.

Marinus Analytics's Traffic Jam is a web-based service that includes facial recognition capabilities. Traffic Jam uses images from the online commercial sex market to identify victims of human trafficking both in the United States and abroad, according to service representatives and website materials.

Thorn's Spotlight is a web-based service that includes facial recognition capabilities. Spotlight uses images from the online commercial sex market to find exploited children and identify their traffickers to support sex trafficking investigations, according to service representatives and website materials.

Clearview AI is a web-based facial recognition service using 30+ billion facial images sourced from publicly available websites, including news media, mugshot, and social media websites, among others, according to service representatives and website materials.

Source: GAO analysis of facial recognition service information. | GAO-24-107372

[7]We reviewed agency documentation and interviewed agency officials to identify commercial and nonprofit facial recognition services that agencies used from October 2019 through March 2022 to support criminal investigations.

Note: We reported the information included in this figure in September 2023, as part of GAO-23-105607. Thus, the service provider information may not be current as of March 2024.

The seven agencies reported using facial recognition technology to support various activities, such as criminal investigations, security operations, and traveler verification.[8] Selected examples that agencies reported included the following:

- **Criminal Investigations.** A Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) task force used a facial recognition service to investigate the suspected arson of a police vehicle in Philadelphia. According to ATF officials, investigators uploaded images from video footage of the incident to the facial recognition service, identified a potential match, and further investigated the incident. They said the individual was ultimately arrested, confessed to the arson, and was sentenced to 364 days in jail.
- **Security Operations.** The U.S. Secret Service reported that it piloted a system with facial recognition technology to determine whether it could be incorporated into the agency's White House complex security operations. Secret Service officials told us they did not plan to implement the system based on the results of the pilot.
- **Traveler Verification.** U.S. Customs and Border Protection's (CBP) Traveler Verification Service uses facial recognition technology to verify the identity of certain travelers entering and exiting the United States. The system uses real-time capability to compare a traveler's live photo to photos stored in DHS databases, such as passport photos, or to a photo embedded in a travel identification document.
- **Research and education.** The Federal Bureau of Investigation (FBI) reported that it used facial recognition systems for research and education purposes, such as examining how well systems perform when used on casework.
- **Other.** In August 2021, we also reported the results of a government-wide survey on the use of facial recognition technology.[9] For instance, DHS and DOJ reported using the technology for digital access, and national security and defense purposes. DOJ also reported using it for physical security.[10]

Following the killing of George Floyd while in the custody of the Minneapolis, Minnesota, police department on May 25, 2020, nationwide civil unrest, riots, and protests occurred. In June 2021, we reported that three of the seven agencies (ATF, FBI, and U.S. Marshals Service) reported using facial recognition technology during May through August 2020 to support criminal investigations related to civil unrest, riots, or protests. All three agencies reported that these searches were on images of individuals suspected of violating the law. In addition, after the

[8]CBP told us that it does not lead criminal investigations but has used facial recognition technology to develop and share information in support of other agencies' criminal investigations. CBP officials told us that the agency used facial recognition services primarily for immigration enforcement and border security purposes.

[9]GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526 (Washington, D.C.: August 24, 2021). This report was primarily based on survey information gathered at the department level.

[10]In our August 2021 report, we surveyed 24 federal agencies about their use of facial recognition technology. Agencies that used facial recognition technology for digital access could have used it to control access to a personal computer, smartphone, or mobile application. Agencies that used facial recognition technology for national security and defense may have used the technology to identify individuals known or suspected to be terrorists, for example. Agencies that used facial recognition technology for physical security could include using the technology to control physical access, such as to facilities or buildings.

Capitol attack on January 6, 2021, one agency (CBP) reported using facial recognition technology. Specifically, at the request of another federal agency, CBP used an internal system with facial recognition technology to support criminal investigations related to the civil unrest, riots, or protests.

Some Agencies Had Policies Specific to Facial Recognition to Help Protect Civil Rights and Civil Liberties

In September 2023, we reported that three of the seven agencies (Homeland Security Investigations (HSI), U.S. Marshals Service, and Secret Service) had policies specific to facial recognition technology that were intended to help protect civil rights and civil liberties. For example, HSI's policy, first established in January 2021, included requirements such as limiting the use of facial recognition technology to certain criminal investigations.[11] Additionally, HSI's policy placed explicit limits on the collection of probe photos taken while individuals are exercising their First Amendment rights (such as at protests), among other things.

We reported that the remaining four agencies (FBI, CBP, ATF, and Drug Enforcement Administration (DEA)) did not have guidance or policies specific to facial recognition technology that addressed civil rights and civil liberties. However, these agencies told us that staff must abide by more general guidance that helps ensure the protection of civil rights and civil liberties during investigatory activities, including when using facial recognition technology. For example, CBP officials identified a DHS memorandum on protecting First Amendment rights as a source of guidance for staff using facial recognition technology.

In September 2023, we also reported that DHS planned to issue a department-wide policy on the use of facial recognition technology. DHS has since issued the policy, which includes topics such as limiting the use of the technology; protecting privacy, civil rights, and civil liberties; and testing and evaluation of the technology.[12] For example, the policy states that in criminal investigations, DHS officials may not take action based solely on identifications made by facial recognition technology.[13] The policy also says any potential matches must be manually reviewed by human face examiners prior to any law or civil enforcement action.

DOJ officials said the department formed a working group to develop a department-wide facial recognition policy that would include safeguards for civil rights and civil liberties. DOJ officials also stated that the department has existing general guidance and policies that apply to the use of facial recognition technology. However, there may also be unique issues raised by the technology that DOJ has not yet addressed through existing policy. As of September 2023, DOJ had faced delays and not finalized the policy. As a result, we recommended that the Attorney General should develop a plan with timeframes and milestones for issuing its facial recognition technology policy that addresses safeguards for civil rights and civil liberties. DOJ concurred with our recommendation.

[11]According to HSI, in November 2023 HSI limited the use of facial recognition technology to child sexual exploitation and abuse investigations, and certain authorized exceptions.

[12]Department of Homeland Security, *Use of Face Recognition and Face Capture Technologies,* Directive 026-11, Rev. 00 (Sept. 11, 2023).

[13]Identification searches compare a photo of a single unknown individual against a gallery of photos to determine if there is a potential match.

We provided a copy of this statement to DOJ for review and comment. In its comments, DOJ told us that in December 2023 it issued an interim policy on the use of facial recognition technology. According to DOJ, the interim policy will, among other things, help ensure that facial recognition technology is used "in an appropriate and responsible manner that advances the department's mission, promotes public safety, and protects privacy, civil rights, and civil liberties." We did not have an opportunity to obtain and review the policy and thus could not confirm this information. We plan to review the interim policy as part of our recommendation follow-up process to assess the extent to which it addresses our recommendation.

Agencies Used Facial Recognition Services Before Requiring Training

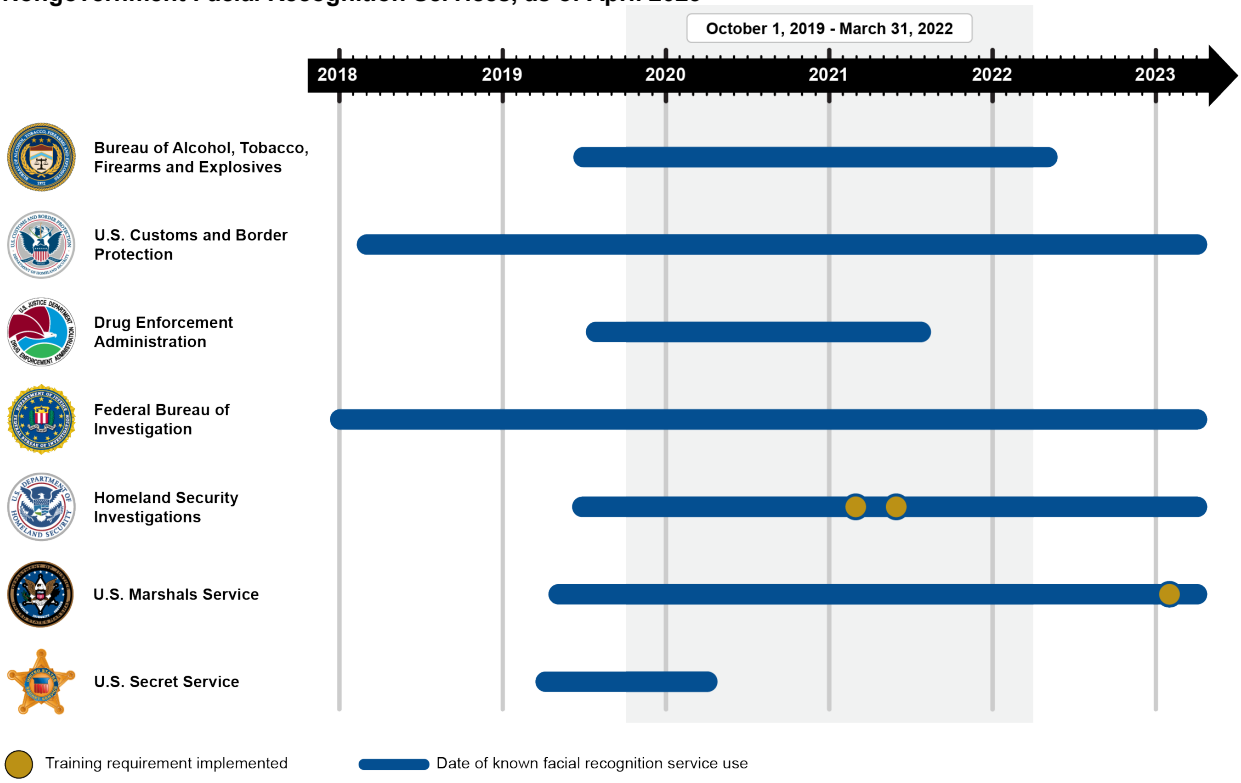
All seven agencies initially used facial recognition services without requiring staff to take training on topics such as how facial recognition technology works, what photos are appropriate to use, and how to interpret results.[14] We found that, cumulatively, agencies with available data reported conducting about 60,000 searches without requiring that staff take training on facial recognition technology to use these services.[15] Two of the seven agencies ultimately implemented training requirements—HSI and the U.S. Marshals Service.[16] Among the five agencies that did not have training requirements, as of April 2023, CBP and FBI continued to use the services, while ATF, DEA, and the Secret Service had halted their use of them. Figure 2 illustrates when agencies implemented training requirements and when they began using the four facial recognition services mentioned earlier in this statement.

[14]We assessed the extent to which agencies had implemented training specifically required for using facial recognition services. We did not assess requirements for more general training that agency staff may receive, such as general privacy training. We considered a training requirement to be written instruction to staff mandating training as a condition of access to a facial recognition service. Some agencies required general privacy training for all staff, and made optional facial recognition training available to staff, both of which may have benefited staff using facial recognition services.

[15]It is difficult to determine the overall extent to which agencies use facial recognition services, in part, because of variation in how facial recognition services and agencies using those services track the number of searches conducted by agency staff. Additionally, in some instances agencies were unable to provide information on the number of facial recognition searches staff conducted because neither the agency nor the services tracked the information. In June 2021, we also found that some agencies did not track what facial recognition systems staff used and therefore agencies may not have a complete list of facial recognition searches on untracked systems.

[16]In September 2023, we reported the results of our analysis of agency training requirements. Specifically, we determined whether agencies had training requirements as of April 2023.

Figure 2: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Nongovernment Facial Recognition Services, as of April 2023



Source: GAO analysis of agency information. | GAO-24-107372

Note: This timeline represents agencies' use of commercial and nonprofit facial recognition services and training requirements to use such services between October 1, 2019, through March 31, 2022 (see gray shading in figure). The timeline ranges from January 2018 to April 2023 because agencies may have used these four services prior to October 1, 2019, and continued to use these services after March 31, 2022. For agencies that continued to use selected services after our scope ends, we collected data as of April 12, 2023, the most recent data available at the time of our review. We assessed the extent to which agencies had implemented training specifically required for using facial recognition services. We did not assess requirements for more general training that agency staff may receive, such as general privacy training.

In September 2023, we reported that there are no federal laws or regulations that require specific training for DHS or DOJ employees using facial recognition technology or services to support criminal investigations. However, some agencies have implemented training requirements. For instance, in 2021, HSI implemented two training requirements that staff must complete prior to using Clearview AI. According to course materials we reviewed, the training covers agency policies designed to help avoid discrimination and a policy limiting the collection of probe photos in certain contexts, such as participation at events protected by the First Amendment (e.g., protests).

Other agencies continued to use the technology without training specific to facial recognition services. For instance, although the FBI determined that training is needed and officials said they planned to implement a requirement, the agency had not yet implemented a training requirement as of September 2023. The agency also did not provide clear documentation to stakeholders—the FBI AI Ethics Council and the FBI Privacy and Civil Liberties Unit—about the

status of its training requirement.[17] FBI officials told these internal stakeholders that certain staff must take training to use Clearview AI. However, in practice, FBI had only communicated to staff that training was a best practice, not a requirement. We found that only 10 staff had completed facial recognition training of 196 staff that accessed the service.[18] In our September 2023 report, we made three recommendations to DHS agencies and two recommendations to DOJ agencies related to training for facial recognition services. DHS and DOJ concurred with the recommendations, and DHS said it would develop specific training and guidance on the use of facial recognition services. As of February 2024, the agencies had not yet implemented our recommendations.

We provided a copy of this statement to DOJ for review and comment. In its comments, DOJ said the December 2023 interim policy will, among other things, require each component that uses facial recognition systems to develop and implement training and qualification requirements, as applicable, tailored to that component's missions. DOJ also said that only those personnel qualified by their component as having completed these requirements may use or approve facial recognition technology systems. We did not have an opportunity to obtain and review the policy and thus could not confirm this information. We plan to review the interim policy as part of our recommendation follow-up process to assess the extent to which it potentially addresses our recommendation.

[17]According to FBI officials, the agency's AI Ethics Council helps the FBI identify, review, and assess new and existing AI deployed and operating in support of agency missions. FBI's Privacy and Civil Liberties Unit within the Office of General Counsel is responsible for, among other things, providing legal advice and counsel on compliance with federal law protecting individual privacy, and best practices to achieve an appropriate balance between protecting civil liberties and facilitating FBI activities. Officials stated that the AI Ethics Council evaluated whether FBI's AI use cases and systems comply with ethical principles in accordance with Executive Order 13960. Exec. Order No. 13960, § 3(a)-(i), 85 Fed. Reg. 78,939 (Dec 3, 2022).

[18]We obtained and analyzed available data on training and FBI Clearview AI accounts to determine the number of trained and untrained staff. Specifically, we reviewed training records for each staff person that completed facial recognition training and compared that to a list of staff that accessed the facial recognition service. We considered staff trained if they accessed the service and completed the training, and untrained if they accessed the service but did not complete training. FBI officials stated that since we conducted our analysis, additional FBI users of the service had completed training.

Three of Seven Agencies Took Some Steps to Address Selected Privacy Requirements for Facial Recognition Services

In our September 2023 report, we reviewed four DHS and DOJ privacy requirements applicable to the use of facial recognition services.[19] We found that, as of April 2023, three of the seven agencies (CBP, HSI, and FBI) addressed some of the privacy requirements, which helped them identify privacy risks and develop related mitigation strategies. However, we also found several instances where these agencies did not address privacy requirements. The remaining four agencies (ATF, DEA, the U.S. Marshals Service, and the Secret Service) did not fully address any of the privacy requirements we reviewed as of April 2023.

Across the seven agencies, program officials told us they did not fully address the privacy requirements, in part, because they (1) did not initially recognize the photos used as personally identifiable information, which can make certain privacy requirements applicable; (2) did not realize staff transmitted photos to facial recognition services; or (3) did not fully coordinate with privacy officials while acquiring these services. For example, CBP program officials stated they initially did not consider transmitted photos to facial recognition service providers as personally identifiable information. ATF headquarters officials stated they were initially unaware ATF staff sent photos to Clearview AI.

In our September 2023 report, we made two recommendations to both DHS and DOJ related to privacy requirements. DHS and DOJ concurred with the recommendations, and DHS said its Privacy Office would continue to work with components using facial recognition technologies to ensure adherence to privacy requirements. As of February 2024, DHS and DOJ had not implemented our recommendations. However, some DHS and DOJ agencies have begun to address outstanding privacy requirements identified during our review. For example, the U.S. Marshals Service finalized an initial privacy assessment for a facial recognition service. Additionally, ATF, DEA, and the Secret Service told us they halted their use of these services as of April 2023.

Chair Garza, Vice Chair Nourse, and Members of the Commission, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

Agency Comments

We provided a draft of this testimony to DHS and DOJ for review and comment. Both departments provided technical comments, which we incorporated, as appropriate. In addition, DOJ said that due to time constraints, its comments were not inclusive of all the actions the department has taken to address issues identified by GAO.

[19]DHS and DOJ have requirements generally applicable to the use of facial recognition services to help prevent the inappropriate collection, use, and release of personally identifiable information (PII). We reviewed four of these requirements: (1) conducting an initial privacy review prior to acquiring the service, (2) conducting a privacy impact assessment prior to acquiring the service, (3) assessing privacy needs prior to acquisition, and (4) overseeing privacy controls for contractor access to PII. In addition, not all listed privacy requirements may apply to an agency's use of a facial recognition service. We were unable to evaluate the extent to which agencies executed certain privacy requirements if the agency had not yet determined whether they applied when we conducted our audit work. For more information, see GAO-23-105607.

We are sending a copy of this testimony to the U.S. Commission on Civil Rights. In addition, the testimony is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this testimony, please contact me 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), Emily Flores (Analyst-In-Charge), Andrea Bivens, Patricia Broadbent, Caitlin Cusati, Heidi Nielson, Monica Perez-Nelson, and Kevin Reeves.

Gretta L. Goodwin
Director, Homeland Security and Justice