GAO Highlights

June 29, 2022

FACIAL RECOGNITION TECHNOLOGY

Federal Agencies’ Use and Related Privacy Protections

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

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

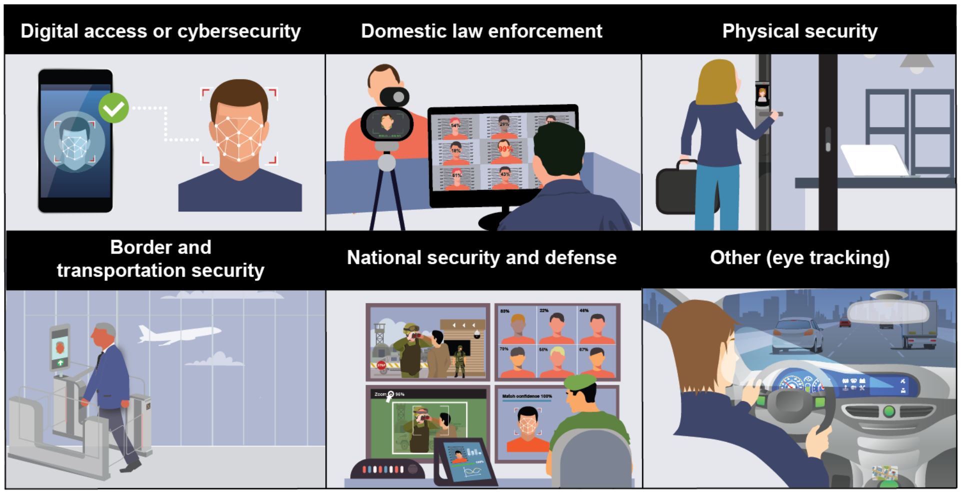
In prior reports, GAO made recommendations to 13 agencies to implement a mechanism to track use of non-federal systems by employees and assess the risks of these systems and to CBP to develop and implement a plan to conduct privacy audits of its partners, among others. Agencies generally concurred with 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


Digital access or cybersecurity
Domestic law enforcement
Physical security
Border and transportation security
National security and defense
Other (eye tracking)

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.