GAO Highlights

Highlights of GAO-20-522, a report to congressional requesters

July 2020

FACIAL RECOGNITION TECHNOLOGY

Privacy and Accuracy Issues Related to Commercial Uses

Why GAO Did This Study

Facial recognition technology can verify or identify an individual from a facial image. Advocacy groups and others have raised privacy concerns related to private companies' use of the technology, as well as concerns that higher error rates among some demographic groups could lead to disparate treatment.

GAO was asked to review the commercial use of facial recognition technology and related accuracy and privacy issues. Among other issues, this report examines how companies use the technology, its accuracy and how accuracy differs across demographic groups, and how privacy issues are addressed in laws and industry practices.

GAO analyzed laws; reviewed literature and company documentation; interviewed federal agency officials; and interviewed representatives from companies, industry groups, and privacy groups. GAO also reviewed selected privacy frameworks, chosen based on expert recommendations and research.

What GAO Recommends

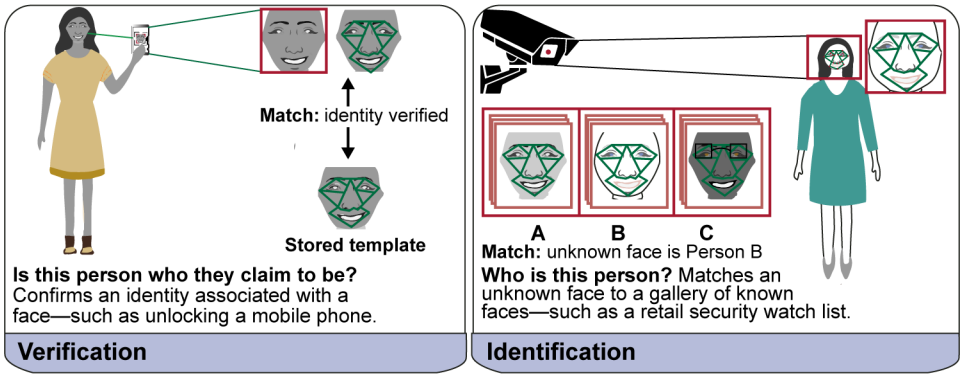
GAO reiterates its previous suggestion from a 2013 report (GAO-13-663) that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace.

View GAO-20-522. For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

What GAO Found

Market research and other data suggest that the market for facial recognition technology has increased in the number and types of businesses that use it since GAO's 2015 report on the topic (GAO-15-621). For example, newer functions of the technology identified by stakeholders and literature included authorizing payments and tracking and monitoring attendance of students, employees, or those attending events.

Functions of Facial Recognition Technology



Source: GAO analysis. | GAO-20-522

Accuracy. Although the accuracy of facial recognition technology has increased dramatically in recent years, differences in performance exist for certain demographic groups. National Institute of Standards and Technology tests found that facial recognition technology generally performs better on lighter-skin men and worse on darker-skin women, and does not perform as well on children and elderly adults. These differences could result in more frequent misidentification for certain demographics, such as misidentifying a shopper as a shoplifter when comparing the individual's image against a data set of known shoplifters. There is no consensus on what causes performance differences, including physical factors (such as lighting) or factors related to the creation or operation of the technology. However, stakeholders and literature identified various methods that could help mitigate differences in performance among demographic groups.

Privacy. Stakeholders and literature identified concerns related to privacy, such as the inability of individuals to remain anonymous in public or the use of the technology without individuals' consent. Facial recognition technology may collect or store facial images, posing varying levels of risk. Some federal and state laws and the European Union's General Data Protection Regulation impose requirements on U.S. companies related to facial recognition technology. However, as we reported in 2015, there is no comprehensive federal privacy law governing the collection, use, and sale of personal information by private-sector companies. Some stakeholders, including privacy and industry groups, have developed voluntary frameworks that seek to address privacy concerns. Most of these frameworks were consistent with internationally recognized principles for protecting the privacy and security of personal information. However, U.S. companies are not required to follow these voluntary frameworks.