December 2024

LAW ENFORCEMENT

DHS Could Better Address Bias Risk and Enhance Privacy Protections for Technologies Used in Public

GAO Highlights

Highlights of GAO-25-107302, a report to congressional requesters

Why GAO Did This Study

Technologies such as automated license plate readers and drones can support federal law enforcement activities. However, the use of these technologies in public spaces—where a warrant is not necessarily required prior to use—has led to concerns about how law enforcement is protecting civil rights, civil liberties, and privacy.

GAO was asked to review federal law enforcement's use of detection, observation, and monitoring technologies. This report examines 1) the use of these technologies in public spaces without a warrant by selected DHS law enforcement agencies and 2) the extent to which the agencies have policies to assess the use of technologies for bias and protect privacy.

GAO selected CBP, ICE, and the Secret Service within DHS based on various factors, including the large number of law enforcement officers in these agencies. GAO administered a structured questionnaire and reviewed documents, such as technology policies. GAO also interviewed agency officials.

What GAO Recommends

GAO is making five recommendations including that DHS develop policies and procedures to assess the risks of bias and ensure CBP, ICE and Secret Service implement privacy protections through technology policies. DHS concurred, but ICE and Secret Service described actions they have taken that do not address the recommendations, as discussed.

View GAO-25-107302. For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.

What GAO Found

Department of Homeland Security (DHS) law enforcement agencies reported using over 20 types of detection, observation, and monitoring technologies in fiscal year 2023. This includes both technologies the agencies owned or leased, as well as technologies the agencies accessed through third parties such as commercial vendors and other law enforcement agencies. For example, all three selected DHS law enforcement agencies reported that they have agreements to query or view information from third-party automated license plate readers, providing law enforcement personnel with access to a nationwide source of license plate data. The selected DHS agencies also reported using a variety of analytic software, including some based on artificial intelligence (AI), that can enhance the capabilities of their detection, observation, and monitoring technologies.

Figure: Examples of Detection, Observation, and Monitoring Technology

Source: Tartila and Svitlana/stock.adobe.com. | GAO-25-107302

DHS is developing policies and procedures to address bias risk from technologies that use AI, but it does not have policies or procedures to assess bias risks from the use of all detection, observation, and monitoring technology. DHS law enforcement agencies may seek out advice from DHS's Office for Civil Rights and Civil Liberties (CRCL) on bias issues related to technology use; however, there are no requirements to do so. As a result, CRCL's level of review of detection, observation, and monitoring technologies has varied. By developing policies and procedures to assess and address the risk of bias posed by DHS law enforcement agencies' use of detection, observation, and monitoring technologies, CRCL could help ensure these technologies are not infringing on civil rights and civil liberties by introducing bias.

Technology use policies GAO reviewed at U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and Secret Service did not always address key privacy protections. DHS conducts privacy impact assessments to provide the public with information on how the agency plans to address key privacy protections. Policies, however, are needed to direct employees in how they are to implement these privacy protections when using a particular technology. By requiring that policies for the use of each technology address key privacy protections, DHS agencies would have better assurance that the privacy protections are being implemented and that technology users are aware of their responsibilities to protect privacy.