BIOMETRIC IDENTIFICATION TECHNOLOGIES

Considerations to Address Information Gaps and Other Stakeholder Concerns

Report to Congressional Committees

April 2024
GAO-24-106293
United States Government Accountability Office

Accessible Version

GAO Highlights

View GAO-24-106293. For more information, contact Candice N. Wright at (202) 512-6888 or WrightC@gao.gov.
Highlights of GAO-24-106293, a report to congressional committees
April 2024

BIOMETRIC IDENTIFICATION TECHNOLOGIES

Considerations to Address Information Gaps and Other Stakeholder Concerns

Why GAO Did This Study

Biometric identification is the recognition of individuals based on their biological characteristics. These technologies include facial recognition, iris scanning, and fingerprinting, among others. Advocates for the use of biometric identification point to potential for the technologies to increase convenience, security, and efficiency. At the same time, several organizations have raised concerns about the accuracy of the technologies and their effect on privacy and civil liberties.

The Research and Development, Competition, and Innovation Act includes a provision for GAO to examine "the impact of biometric identification technologies on historically marginalized communities, including low-income communities and minority religious, racial, and ethnic groups."

This report (1) describes literature and researcher views on the accuracy of biometric identification technologies across populations; (2) describes selected stakeholders' perspectives on how, if at all, use of biometric identification technologies affects access to resources or levels of inequality for communities that have faced historical patterns of disadvantage; and (3) identifies key considerations that could help address stakeholder concerns about the use of biometric identification technologies.

GAO reviewed academic literature, government reports, and industry documents. GAO also interviewed researchers and a range of stakeholders, including community advocates; technology vendors; and local, state, and federal governments.

What GAO Found

The accuracy of biometric identification technologies has improved according to the body of research conducted in a laboratory setting, particularly for facial recognition, but gaps remain in understanding real-world performance. Various factors, such as a lack of demographic diversity in the datasets on which biometric algorithms are trained, can lead to differences in accuracy across demographic groups according to literature GAO reviewed and researchers GAO interviewed. While differences in technologies' performance have been studied in laboratory testing, performance in real-world settings has been much less extensively studied because, for example, of challenges acquiring meaningful samples across demographic groups.

Selected stakeholders provided examples of positive and negative effects associated with the use of biometric identification in communities facing historical patterns of disadvantage. Positive examples included convenience and increased access to public benefits and services, while negative examples included false arrests and subjecting communities to surveillance. The selected stakeholders identified concerns about the use of biometric identification technologies, which GAO grouped into six areas: biased outcomes, limitations understanding technology performance and effects, data and privacy, systemic inequity, lack of transparency, and technical expertise of users.

GAO identified five key considerations that could help policymakers address one or more areas of stakeholder concern through a review of relevant literature and stakeholder interviews. These key considerations include: (1) conducting comprehensive evaluations to provide a fuller picture of the effects of biometric identification technologies, (2) encouraging more widespread sharing of information about the use of the technologies, (3) applying a risk-based approach in developing regulation and guidance, (4) enacting comprehensive privacy laws or guidance, and (5) providing technology users with additional training and guidance on how to select and use relevant technologies appropriately.

Six Stakeholder Concerns About the Use of Biometric Identification Technologies and Five Considerations for Addressing Concerns

Source: GAO analysis of information gathered from stakeholders (data); Dilok/ox/ryanking999/stock.adobe.com (photos). | GAO-24-106293

Contents

Abbreviations

AI	artificial intelligence
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CBP	U.S. Customs and Border Protection
COVID-19	Coronavirus Disease 2019
DHS (S&T)	Department of Homeland Security (Science and Technology Directorate)
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
IRS	Internal Revenue Service
ISO	International Organization for Standardization
LGBTQI+	lesbian, gay, bisexual, transgender, queer, and intersex
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
TSA	Transportation Security Administration
VA	Department of Veterans Affairs

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 22, 2024

Congressional Committees

Biometric identification is the recognition of individuals based on their distinctive behavioral and biological characteristics.[1] The use of advanced technologies such as facial recognition and iris recognition to conduct and automate this type of identification has become increasingly common in both the public and private sectors. Advocates for the use of biometric identification point to potential for the technologies to provide increased convenience, security, and efficiency. They believe that the technologies can provide society-wide advantages, including improved access to public benefits and services.

At the same time, several organizations have raised concerns about the accuracy of the technologies and their effect on privacy and civil liberties. There is particular concern that these technologies can reflect and reinforce existing inequities or embed new harmful bias and discrimination.[2] For example, studies have shown that facial recognition can be less accurate for women, people with dark skin, and under-represented groups.[3] Since 2019, there have been at least six instances reported in the press in which people were falsely arrested for crimes they did not commit based on inaccurate biometric matches—all of those individuals have been African American.[4]

As the National Academies of Sciences, Engineering, and Medicine (National Academies) noted in a 2023 report, alignment of the ecosystem for science, technology, and innovation with such ethical concepts as equity, justice, fairness, and the common good has not always been a priority.[5] Studying the impact of emerging technologies across specific demographic groups is an important step in ensuring that technological innovations fairly distribute the potential benefits and burdens. Specifically, as it relates to facial recognition—one of the most commonly used biometric identification technologies—a January 2024 National Academies' report found that facial recognition raises significant equity, privacy, and civil liberties concerns that merit attention by organizations that develop, deploy, and evaluate the technology.[6]

---

[1]See National Academies of Science, Engineering, and Medicine, *Biometric Recognition: Challenges and Opportunities* (Washington, D.C.: The National Academies Press, 2010).

[2]See Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Washington, D.C.: October 2022) https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[3]For example, see National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST Interagency Report 8280* (Gaithersburg, MD.: Dec. 19, 2019); Jacqueline Cavazos, et al., *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?* arXiv:1912.07398v1[cs.CV] (Dec. 16, 2019); and Cynthia Cook, et al., "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1 (Jan. 2019).

[4]See, for example, Kashmir Hill, "Eight Months Pregnant and Arrested After False Facial Recognition Match," *New York Times*, (Aug. 6, 2023).

[5]National Academy of Medicine, *Toward Equitable Innovation in Health and Medicine: A Framework* (Washington, D.C.: The National Academies Press: 2023) https://doi.org/10.17226/27184.

[6]National Academies of Sciences, Engineering, and Medicine, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* (Washington, D.C.: The National Academies Press: 2024) https://doi.org/10.17226/27397.

The Research and Development, Competition, and Innovation Act includes a provision for GAO to examine "the impact of biometric identification technologies on historically marginalized communities, including low-income communities and minority religious, racial, and ethnic groups."[7] This report (1) describes information obtained from relevant literature and interviews with academic researchers and agency officials regarding accuracy of biometric identification technologies across populations; (2) describes selected stakeholders' perspectives on how, if at all, the use of biometric identification technologies affects access to resources or levels of inequality for communities that have faced historical patterns of disadvantage; and (3) identifies key considerations that could help address stakeholder concerns about the use of biometric identification technologies in communities that have faced historical patterns of disadvantage.

To address our objectives, we reviewed academic literature, government reports, and industry documents. We searched for documents that discussed the effects that the use of biometric identification technology has on communities that have faced historical patterns of disadvantage. During our initial review of documents, we found minimal discussion of data or metrics used to measure effects. We therefore focused on obtaining stakeholder perspectives on how, if at all, the use of biometric identification technologies can affect communities that have faced historical patterns of disadvantage.

We interviewed researchers with relevant experience and selected a broad range of stakeholders to interview across different types of technologies, communities, and use cases. Our semi-structured interviews with selected stakeholders included academics, advocacy groups that represent communities potentially affected by biometric identification, users of biometric identification technologies, and technology developers and vendors. In selecting stakeholders, we prioritized (1) broad inclusion of different communities potentially affected by biometric identification, (2) representation of viewpoints discussing both positive and negative effects of the technologies, and (3) discussion of use cases with the greatest potential to affect communities and individuals.

In addition, we interviewed federal officials—the Departments of Commerce, Education, Homeland Security (DHS), Justice (DOJ), Labor, Treasury, and Veterans Affairs (VA); the Federal Trade Commission (FTC); the Office of Science and Technology Policy (OSTP); and the Social Security Administration. We interviewed federal officials both as subject matter experts and as users of biometric identification technologies. We interviewed a total of a total of 44 stakeholders.[8] Appendix I provides more detail on our objectives, scope, and methodology.

We conducted this performance audit from October 2022 to April 2024 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

[7]Pub. L. No. 117-167, § 10226(c), 136 Stat. 1366, 1480 (2022). For the purposes of this report, we have adopted definitions of communities; equity; and rights, opportunities, or access from the Office of Science and Technology Policy's Blueprint for an AI Bill of Rights. We have operationalized the term "historically marginalized communities" as those communities that have been systematically denied a full opportunity to participate in aspects of economic, social, and civic life. See appendix II for the full list of definitions that we adopted.

[8]In our report, we characterized perspectives gathered through our 44 stakeholder interviews in the following manner: "several" represents stakeholders in three to 8 of the interviews; "some" represents stakeholders in 9 to 21 of the interviews; "many" represents stakeholders in 22 to 33 of the interviews; and "most" represents stakeholders in 34 or more of the interviews. When reporting on the views of a subset of stakeholders—for example, only advocacy organizations—we quantified the exact number. The stakeholders excluded in those counts did not necessarily disagree with that statement and may have instead not commented on the issue.

audit objectives. We believe that the evidence obtained provides a reasonable basis for any findings and conclusions based on our audit objectives.

Background

Overview of Biometric Identification Technologies

Biometric identification is the recognition of individuals based on their biological (also called physiological) and behavioral characteristics. Physiological characteristics are based on a direct measurement of a part of the body—fingertips, face, and iris. Behavioral characteristics are based on data derived from actions such as speech and signature. Biometric identification relies on the presumption that individuals are physically and behaviorally distinct in various ways.

To determine an identity, biometric technologies use algorithms to automate and check whether an individual's biometric information matches previously saved samples using two primary methods: one-to-one matching and one-to-many matching. In one-to-one matching, also called verification, the algorithm confirms if an individual matches the known sample of their information. In one-to-many matching, the algorithm runs information against the database of known samples to determine a potential match.

Datasets are used to "train" modern biometric algorithms to identify patterns and improve overall algorithm performance. Many of the top performing biometric identification algorithms use artificial intelligence (AI) in determining matches. For this report, we do not include analysis of biological behavioral characteristics that for example, estimate or classify personal characteristics such as age or sex, or that track facial features or movement to recognize expressions, among other analyses. This report focuses only on biometric identification, which aims to verify a person's identity by measuring and analyzing biological and behavioral characteristics.

There are a wide range of technologies that can be used to verify a person's identity by measuring and analyzing biological and behavioral characteristics. According to literature we reviewed and individuals we interviewed, face, fingerprint, and iris are the three most widely used biometric characteristics deployed in identification technologies. Other biometric characteristics used in identification technologies include voice, hand geometry, vascular patterns (i.e., the unique shapes of a person's veins), and gait (i.e., a person's manner of walking).[9]

Biometric identification technologies function as complex systems that depend, in many aspects, on human judgement. These systems include hardware to capture biometric characteristics (e.g., cameras and scanners) and software to perform data analysis (e.g., algorithms and AI). Human input also plays a role in many steps of the system process. For example, human experience and training can influence image quality. Human judgement can also play a role in interpreting and evaluating biometric data outputs (e.g., making final

[9]Our report does not include discussion of DNA as a type of biometric identification technology, because the technologies for using DNA are generally not sufficiently automated to allow immediate identification or identity verification. Rapid-DNA testing still requires 1-2 hours for processing.

decisions about matches). In addition, officials from the National Institute of Standards and Technology stated that human accuracy in facial recognition has been found to be variable and demographically biased.[10]

Testing and evaluation are an important component in the design, development, and deployment of biometric identification systems. There are multiple types of testing that can be done to assess the performance of biometric identification technologies, including technology, scenario, and operational testing.

- Technology testing evaluates components of a biometric identification technology system, such as the matching algorithms or system equipment, in a laboratory setting.

- Scenario testing uses volunteers to model the system performance in a laboratory environment designed to mimic the real-world application setting.

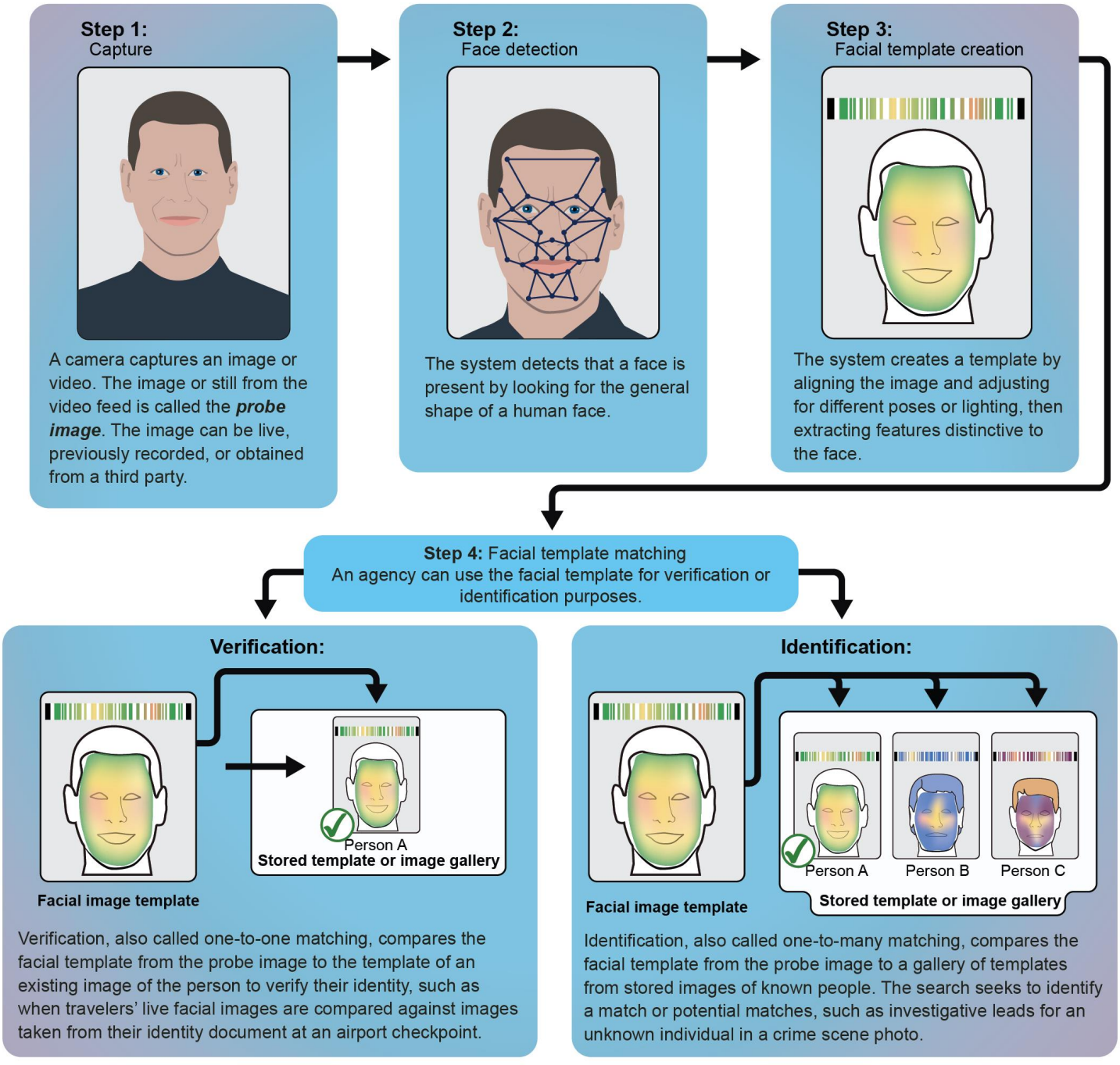
- Operational testing looks at a complete biometric identification system in the real-world setting where it is used.

Facial Recognition

Facial recognition technology identifies people by analyzing features of the face not easily altered—for example, the upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth. Facial recognition technology uses a photo or still image from a video feed of a person—often called a probe or live photo—and converts it into a template, or a mathematical representation of the photo. The most accurate facial recognition algorithms use an AI method to prepare the template. A matching algorithm can then compare the template to one from another photo and calculate their similarity, as shown in figure 1.

[10]See for example, David White, James D. Dunn, Alexandra C. Schmid, and Richard L. Kemp, "Error Rates in Users of Automatic Face Recognition Software." *PLOS ONE,* vol. 10, no. 10 (2015), https://doi.org/10.1371/journal.pone.0139827 and Hoo Keat Wong, Ian D. Stephen, and David R. T. Keeble, "The Own-Race Bias for Face Recognition in a Multiracial Society" *Frontiers in Psychology*, vol. 11, no. 208 (2020), https://doi.org/10.3389/fpsyg.2020.00208.

Figure 1: Workflow of a Facial Recognition Technology System



Source: GAO analysis (information and illustration). | GAO-24-106293

Fingerprint Recognition

Fingerprint recognition technology extracts features from impressions made by the distinct raised patterns, called friction ridges, primarily on the skin of human fingertips. An image of the fingerprint is captured by a

scanner and converted into a template. Latent prints, those from skin that is left behind cut that cannot be seen by the naked eye, can also be entered into a database and searched against the previously created templates of known fingerprint records. As with facial recognition, a matching algorithm can then compare the template to one from another fingerprint and calculate their similarity. Newer technologies include contactless fingerprint scanning where fingerprint patterns can be collected using a mobile device such as a smartphone's camera without the need for physical contact between fingers and a scanner. According to DHS, the accuracy of searching contactless fingerprint records against contact fingerprint records requires further study. Fingerprint matching algorithms may use AI to overcome challenges associated with low-quality fingerprints.

Iris Recognition

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. All currently deployed iris recognition systems operate on images of the iris illuminated in the near-infrared band of the electromagnetic spectrum. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system. Similar to facial and fingerprint recognition, a template is created for the iris, which is used for comparison in a matching algorithm that may use AI in its computations.

Other Biometrics

According to literature we reviewed, biometric characteristics such as voice, signature, hand geometry, and vascular patterns (palm vein, hand vein, or finger vein) have been deployed in commercial applications. These biometric identification technologies work by converting measurements into a digital template. Additionally, characteristics like gait, ear, sclera (the white area of the eyeball), keystroke dynamics (a behavioral biometric), and electrocardiogram and electroencephalogram signals have been proposed by researchers to recognize individuals in specialized applications. However, biometric identification technologies relying on these characteristics generally have not yet attained technological maturity or widespread acceptance.

Use Cases for Biometric Identification Technologies

Biometric identification technologies are used in a wide range of situations where a need or desire exists to verify a person's identity. The literature we reviewed described several different technology use cases, including domestic law enforcement; border security, including passenger screening at ports of entry; public education; access to public benefits, such as unemployment; health care; and commercial uses. Some of these use cases include biometrics as an option, and other cases require its use.

Domestic Law Enforcement

Law enforcement agencies have used fingerprint biometrics for decades to identify individuals. Law enforcement agencies also use facial recognition to assist in identifying individuals for multiple purposes, including identifying a deceased or unresponsive person, developing investigative leads, rescuing missing or exploited persons including children, and assisting in mental health situations or post-event investigations. Law enforcement agencies may own and operate their own automated biometric identification systems or may partner with other entities to use their systems. Other entities may include other law enforcement agencies,

departments of motor vehicles, and fusion centers.[11] We have previously reported on federal law enforcement use of facial recognition.[12]

Border and Transportation Security

Biometric identification technologies are used in a variety of ways in border and transportation security. For example, U.S. Customs and Border Protection (CBP) told us that they use fingerprint, face, and iris recognition technologies to carry out their mission. CBP has operationalized and deployed facial recognition technology, now known as the Traveler Verification Service, to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. The Transportation Security Administration (TSA) told us that they are currently testing facial recognition at some U.S. airports to automate the identity verification process.[13]

Education

Fingerprint scanning is sometimes used to identify students in schools. One application of scanning students' fingerprints is to connect their identity to an account as a method of payment for school lunches. Facial recognition is also used in some schools for various reasons, including security and monitoring student behavior. For example, facial recognition may be used to detect unauthorized people on or near a school campus.

Public Benefits and Services

People may be asked to verify their identity using biometric identification technology to apply for and access public benefits and services across different levels of government. For example, the Internal Revenue Service (IRS) uses a company that provides identity verification for governments as a method for identity verification on the agencies' websites. This method includes the option for biometric verification through facial recognition. According to the Department of Labor, 24 of 53 state workforce agencies hired a combined total of 10 identity verification service contractors that used facial recognition technology. In addition, some federal agencies, such as VA and Social Security Administration, use Login.gov for identity verification for the public to access their websites and services.[14] The Department of Labor is also offering state unemployment agencies a digital online identity verification option through Login.gov.[15] The General Services Administration announced in

[11]Under federal law, a fusion center is defined as a collaborative effort of two or more federal, state, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity. 6 U.S.C. § 124h(k)(1).

[12]For more information about federal law enforcement's use of facial recognition, see GAO, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, GAO-23-105607 (Washington, D.C.: Sept. 5, 2023).

[13]For more information about CBP and TSA's testing and deployment of facial recognition, see GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568 (Washington, D.C.: Sept. 2, 2020).

[14]Login.gov is a secure sign-in service administered by the General Services Administration that provides identity proofing and authentication for individuals wanting to log into government websites.

[15]According to officials from the Department of Labor, the agency is using one time funding available through the American Rescue Plan Act to make these services available to states for two years. They stated that an ongoing funding stream will be needed to continue this service beyond the two years.

October 2023 that Login.gov would begin offering a digital identity verification option that uses facial recognition.

Health Care

Health care applications of biometric identification technologies include patient and staff identity verification. Biometric identification technologies can be used to expedite patient check-in processes, for verifying patient identities for telemedicine, and for secure access to medical records and medication by patients and staff. For example, some pharmacies require a pharmacist to scan their own fingerprint before authorizing the sale of certain medications.

Commercial Uses

There are several commercial applications for biometric identification technologies, with facial recognition, iris scanning, and fingerprint scanning being the most commonly used. We have previously reported on the commercial uses of facial recognition technology.[16] Commercial uses include securing physical access to businesses and entertainment venues and allowing retailers to identify customers for personalized marketing and services. Businesses also use biometrics to verify identity for secure digital transactions, both online and in retail stores.

Federal Roles and Responsibilities

Federal agencies play various roles in the use of biometric identification technologies. These roles include conducting research and testing to support technology development, using the technologies in their operations, providing funding for state and local governments that use the technologies, and acting as regulators of commercial technology providers and users.

Research, Development, and Testing

Federal agencies, such as the Department of Commerce's NIST and DHS's Science and Technology Directorate (DHS S&T), conduct research and testing to support the development and use of biometric technologies. They conduct evaluations to characterize the performance and limitations of technology capabilities, identify capability gaps for additional research, and inform standards development activities. NIST evaluates facial recognition technology. For example, NIST's ongoing Face Recognition Technology Evaluations test the accuracy and performance of facial recognition algorithms that developers voluntarily submit. In these technology tests, NIST evaluates, among other metrics, two primary types of performance errors: (1) false positives—incorrectly declaring two images to be match when they are actually from two different people (sometimes called a false match), and (2) false negatives—failing to declare two images to be a match when they are actually from the same person (sometimes called a false non-match).

DHS S&T hosts annual biometric technology evaluation events which bring together subject matter experts, technology vendors, and volunteers to participate in scenario tests of new and emerging biometric technology systems. Each annual event focuses on a specific use case challenge. For example, in 2021 the event focused

[16]GAO, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, GAO-20-522 (Washington, D.C.: July 13, 2020).

on the challenge of identifying diverse individuals, including those wearing face masks. DHS S&T's biometric testing efforts also include the Remote Identity Validation Technology Demonstration which tests the effectiveness of biometric and other identity authentication technologies. Additionally, the General Services Administration is conducting a study to assess the impact of facial recognition technology across multiple demographic groups and vulnerable populations to make sure government websites that use remote identity verification work for everyone.

Technology Use in Operations

We previously reported on federal agencies' use of biometric identification technologies to carry out their missions, as shown in figure 2 below.[17] For example, DOJ and DHS use biometric technologies in their law enforcement and security operations. This may include relying on facial recognition for identity verification and developing investigative leads. DHS also uses facial recognition for collecting and analyzing biometric data for immigration, travel purposes, traveler inspection and screening, and border security. Some agencies may use it for employee access to buildings or networks.

[17]See GAO, *Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections*, GAO-22-106100 (Washington, D.C.: June 29, 2022).

Figure 2: Examples of Biometric Identification Technologies Use by Federal Agencies

Source: GAO analysis of survey results (data); GoldenSikora/metamorworks/Cipta/stock.adobe.com (images). | GAO-24-106293

Funding State and Local Entities

Federal funding may support state and local entities using commercial biometric technology services. For example, according to the Department of Labor, they provide grants to state workforce agencies with the aim of strengthening unemployment integrity (e.g., identity verification services or fraud prevention and detection

solutions) and of improving equitable access to unemployment benefits. In some states, this includes use of biometric identification systems that can verify the identity of the individual applying for benefits and enable individuals to apply for and access benefits remotely without travelling to a state unemployment office. Also, DOJ provides grants to state and local police and sheriff's offices and offers technical assistance to local law enforcement and tribes for their use of biometric identification technologies.

Regulation, Oversight, and Guidance

Federal agencies may regulate, provide oversight, or issue guidance related to biometric identification technologies. A variety of federal frameworks and other documents guide the development and use of biometric identification technologies, some through their guidance on AI which is directly relevant to biometric identification technologies since many of them use AI in their matching algorithms. For example,

- OSTP published a Blueprint for an AI Bill of Rights that highlights the importance of equitable access, privacy, and security in developing and using AI.[18]
- In January 2023, NIST published an Artificial Intelligence Risk Management Framework. The framework addresses, among other issues, privacy concerns related to individuals' identity (e.g., body, data, reputation) and AI bias, including demographic balance and data representativeness.[19]
- In September 2023, DHS published a directive to establish an enterprise-wide policy for the authorized use of face recognition and face capture technologies by DHS.[20]
- The Department of Labor recently issued guidance regarding the use of biometric identification technologies in unemployment insurance programs, encouraging states to carefully review ID verification and proofing solutions that use biometrics such as facial recognition.[21]
- The FTC enforces federal consumer protection laws that, among other things, prohibit deceptive and unfair business practices.[22] In a May 2023 policy statement, the FTC committed to combatting unfair or deceptive acts and practices related to the collection and use of consumers' biometric information and the marketing and use of biometric information technologies.[23]
- Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence encourages the Architectural and Transportation Barriers Compliance Board to issue technical assistance and recommendations on the risks and benefits of AI in using biometric data as an input.[24]

[18]Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Washington, D.C.: Oct. 2022).

[19]National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework AI RMF 1.0*, (Jan. 2023).

[20]Department of Homeland Security, *Use of Face Recognition and Face Capture Technologies, Directive Number: 026-11.* (Sept. 11, 2023).

[21]U.S. Department of Labor, *Unemployment Insurance Program Letter No. 11-23* (July 13, 2023).

[22]15 U.S.C. § 45(a)(1).

[23]Federal Trade Commission, *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, Matter Number: P225402 (May 18, 2023).

[24]88 Fed. Reg. 75,191 (Nov. 1, 2023).

- Executive Order 14074 mandates a study on the use of biometrics by law enforcement.[25]
- Executive Order 14091 commits the federal government to rooting out bias in the design and use of new technologies, such as AI.[26]
- In June 2021, we published an AI Accountability Framework that provides key practices for federal agencies and others to ensure accountability and the responsible use of AI, including biometric identification technologies.[27]

Accuracy Has Improved, Particularly for Facial Recognition, but Knowledge Gaps Persist for Real-World Performance

According to information gathered during our review of relevant literature and interviews, biometric identification technologies vary in accuracy for different populations, but recent advances have led to improvements for facial recognition technology. The accuracy of facial recognition, for example, has improved significantly over the last 4 years, with the best performing systems showing very little variation in false negative rates across different populations in laboratory testing. This is not true with false positive rates where performance differentials have decreased but differences remain. However, gaps remain in understanding the real-world performance of biometric identification technologies.

Technologies Perform Differently across Populations, but Accuracy of Facial Recognition Has Improved in Recent Years

According to information gathered during our review of relevant literature and interviews, facial recognition, fingerprinting, iris recognition, and voice recognition all perform differently across populations, depending on various factors. While some differences in accuracy still exist, the accuracy of facial recognition algorithms has improved in recent years.

Technologies Perform Differently across Populations

According literature we reviewed and one researcher we interviewed, various factors contribute to the accuracy of facial recognition systems including image quality, skin tone, gender, and the databases being used for matching. Factors such as the presence or absence of facial hair, lighting, and facial occlusion have also been known to affect facial recognition accuracy. In addition, aspects of the image capture, such as camera angle, camera settings, and image resolution, can affect accuracy.

[25]87 Fed. Reg. 32,945, 32,955-56 (May 31, 2022).

[26]88 Fed. Reg. 10,825, 10,826-27 (Feb. 16, 2023).

[27]See GAO, *Artificial Intelligence: An Accountability, Framework for Federal Agencies and Other Entities*, GAO-21-519SP (Washington, D.C.: June 30, 2021).

Facial Recognition

Image quality. According to literature we reviewed, image quality is a leading factor that can lead to differential accuracy among demographic groups, and this is closely related to skin tone (below). In July 2020, we reported on the importance of image quality to facial recognition algorithm performance.[28] In that report, we stated that better control over lighting and camera settings could improve image capture resulting in improved facial recognition technology performance. Both NIST and the International Organization for Standardization (ISO) have established image quality standards for use in facial recognition technology. According to NIST, while these standards are voluntary in the private sector, they have been widely adopted in most civilian identification documents (e.g. passports and driver's licenses) and in criminal booking processes. In addition, there are automated means to check photo quality, and to improve compliance with photographic standards. Some government agencies have internal policies related to image quality.

Skin tone. According to literature we reviewed, differences in skin tone that may be correlated with race give rise to variations in the appearance of the face. For example, the same individual may appear to have different skin tones in different lighting and under different camera settings. In addition, lighter skin tones can cause pictures to be overexposed while darker skin tones can lead to underexposed pictures. Both over- and under-exposed images can result in false negatives.

Gender. According to the literature we reviewed, facial recognition accuracy for some algorithms can be lower for females, who often have both higher false match and non-match rates.[29] The main causes of lower face recognition accuracy for females are gendered social conventions for hairstyle and makeup, and differences in face size and shape, all of which result in a smaller fraction of an image, on average, containing face information for females. There is therefore less data available for analysis.

Facial occlusion. According to literature we reviewed facial occlusion, the covering of certain parts of the face with glasses, a mask, niqab (a veil worn by Muslim women that covers most or all of the face, having a narrow opening or mesh covering for the eyes), hair or clothing can decrease the accuracy of facial recognition. DHS S&T studied the effect of masks on facial recognition technologies, finding that the median system performance was a successful identification rate of approximately 77 percent, while the best was successful for 96 percent of subjects.

Representative databases. According to literature we reviewed, agency officials, and one researcher, differences in accuracy of biometric technologies for different demographic groups may be largely related to existing datasets that are used to train biometric algorithms, which may not be diverse enough to gain meaningful sample sizes from underrepresented demographic groups. To help address this issue, DHS officials told us that they are taking steps to test biometrics with more diverse groups of volunteers.[30]

[28]GAO-20-522.

[29]See, for example, NISTIR 8280 (2019) and Albiero et al., "Gendered Differences in Face Recognition Accuracy Explained by Hairstyles, Makeup, and Facial Morphology," *IEEE Transaction on Information Forensics and Security*, vol. 17 (2022).

[30]In the autumn of 2023, DHS held its annual Biometric Rally in San Diego in order to recruit a more diverse pool of volunteers.

Fingerprinting

According to literature we reviewed and agency officials we interviewed, fingerprint biometrics can perform differently for different groups, but the application of advanced algorithms can improve accuracy. Obtaining accurate fingerprint biometric data can be more challenging for older people, people who conduct manual labor, and women. As people age, they lose elasticity in the fingers and the skin sags on the finger pads, which causes fingerprint collection issues. People who do manual labor (for example, construction or dishwashing) can wear down their fingerprint ridges faster than skin cells are replaced, making it hard to capture their fingerprints. Women generally have finer ridges on their fingers.

Iris Recognition

According to NIST, factors that affect accuracy in iris recognition can be related to demographics, but further study is needed. According to a 2018 report by NIST, an evaluation of automated iris recognition algorithms showed that matching algorithms tended to perform best on Whites and worst on Asians.[31] The most accurate matching algorithms tended to perform slightly better on lighter eyes, but eye color varies in correlation with many other factors and demographic traits which could be responsible for the differences in accuracy among eye color. Because the test dataset consisted of samples collected in various environments over a period of years, NIST could not discount the possibility that any apparent demographic effects were due to confounding factors and found that further investigation was necessary before drawing any solid conclusions.

Voice Recognition

According to literature we reviewed, and agency officials, the accuracy of voice recognition technology can be affected by age, gender, accent, health, and other demographic factors. An agency official told us that performance difference in these systems could be due to the lack of diverse training data, characteristics of the voices or speech of various populations, or the feature extraction technology performance for different populations. According to officials from the Federal Bureau of Investigations (FBI), systems trained with data that does not sufficiently represent gender, language, dialect, age, or other factors spoken by certain demographic populations can result in reduced or biased performance when analyzing speakers from those populations. For example, two research studies have also shown that voice recognition technologies, such as virtual assistant software that use voice recognition to identify who is speaking, have lower performance with Black, Asian, and Hispanic people than other groups because of a lack of training data.[32] Reliability also varies by gender and age.

The Accuracy of Facial Recognition Has Improved Over Time

NIST's recent evaluations of facial recognition algorithms found significant improvements over time in the accuracy of facial recognition technology, but they have found that performance differences still exist for certain demographic groups. NIST reported in February 2020 that with good quality portrait photos, the most accurate algorithms will fail to identify the correct person 0.1 percent of the time when searching a gallery containing 12 million individuals. This result shows substantial improvements in recent years, with rates

[31]National Institute of Standards and Technology, *NIST Interagency/Internal Report 8207, IREX IX Part One Performance of Iris Recognition Algorithms* (Gaithersburg, MD.: Apr. 18, 2018) https://doi.org/10.6028/NIST.IR.8207.

[32]Koenecke et al., "Racial disparities in automated speech recognition," *PNAS*. vol. 117, (2020), 7684-7689; and Chen et al., "Exploring racial and gender disparities in voice biometrics," *Scientific Reports*, vol. 12 (2022), 3723.

decreasing from 4.1 percent in 2014 to 0.23 percent in 2018. NIST officials told us that algorithms are becoming more tolerant of changes in a person's appearance such as the addition or subtraction of facial hair and glasses, and the effects of shadows. They also told us that they have observed improvements in accuracy over time related to demographic differences; however, false positive rates are still higher for certain demographic groups that are not sufficiently represented in the training data such as elderly East Asian women and elderly East African women.

Gaps Remain in Understanding Technologies' Accuracy and Real-World Performance Across Populations

Gaps remain in understanding the accuracy and real-world performance of biometric identification technologies because of challenges associated with capturing demographic information, a lack of research focus and funding on differences in performance across demographics, and self-exclusion from testing. Agency officials noted limitations in the evaluations of biometric identification technologies which lead to gaps in knowledge about whether accuracy varies across technologies and populations in operational settings (i.e., in real-world performance). NIST and DHS S&T perform extensive testing of biometric identification technologies and report their results publicly. However, officials from DHS S&T noted the need for more real-world testing of these technologies. According to NIST officials, laboratory tests of algorithms produce insight into what will happen when that algorithm is fielded operationally; however, it will not predict performance exactly because populations will be different. Officials stated that algorithm and scenario testing are very important, but the shortcoming is that there is still a need for more operational (i.e. real-world) testing.

Capturing Demographic Information

According to agency officials, it can be challenging to capture sufficient information to analyze performance across groups. Officials from DHS S&T said that their biometric tests are not necessarily designed to capture certain demographic information. They told us it is challenging to test biometric accuracy in an operational setting with sample sizes sufficient to make strong conclusions about any given demographic group. They said this can be especially challenging for certain minority groups that may only represent a small proportion of volunteers even when the total number of volunteers is near 1,000. DHS S&T also does not collect certain demographic information (like religion) from volunteers during these tests.

Biometric testing in real-world settings like an airport security checkpoint does occur, but typically does not capture detailed demographic factors like race, ethnicity, religion, income, or, in some instances, gender. Collecting this type of demographic information in a real-world setting would be complicated because people might not want to provide this information voluntarily. A DHS official also noted that it would be inappropriate to label datasets with demographic information such as perceived race, skin color, gender, or age, as this subjective labeling could result in embedding bias into the data. Additionally, while it is possible to collect demographic information from consenting volunteers in a controlled test facility, it is challenging to acquire meaningful samples across all demographic groups at a single location with a limited pool of volunteers. Furthermore, it is often very challenging to collect demographic information in a real-world setting where larger sample sizes could be acquired, such as from people who are passing through an airport security checkpoint.

Additional Areas of Research Focus

According to officials from three agencies and one researcher, there is a lack of research focus on differences in performance across demographics. One researcher told us that the majority of biometrics research funding comes from the private sector, which is focused on improving overall accuracy and efficiency, not on reducing error rate differences between demographic groups.

Additionally, a Secret Service official stated that research is lacking on how much voice recognition systems degrade in performance for various populations. FBI officials noted that forensic speaker recognition case conditions can vary widely and may not be similar enough to conditions under which a system is trained to produce verifiably accurate results.[33]

OSTP officials said that industry and the public are still determining how to measure and understand the performance of biometric technologies. OSTP identified the need for additional research on gender disparities, including the accuracy of biometric systems in recognizing and identifying transgender and non-binary individuals. OSTP also supported further research into other identities and communities for which biometric technologies consistently perform poorly. For example, OSTP noted that some people with disabilities or certain medical conditions may not be recognized by facial recognition technology or iris and fingerprint-based biometric identification systems. A lack of clarity on how to measure and understand performance may present an impediment to focusing research on better understanding the benefits or harms of these technologies including across demographic groups.

FBI officials also pointed to recent studies that demonstrate progress being made with facial recognition technologies, especially studies published within since 2023.[34] They noted that the findings of studies looking at demographic differences in the performance of biometric identification technologies are complex and that the technologies are not always biased against the same demographic groups. This complexity reinforces the need for testing biometric identification systems in real-world operational environments to evaluate the results on the effected populations.

Self-exclusion from Testing

According to stakeholder interviews and literature we reviewed, information on biometric accuracy for some groups could also be impeded because of self-exclusion from biometric testing and use. Individuals from some groups may decide not to participate in biometric testing and use because of religious values, cultural norms, an aversion to the data collection process, or mistrust of those collecting the data. For example, according to a 2010 National Research Council report, religious beliefs about the body and sectarian jurisdiction over personal characteristics (e.g., beards and headscarves) or interpersonal contact (e.g., taking photographs, touching, exposing parts of the body) may make a biometric system an unacceptable intrusion. In addition,

[33]For the purposes of this report, “speaker recognition” and “voice recognition” are synonymous. According to the FBI: “Speaker, or voice, recognition is a biometric modality that uses an individual’s voice for recognition purposes.”

[34]See for example, National Physical Laboratory, *Facial Recognition Technology in Law Enforcement Equitability: Study Final Report*, MS 43 (Teddington, England: March 2023) and Aman Bhatta, Gabriella Pangelinan, Michael C. King, and Kevin W. Boyer, “Impact of Blur and Resolution on Demographic Disparities in 1-to-Many Facial Identification” (pre-publication 2024) https://arxiv.org/pdf/2309.04447.pdf.

stakeholders from multiple advocacy groups told us that some historically underserved communities are distrustful of government and law enforcement, and may see collection of biometric data as a potential harm.

Stakeholders Shared Examples of Effects on Communities Facing Historical Patterns of Disadvantage and Identified Areas of Concern

Selected stakeholders we interviewed provided examples of positive and negative effects of the use of biometric identification technologies on communities facing historical patterns of disadvantage and identified concerns related to the use of these technologies.[35] However, information about the positive and negative effects is limited, as the stakeholders largely provided examples related to anecdotal or firsthand experiences or potential effects. While stakeholders we interviewed were often not able to provide details about the effects of these technologies, they identified concerns about the use of biometric identification technologies, which we grouped into six overarching areas. Areas include concerns about biased outcomes, data security and privacy protections, and limitations understanding technology performance and effects, among others.

Stakeholders Shared Examples of Positive and Negative Effects, but Information Is Limited

Selected stakeholders we interviewed provided examples of positive and negative effects that biometric identification technologies can have on access to resources and levels of inequality for communities facing historical patterns of disadvantage, but information about those effects is limited. Overwhelmingly, the stakeholders we interviewed shared examples about facial recognition and provided few examples related to other types of biometric identification, including iris, fingerprint, and voice recognition. The stakeholders shared firsthand observations, anecdotal experiences, and potential concerns about the effects of biometric identification technologies. However, they were often not able to provide detailed or quantifiable information related to the extent of effects resulting from the use of biometric identification technologies.[36]

Selected stakeholders representing communities potentially affected by the technologies may not have access to the data needed to quantify effects or identify causal mechanisms and therefore do not know whether their experiences are representative. For example, of the 35 stakeholders who commented on this topic, 24 said that the users of biometric identification technology are not sharing information with the public about how well the biometric identification systems perform across all populations and whether there are potential biases, inequities, or other social concerns resulting from using the systems. Three technology vendors we interviewed

[35]We conducted a literature search and found limited information about the effects of biometric identification technologies on communities that have faced historical patterns of disadvantage. As a result of this limited information, we interviewed stakeholders representing a variety of communities and viewpoints about their experiences with the effects of biometric identification technologies on communities. See Appendix I Objectives, Scope, and Methodology for more details.

[36]One example of a lack of quantifiable information is law enforcement use of facial recognition. According to the National Academies' 2024 report, facial recognition has played a role in at least six high-profile arrests of Black individuals. Although these incidents likely represent a small percentage of known arrests involving facial recognition, comprehensive data on the prevalence of facial recognition use, how often facial recognition plays a role in arrests and convictions, or the total number of wrongful arrests that have occurred on the basis of facial recognition do not exist.

said they share information with their customers, but either do not share it with the public or did not say whether they share information with the public.

Overall, selected stakeholder perspectives about the positive and negative effects of biometric identification technologies on communities that have faced historical patterns of disadvantage varied by use case.[37] For example, stakeholders shared a mix of both positive and negative examples about the effect of biometric identification technologies to access public benefits and services. Conversely, stakeholders had a more critical view about the use of biometric identification technologies for domestic law enforcement and border security use cases, with negative examples outnumbering the positive ones. Stakeholders identified fewer examples of either positive or negative effects for health care, commercial, and education use cases. In some use cases, stakeholders identified trade-offs between potential effects. For example, several stakeholders said that biometric identification technologies can offer positive effects to an individual in the form of convenience but could overall have negative effects for privacy or data security.

Positive effects. Selected stakeholders shared a limited number of positive effects resulting from the use of biometric identification technologies on communities that have faced historical patterns of disadvantage. The positive effects shared by stakeholders fell into the following categories: increased convenience, access to benefits or services, public safety, matching individuals to their health records, autonomy for individuals with disabilities, reduced fraud, and reduced unnecessary interactions with law enforcement (i.e., police may be less likely to engage with individuals who are not relevant to an investigation if facial recognition is applied with accuracy). The most frequently cited examples of positive effects shared by stakeholders were increased access to public benefits and services, and increased convenience:

- One industry group and one technology vendor said using biometric identification to access public benefits and services is an improvement over the current methods used to verify identity. These stakeholders said that the current methods, such as answering questions about one's credit history, have low rates of successful verification. For example, the vendor said that rates for successful identity verification for residents of Puerto Rico to access tax information on the IRS website were markedly higher using biometric identification as compared to verifying identity with questions about credit history.
- Some stakeholders said that biometric identification technologies can offer convenience for members of communities that have faced historical patterns of disadvantage. For example, several stakeholders said that voice, fingerprint, and facial recognition could offer increased autonomy for people with disabilities. However, one research organization cautioned these technologies could also create barriers to access if the technology was not compatible with their abilities, such as requiring an individual needing to hold their head or finger still for a certain amount of time. Additionally, a state agency and industry group said using fingerprints to pay for school lunch may be more convenient for young children who may not remember a password or form of payment and can mask that low-income students qualify for free or reduced lunch.

Our focus during interviews with stakeholders were examples of effects specific to communities facing historical patterns of disadvantage; however, several stakeholders, including those from federal agencies, were unable to comment on specific communities, and instead spoke about positive effects of biometric identification on the U.S. population more broadly. For example, CBP and ATF agency stakeholders said that they have not observed disparate effects of the biometric identification technologies their agency uses, and CPB

[37]Our discussion with stakeholders about the effects of biometric identification technologies was not focused exclusively on federal uses of the technologies. We sought examples of effects arising from all potential use cases, including those involving private actors as well as local, state, and federal governments.

stakeholders stated that use of these technologies improves public safety overall by removing terrorists, criminals, and sexual predators from the general population. Additionally, a local government stakeholder said that when a first responder finds an unresponsive person without an ID, they can use facial recognition to identify them and retrieve their medical history. In cases of a natural disaster, such as an earthquake, the stakeholder noted biometric identification can be used to identify victims.

Negative effects. Overall, stakeholders provided more examples of negative effects than positive effects. The negative effects shared by stakeholders included false arrests, reduced access to benefits or services and immigration systems, being subjected to surveillance, unequal access to commercial spaces, and adverse implications for transgender individuals whose ID may not match their identity. The most frequently cited negative examples of effects of biometric identification technologies shared by stakeholders were false arrests or misidentification, barriers to accessing a desired public benefit or service, and being subjected to surveillance:

- Several stakeholders said that the use of facial recognition has led to false arrests or misidentification of Black or African American men. In this example, both demographic differences in how well facial recognition technologies perform and historical racial disparities in policing may contribute to the effect. When a law enforcement officer runs a search using facial recognition technology, they submit a photo of a suspect—which may not be a high-quality image—and the system turns up potential matches. A false match, or being incorrectly identified as the suspect, could result in an innocent individual being investigated or arrested. Two advocacy organizations said that there is little redress for being wrongfully arrested. Several stakeholders, said that it was important for law enforcement to recognize that matching results are intended to only be used as an investigative lead, and not a positive identification. A technology vendor said that following proper procedure and thoroughly investigating leads could have prevented these instances of false arrests.
- Several stakeholders said that the use of biometric identification technologies affected the ability of communities that have faced historical patterns of disadvantage to receive unemployment benefits. Attempting to verify your identity using a “selfie” photo that is matched against the photo on your ID—and failing—can result in being denied access to a service or benefit, including accessing tax information online or applying for rental assistance. One state employment agency found there were disparate outcomes for using biometric identification to complete the unemployment insurance application process during COVID-19. People who self-identified as Black or African American, American Indian or Alaska natives, and native Spanish speakers, among others, were less likely to complete their application to obtain unemployment insurance.
- An advocacy organization that supports applicants for unemployment insurance said that an estimated 20 percent of applicants were not able to verify their identity. Several stakeholders said difficulty completing biometric identity verification may be more likely to affect communities that may not have access to broadband, which can disproportionately be rural and low-income areas, and non-English speaking communities because there may be a language barrier.[38] In the context of public benefits and services, two state employment agencies said that challenges using the technology—not necessarily the accuracy of the biometric identification— may have contributed to effects they observed. If applicants cannot verify their identity using the “selfie” match, customer support offers a non-biometric alternative to verify identity, such as meeting virtually with a representative from the vendor and presenting identification documents.

[38]GAO, *Broadband: National Strategy Needed to Guide Federal Efforts to Reduce Digital Divide*, GAO-22-104611 (Washington D.C.: May 31, 2022).

However, one stakeholder said that, during COVID-19, there were long wait times for these non-biometric alternatives and a limited number of representatives who spoke languages other than English.

- Several stakeholders said that using biometric identification technologies for surveillance can have negative effects, with two stakeholders noting that surveillance disproportionately affects low-income and Black or African American communities. One-to-many matching can be used to scan a crowd to attempt to identify people of interest. Several stakeholders cited examples of domestic law enforcement agencies using facial recognition on protestors in 2020. The law enforcement community can access tens of billions of photos through databases owned by a private company or government agencies.

In some use cases, stakeholders identified trade-offs between potential effects. For example, the public benefits and services use case is reflected under both positive and negative effects above. There may be trade-offs between fraud and challenges with accessing benefits in this use case. During the COVID-19 pandemic, facial recognition was often implemented to combat unemployment insurance fraud.[39] A research organization and a vendor said that reducing the instance of fraud could increase the resources available for legitimate claimants; however, two state agencies said that steps to limit fraud may simultaneously create barriers to completing the application for these claimants. Similarly, in a domestic law enforcement context, several stakeholders identified that there may be tensions between the positive effects of public safety versus the negative effects of intrusive surveillance. Additionally, several stakeholders said that biometric identification technologies can offer positive effects to an individual in the form of convenience but could overall have negative effects for privacy or data security. One advocacy organization told us that assessing these trade-offs is challenging because the effects are not yet fully understood.

Several stakeholders cautioned against lumping together multiple use cases or types of technologies, which one stakeholder said could lead to reduced use of beneficial applications that are relatively low risk. Specifically, two stakeholders said that the concerns about law enforcement use biometric identification should not be conflated with other use cases. Additionally, several stakeholders described use cases that use one-to-one matching as a less risky application of biometric identification technologies than use cases that use one-to-many matching.

Stakeholders' Concerns Span a Variety of Areas, Including Biased Outcomes and Challenges with Evaluation

In describing examples of current or potential effects of the use of biometric identification technologies, stakeholders also shared some overarching areas of concern. Although there was no consensus across stakeholders, we grouped these areas of concerns into six categories through our analysis. These categories are not mutually exclusive, and there is some overlap between the topics discussed within the different categories. The six areas of concern are identified in figure 3 and listed below.

[39]GAO has previously reported on unemployment fraud issues and added unemployment insurance to its High-Risk List in 2022. GAO, *Unemployment Insurance: Estimated Amount of Fraud During Pandemic Likely Between $100 Billion and $135 Billion*, GAO-23-106696 (Washington, D.C.: Sept. 12, 2023); and GAO, *Unemployment Insurance: DOL Needs to Address Substantial Pandemic UI Fraud and Reduce Persistent Risks*, GAO-23-106586 (Washington, D.C.: Feb. 8, 2023).

Figure 3: Stakeholder Areas of Concern with Biometric Identification Technologies

Limitations understanding technology performance and effects

There is limited availability of data to understand real-world performance of the technologies.

Technical expertise of users

Technology users may not have the technical expertise or adequate training to operate these technologies appropriately.

Data security and privacy protections

There are concerns about biometric data being collected from individuals and used without their consent, a lack of security in the storage of the data, and data being used for purposes other than it was initially intended.

Biased outcomes

Disparate treatment, profiling, or other negative consequences for certain demographic groups may result from the use of biometric identification technologies, which can be caused both by performance differences across populations and how the technologies are implemented.

Lack of transparency

Limited information about where and how technologies are used.

Exacerbating systemic inequity

Technologies may be deployed in a way that exacerbates existing societal inequities.

Source: GAO analysis of information gathered from stakeholders (data); Dilok/ox/ryanking999/stock.adobe.com (photos). | GAO-24-106293

Biased Outcomes

Several stakeholders identified concerns about disparate treatment, including profiling, misidentification, or other negative issues of bias affecting certain demographic groups resulting from the use of biometric identification technologies. These concerns stemmed from both performance differences across populations and how the technologies are implemented. Differential performance—performance differences between demographic groups processed by a particular biometric identification algorithm resulting in more false positives or false negatives for certain groups—was a repeated concern and was mentioned by more than half of stakeholders who discussed bias.

There are multiple ways that the design and operation of biometric identification systems can result in biased outcomes:

- **Data.** Differences in accuracy of biometric technologies for different demographic groups may be largely related to lack of diverse datasets on which the biometric algorithms are trained. For example, an industry association and an academic stakeholder said that algorithms are often trained on datasets that

feature predominantly White features and characteristics. Several stakeholders told us that the data used to train biometric identification technologies are critical: if the training data do not represent a particular community, the technology will not work as well for them compared to those who are represented.

- **Testing.** DHS S&T officials said that in their scenario testing—testing designed to mimic real world situations—they have found more errors resulting from how the image of an individual is captured than from the matching algorithm. This may create a gap between the results of algorithm testing and real-world performance.

- **Deployment and implementation practices.** Several stakeholders shared concerns about biased outcomes resulting from how humans implement biometric identification technologies. For example, a former law enforcement officer said that biometric identification technologies are implemented at police discretion and are often disproportionately deployed in predominantly Black or African American neighborhoods. Three stakeholders said that Black or African Americans are likely overrepresented in law enforcement databases, with one advocacy organization stating that as a result, they are more likely to be subject to a false match. A facial recognition system can only match people who are in its reference database. If Blacks or African Americans are more heavily represented in those databases, they are more likely to be incorrectly identified through false matches or they may be more likely to be affected by inappropriate interpretation of facial recognition results. Additionally, two stakeholders pointed out that even if there were no demographic differentials, historically marginalized communities cold be subject to use of these technologies more frequently.

Limitations Understanding Technology Performance and Effects

Many stakeholders expressed concerns about measuring the performance and effects of biometric identification technologies. Several stakeholders identified challenges with understanding the effects of biometric identification technologies on communities that have faced historical patterns of disadvantage, including limited information about the performance of biometric identification technologies in a real-world setting; limited availability of data; and limited resources, incentives, or requirements for evaluating the performance of biometric identification technologies.

Several stakeholders said that while NIST conducts testing on how well a given algorithm performs in controlled conditions, these results may not be indicative of real-world performance. While NIST uses operational data in its testing, according to officials, it does not predict how well an entire biometric identification technology performs. One stakeholder from a research organization said that to measure the effects, one would first have to determine how well a given technology performs in a specific use case—for example, how accurate is the technology and for which demographic groups—but there is not enough information yet to do so. The stakeholder said that these types of evaluations tend to be costly and take a long time. An industry association stakeholder said that the biometric identification technology industry as a whole needs a better approach to measure the effects of biometric identification technologies than it has now.

In addition to challenges with measuring how well technologies perform, stakeholders identified challenges with determining the effects of these technologies on communities that have faced historical patterns of disadvantage. Several stakeholders said that data that could be used to determine how well biometric identification technologies are performing is difficult to obtain. For example, one academic institution said it requested data from a vendor about pass rates for individuals applying for public benefits but was unable to obtain these data. One researcher said that if it is not mandatory to share data, some developers or users of the technology may not report it and others may then adopt the same practice. Several stakeholders said that

communities that have faced historical patterns of disadvantage are skeptical about or lack trust in organizations collecting data from them.

Several industry and vendor stakeholders believe that potential benefits of biometric identification technologies are not being fully evaluated. One of the stakeholders said that biometric identification technologies are being compared to hypothetically perfect performance, which does not exist in practice—the status quo is not operating perfectly. For example, stakeholders from an industry group and a vendor said that legacy methods of verifying identity, such answering questions about ones credit history, can have low rates of successful identity verification. A vendor that provides biometric identification services to the IRS did a case study and found that the rate at which individuals in Puerto Rico were able to successfully access tax information on the IRS website were markedly higher using biometric identification as compared to verifying identity with questions about credit history.

Data Security and Privacy Protections

About half of stakeholders shared concerns about data security or privacy protections. Concerns about data and privacy include a complex set of interrelated issues, such as consent, surveillance, infringement on freedom of speech, data storage, and data use. Several stakeholders said that communities that have faced historical patterns of disadvantage are vulnerable to the unwanted collection and use of data. These concerns can contribute to public mistrust in the use of biometric identification technologies.

One industry group said that privacy and consent are a challenge for appropriate use of biometric data, since data collection through photos can happen without explicit consent. In the domestic law enforcement use case, a subject does not need to give consent for biometric identification to occur. Additionally, stakeholders from an advocacy organization said that opting out does not always feel like a viable option. There is fear of retaliation or loss of access to freedom, housing, employment, or public benefits. Stakeholders from the advocacy organization said that individuals in communities that have faced historical patterns of disadvantage may feel they have to provide biometric information even if an opt out is theoretically possible.

Several stakeholders expressed concern about biometric identification technologies being used for surveillance. In several cases, stakeholders were proponents of the use of biometric identification technologies for other use cases but opposed the use of biometric identification technologies for any surveillance purposes. Several stakeholders said that there are privacy concerns with surveillance, and it can have a chilling effect on First Amendment activities.

Some stakeholders shared concerns about how biometric data are stored. One advocacy organization said that there are gaps in legislation around data security and that biometric identification in law enforcement and social services is happening without adequate data protection polices. One vendor said that there are largely no security or data standards for private companies and state or local governments. The vendor said it would be beneficial to have more guidance about how to sufficiently store and protect personally identifiable information. Several stakeholders said that biometric data are particularly sensitive because one cannot change their biometric information and that data breaches may affect people throughout their lifetime.

Several stakeholders also identified concerns about how biometric data are used. For example, one stakeholder said that data may be used for purposes other than which they were initially intended—like driver's

license photos in a database used for other purposes.[40] Individuals often do not have ownership over their biometric data or control over how their data are used. For example, an industry association and an academic stakeholder said they have concerns about a private vendor and how it obtained data from scraping images from the internet. One industry association also noted that this practice may intersect with performance, as using poor quality images lead poor performance of facial recognition technologies. Images taken from the internet were not collected expressly to be used for facial recognition and may be poor quality (e.g., low resolution, poorly lit, or taken from an angle).

Exacerbating Systemic Inequity

Some stakeholders shared concerns that biometric identification technologies are often deployed in a manner that exacerbates existing societal inequities. An advocacy organization said that these technologies are used in a myriad of contexts that can intersect with other structural inequities. Some stakeholders said that biometric identification technologies could intersect with existing racial disparities in law enforcement, for example disproportionate arrest rates and over-policing of neighborhoods that are predominantly Black or African American. Additionally, one stakeholder who studies the distribution of biometric data collection in New York City stated that lower income and predominantly Black or African American areas have more surveillance than wealthier and predominantly White neighborhoods. An advocacy organization said that individuals subject to biometric identification technologies in the workplace, such as real-time video tracking, are more likely to be members of communities that have faced historical patterns of disadvantage.

Two stakeholders said that where biometric identification technologies are used can have effects on communities that have faced historical patterns of disadvantage, even if the technologies do not have differential performance. A researcher said that if biometric identification technologies are more often deployed in communities that have faced historical patterns of disadvantage, some racial groups are more often exposed to the technologies. Even if the false positive rate and false negative rate were identical between racial groups, they would experience more false positives and negatives from these technologies being used in their communities.

Several stakeholders also said that there can be an opportunity cost to biometric identification technologies because investment in biometric identification technologies can reduce resources available for other approaches to improve public safety. As an example, one advocacy organization said that if law enforcement agencies are investing in facial recognition technologies, they will not have financial resources for other approaches to public safety, like services for mental health and addiction.

Lack of Transparency

Several stakeholders identified concerns about the lack of transparency with the use of biometric identification technologies, including how they are used to make decisions. They provided examples of instances in which it is not clear to the public where or how these technologies are being used. In a law enforcement context, several stakeholders said law enforcement agencies are not transparent in their use of these technologies. For example, one advocacy organization said that it is difficult to obtain information from law enforcement agencies

[40]For example, GAO has reported that some federal law enforcement agencies reported using another entity's system with facial recognition technology, including state, local, tribal or territorial entities and non-government entities. GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, GAO-21-518 (Washington, D.C.: June 3, 2021).

about whether facial recognition technologies were used in a given case. In a commercial use case, two advocacy organizations said there is a lack of clarity about how widespread the use of biometric identification technologies is by employers, and it is not clear how data are being used.

Several stakeholders expressed concern that biometric identification technologies are deployed without advance notice or opportunity for public comment. For example, several stakeholders said the public often learns about potential issues with these technologies after the fact, through Freedom of Information Act requests.[41] Additionally, several stakeholders said there is a lack of auditing for biometric identification technologies, which further reduces transparency these technologies.

Technical Expertise of Users

Several stakeholders are concerned technology users do not have the technical expertise or adequate training to operate biometric identification technologies appropriately. For example, two stakeholders said that law enforcement officers are not experts in these technologies and may not have the guidance needed to use the technologies appropriately. Several stakeholders said that it is important for law enforcement to recognize that matching results are intended to serve as an investigative lead and not as positive identification. In September 2023, we reported there are gaps in training for use of facial recognition technologies at the federal level.[42] For example, seven federal law enforcement 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.[43]

Several stakeholders said that it is not clear where to obtain guidance or training about the use of these technologies. Specifically, two state employment agencies said there was limited guidance from the Department of Labor about how to implement biometric identification technologies.

Use Case Examples Illustrate Stakeholder Concerns

The areas of concerns that stakeholders identified about current or potential uses of biometric identification technologies have specific implications by use case. We illustrate how these concerns intersect with the use cases we described above—public benefits and services, commercial use, domestic law enforcement, border security, education, and health care—in a series of vignettes. These use case specific examples are not exhaustive of all concerns that may apply to each use case.

[41]The Freedom of Information Act requires federal agencies to provide the public with access to government records and information on the principles of openness and accountability in government. Federal agencies are generally required to disclose any information requested unless it falls under one of nine exemptions. 5 U.S.C. §552.

[42]We reported in 2023 that law enforcement agencies in DHS and DOJ had begun using commercial and non-profit facial recognition services without requiring training for staff. We recommended that CBP and FBI implement training requirements or evaluate the need for such requirements. As of February 2024, these agencies had not implemented such training requirements. GAO-23-105607.

[43]GAO-23-105607.

Vignette 1

PUBLIC BENEFITS AND SERVICES

Unemployment insurance during Covid-19

At the beginning of the COVID-19 pandemic, there were historic pandemic job losses. Congress created new temporary unemployment insurance programs to provide relief for the unemployed. The unprecedented demand for benefits and need to quickly implement the new programs increased the risk of fraud. For example, one state employment agency we interviewed said they received more applications for unemployment insurance than the total population of the state. In response, it is estimated that half of all states incorporated biometric identification technologies into the application process for unemployment insurance, often using private vendors. This typically involved an applicant taking a "selfie" with a smartphone that is matched against the photo on their ID and was done remotely.

STAKEHOLDER CONCERNS

Biased outcomes

Some communities may have experienced denials or delays in receiving benefits. For example, one state employment agency conducted a study and found that Black or African Americans, American Indians or Alaska natives, and native Spanish speakers were less likely to complete their application and receive benefits. Additionally, officials in another state said that tribal communities may have faced barriers because a vendor did not initially accept tribal IDs as a valid form of identification to match against.

Limitations understanding technology performance and effects

Measuring access to public benefits can be challenging because employment agencies may not know whether applicants who do not make it through the system were eligible claimants or whether the system was correctly identifying fraud.

The benefits of biometric identify verification to access services like unemployment insurance may not be fully evaluated because their performance is being compared to hypothetically perfect performance instead of being compared to other existing methods of verifying identity, like answering question about your credit history. For example, one industry association noted that one biometric identity verification service has an 80 percent rate of successful verification, while other non-biometric methods have closer to a 60 to 67 percent rate of success.

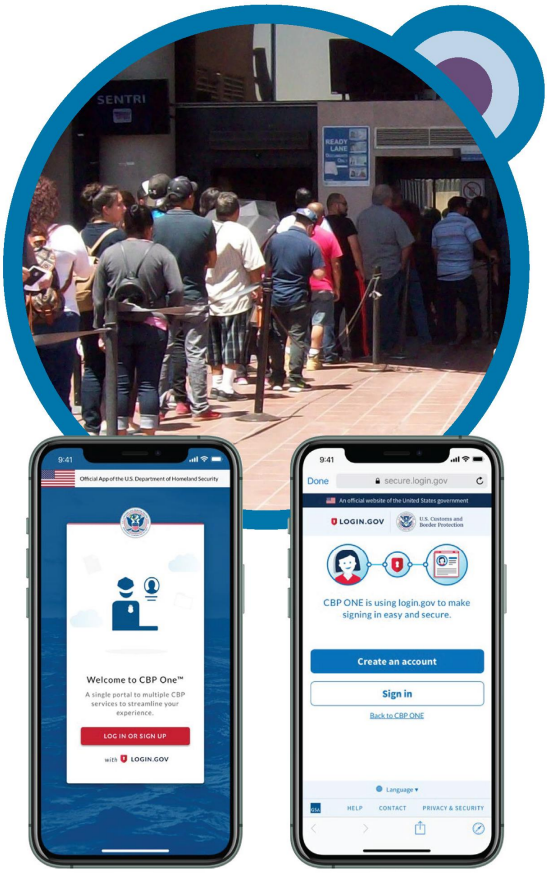
Sources: GAO analysis of stakeholder information (data); Chansom Pantip/curto/freeject.net/stock.adobe.com (photos). | GAO-24-106293

Vignette 2

BORDER SECURITY

CBP One app

In 2020, U.S. Customs and Border Protection (CBP) released a mobile app called CBP One through which users can access a variety of CBP services, including requesting advance travel authorization or checking border wait times. A May 2023 Department of Homeland Security rule directed noncitizens seeking asylum in the U.S. to schedule an appointment to present themselves at the southern border—with some exceptions for extenuating circumstances—through the CBP One app. Scheduling an appointment on the app involves submitting a photograph, which determines facial liveness (e.g. whether the subject is a live person rather than a photograph of a subject). Later, it is matched against the noncitizen's identification documents and against a gallery of images to vet any law enforcement and national security concerns. According to CBP documentation, use of the app to schedule appointments is intended to increase safety and efficiency.



STAKEHOLDER CONCERNS

Biased outcomes

Several stakeholders said that while it has improved, the photograph step on the app may not work as well with darker skin tones, which could affect which noncitizens are able to successfully schedule an appointment on the app. Organizations that assist noncitizens have installed construction or photoshoot lights to aid in capturing a good photo.

A smartphone is needed to use the CBP One app and the app is available in a limited number of language options, which could negatively affect noncitizens with limited financial resources or non-English speakers.

Data security and privacy protections

Noncitizens may not know or understand how their biometric data are going to be retained or used.

Sources: GAO analysis of stakeholder information (data); GAO (upper photo), U.S. Customs and Border Protection (lower photo). | GAO-24-106293

Vignette 3

DOMESTIC LAW ENFORCEMENT

Use of facial recognition technology

Federal, state, and local law enforcement agencies use facial recognition to help solve crimes. For example, law enforcement officers may compare a photo of an unknown suspect from a crime scene against a database of photos, which can include mug shots or driver's license photos. If the photo of the unknown suspect is a potential match to one of the database photos, law enforcement officers can use it as an investigative lead. The law enforcement community can access tens of billions of photos through databases owned by private companies or government agencies.

STAKEHOLDER CONCERNS

User expertise

Law enforcement officials are not experts in these technologies and may not have the guidance needed to use the technologies appropriately.

Additionally, there is no standard threshold for matching, and it is not clear what, if any, standards law enforcement agencies have set for matching. Some law enforcement agencies may use facial recognition at an 80 percent match threshold, while developers may often report efficacy of their technologies at a 95 percent match threshold. When a match threshold is lowered, there is a greater chance that the wrong people are identified as potential matches (i.e. a false positive).

Biased outcomes

Law enforcement use of facial recognition may result in biased outcomes because law enforcement agencies may deploy them more often in areas that are predominantly Black or African American or low-income. Systems that rely on law enforcement databases likely include a disproportionate number of Black or African Americans, which can result in a disproportionate number of Black or African Americans being incorrectly identified through false matches or inappropriate interpretation of facial recognition results.

Limitations understanding technology performance and effects

It is not clear how often false arrests occur when facial recognition has been used because there has been no systematic evaluation about how common these instances are–only several high-profile examples.

Lack of transparency

It may not be clear when law enforcement agencies are using these technologies. For example, their use is often only discovered after the fact through Freedom of Information Act requests.

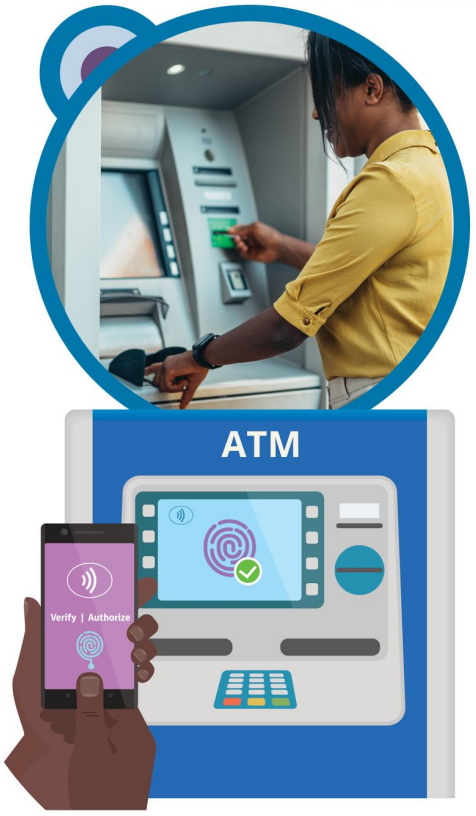
Sources: GAO analysis of stakeholder information (data); Stockmedia/Camerene P/peopleimages.com/knut/stock.adobe.com | GAO-24-106293

Vignette 4

COMMERCIAL USE

Banking and financial services

Biometric identification technologies are used in a variety of commercial applications, including banking and financial services. In 2020, we reported that wider adoption of facial recognition technology for banking and financial services was bolstered, in part, by regulatory changes included in the 2015 European Union's payment services regulation. The regulation calls for two-factor authentication—one of which can be biometric, such as face recognition. For banking and financial services, use of biometric identification technologies also includes use of a fingerprint instead of pin at an ATM and voice recognition to verify your identity over the phone.



STAKEHOLDER CONCERNS

Biased outcomes

A vendor that provides biometric identification technologies for financial services said if biometric identification technologies are not carefully calibrated, demographic differentials will exist, which could result in biased outcomes in who can readily access financial services. The vendor said that to address potential biased outcomes, they can measure the number of false positives across several areas including gender, age, and skin tone.

Lack of transparency

However, there may be limited information about the use and effects of these technologies in commercial use cases. In absence of any requirements to do so, private companies may not share information about use or performance of biometric identification technologies.

Sources: GAO analysis of stakeholder information (data); Zamrznuti tonovi/Julia Tim/stock.adobe.com | GAO-24-106293

Vignette 5

HEALTH CARE

Matching patient records

We have reported that there are challenges with accurately matching patient health records—that is, comparing patient information in different health records to determine if the records refer to the same patient, and that inaccurately matched records can adversely affect patient safety or privacy. We reported that there are some patient populations for which matching is particularly challenging. For example, some east-Asian cultures use the "family name" as the first name, and some Hispanic cultures use multiple last names. Additionally, sometimes a transgender patient's photo ID lists the wrong gender, yet the organizational policy may be to record the gender exactly as it appears on a state-issued photo ID.

Biometric identifiers can be used to match patient records, which may increase accuracy and efficiency in a healthcare setting. This may be a prospective use of biometric identification technologies—a 2022 report by the Pew Charitable Trusts noted that there are no known cases of biometrics being used to match electronic health records across different systems in the U.S., and no national technical standards to facilitate the process.

STAKEHOLDER CONCERNS

Data and privacy

There may be concerns about privacy of patients' biometric data. However, there may be more regulation related to biometric data than in other contexts. For example, the Health Insurance Portability and Accountability Act (HIPAA), and its implementing regulations, where applicable govern the use and disclosure of individually identifiable health information—including biometric data like facial data—and set standards for data security. Two stakeholders noted that, as a result, the health care industry may be better positioned to deploy responsible use of biometric identification technologies than in other use cases.

Sources: GAO analysis of stakeholder information (data); Jade/pandpstock001/stock.adobe.com | GAO-24-106293

Vignette 6

EDUCATION

Use of biometric identification technologies in New York public schools

In 2014, New York state passed a Smart School Bond Act that authorized the issuance of $2 billion to schools for improved educational technology and infrastructure. Some New York schools used available funds for biometric identification technologies, including facial recognition technology. Biometrics may be used with the goal to increase school safety and reduce threats presented by unauthorized access.

STAKEHOLDER CONCERNS

Lack of transparency

In 2016, a New York school began using facial recognition without notifying parents. Parents were concerned about how the technology works, how it is being used on students, where the data are stored, and how the data will be used. These concerns eventually led to a lawsuit against the school and the New York State Education Department.

Effective December 2020, New York passed State Technology Law 106-b, which issued a time-limited general ban on the use of biometric identification technologies in schools. The law also directed the New York Office of Information Technology with assistance from the State Education Department to publish a report containing recommendations as to the circumstances in which the use of biometric identification technologies is appropriate in schools, and what restrictions and guidelines should be enacted.

That report was released in August 2023, and in September 2023, the New York State Commissioner of Education issued an order that prohibits schools in New York State from purchasing or utilizing facial recognition technology. Schools can decide at the local level whether to use biometric identification technologies other than facial recognition, as long as they consider the technologies' privacy implications, impact on civil rights, effectiveness, and parental support.

Data security and privacy protections

Parents, guardians, and teachers in New York State had concerns about how student data are shared and stored and how the data would be used in the future. In a survey conducted by the New York Office of Information Technology, the most frequently cited concerns about the use of biometric identification in school settings were privacy and data security.

Sources: GAO analysis of stakeholder information (data); Thexfilephoto/monkey business/stock.adobe.com | GAO-24-106293

Key Considerations to Address Privacy, Transparency, and Other Concerns

Through a review of relevant literature and analysis of stakeholder interviews, we identified five key considerations that could help address one or more areas of stakeholder concern, as summarized and shown in table 1 and figure 4. These key considerations cover several different policy areas and are provided to inform policymakers—including Congress, federal agencies, state and local governments, academia, industry,

and international organizations—about potential approaches and actions to address the areas of concern identified by stakeholders. While many of the stakeholder concerns arose from examples related to the use of facial recognition, these key considerations encompass broad policy consideration that can apply to any biometric identification technology. Policymakers would need to consider how to align potential actions with existing federal programs and initiatives.

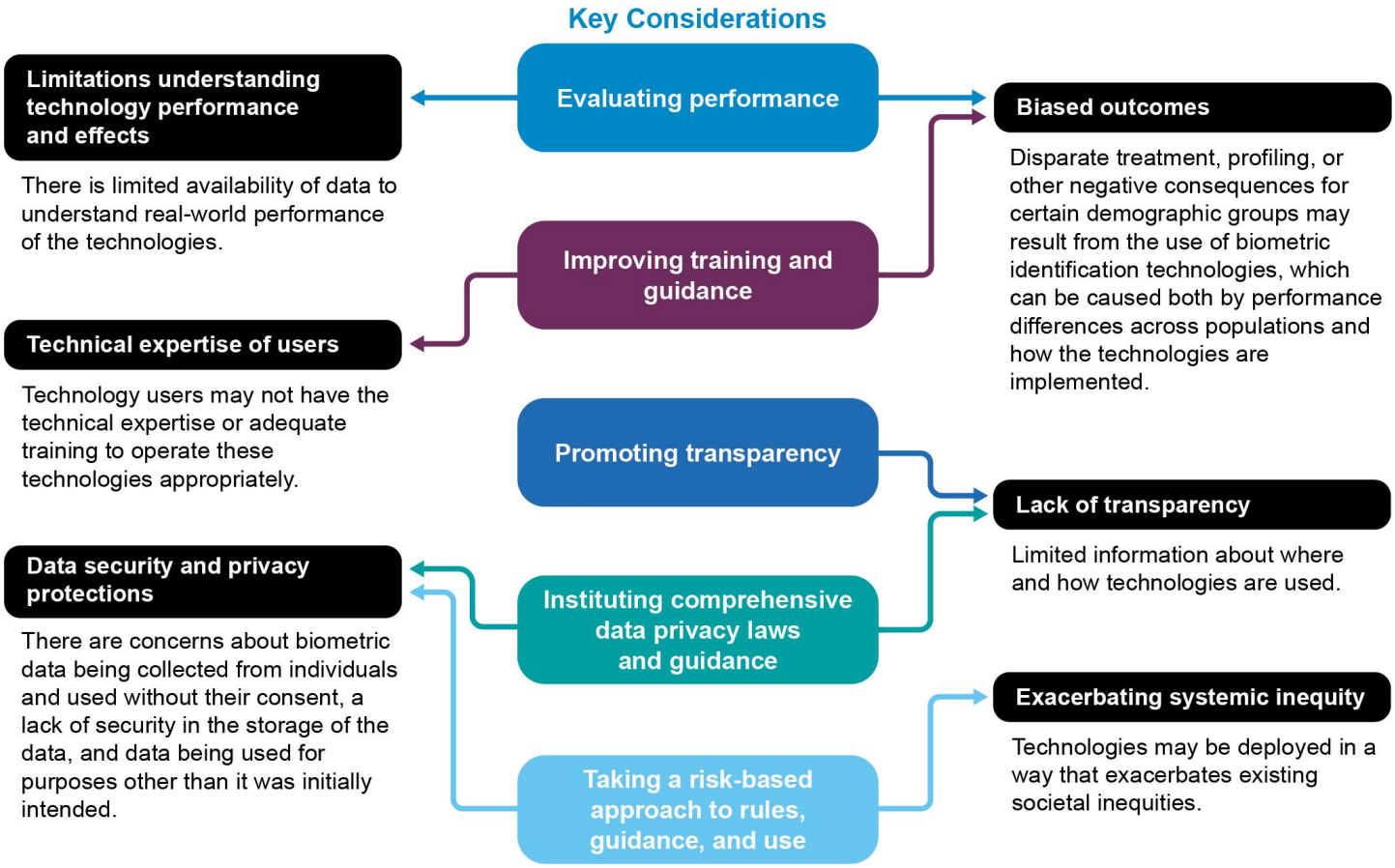
Table 1: Key Considerations to Address Stakeholder Concerns about the Use of Biometric Identification Technologies

Stakeholder concerns	Key considerations to address stakeholder concerns	Key considerations to address stakeholder concerns	Key considerations to address stakeholder concerns	Key considerations to address stakeholder concerns	Key considerations to address stakeholder concerns
na	**Evaluating performance**	**Promoting transparency**	**Taking a risk-based approach to rules, guidance, and use**	**Instituting comprehensive data privacy laws or guidance**	**Improving training and guidance**
Biased outcomes	Addresses stakeholder concerns	Not applicable	Not applicable	Not applicable	Addresses stakeholder concerns
Limitations understanding technology performance and effects	Addresses stakeholder concerns	Not applicable	Not applicable	Not applicable	Not applicable
Data security and privacy protections	Not applicable	Not applicable	Addresses stakeholder concerns	Addresses stakeholder concerns	Not applicable
Exacerbating systemic inequity	Not applicable	Not applicable	Addresses stakeholder concerns	Not applicable	Not applicable
Lack of transparency	Not applicable	Addresses stakeholder concerns	Not applicable	Addresses stakeholder concerns	Not applicable
Technical expertise of users	Not applicable	Not applicable	Not applicable	Not applicable	Addresses stakeholder concerns

Legend: ✓ Addresses stakeholder concerns — Not applicable

Source: GAO analysis of information gathered from stakeholders. | GAO-24-106293

Figure 4: Key Considerations to Address Stakeholder Concerns about the Use of Biometric Identification Technologies



Source: GAO analysis of information gathered from stakeholders. | GAO-24-106293

Since, as we discussed above, many biometric identification technologies are AI-based, addressing concerns about the use of biometric identification technologies should be contextualized in the broader societal and policy conversations about AI. During our interviews, which took place between April and September 2023, most stakeholders said that there should be an oversight role for the federal government to address concerns about the effects of biometric identification systems on historically marginalized communities. Several stakeholders also said that they would like to see the federal government provide more guidance on the use of these technologies.

Subsequent to our stakeholder interviews, in March 2024, the Office of Management and Budget (OMB) issued a memorandum on governance and risk management for federal AI use.[44] The memorandum directs federal agencies to adopt specific minimum risk management practices for uses of AI that impact the rights of the public. The memorandum defines rights-impacting AI to generally include law enforcement use of facial and iris matching, the use of biometric data to determine border access and access to federal immigration related services, surveillance in an education setting and determining eligibility for student aid, and allowing or denying

[44]OMB Memorandum for the Heads of Executive Departments and Agencies, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,* M-24-10, March 28, 2024.

access to government benefits or services. The risk management practices outlined in the memorandum call for actions within four of the five policy areas covered by our key considerations, as described below.

Additionally, in January 2024 the National Academies published a study that assessed facial recognition technology.[45] The study committee reviewed current facial recognition use cases and considered the legal, social, and ethical issues implicated by their use. The study made a number of recommendations that align with some of the key considerations we developed, as outlined below.

Evaluating Performance

Conducting more comprehensive evaluations can provide a fuller picture of the effects (positive or negative) of biometric identification technologies on communities that have faced historical patterns of disadvantage. This can include evaluating the accuracy of a technology and whether there are any demographic differentials across populations, as well as evaluating whether implementation of a technology has any disparate effects on communities that have faced historical patterns of disadvantage. This consideration could help address stakeholder concerns related to biased outcomes, and limitations in understanding technology performance and effects.

As discussed above, there are knowledge gaps in understanding the real-world performance of biometric identification technologies. We described challenges including a lack of testing in real-world conditions and difficulty capturing demographic information. Additionally, stakeholders and agency officials expressed concerns that there are limited resources, incentives, and requirements for evaluating the performance of biometric identification technologies.

Addressing these knowledge gaps through increased, robust evaluations will require a multi-pronged approach. One approach is to incentivize more participation in testing and provide resources for additional types of testing. This could be done in multiple ways. One way is to provide guidance to technology vendors so that they design their products in ways that support more standardized testing. Officials at DHS S&T told us that vendors sometimes decline to participate in technology evaluations because their products are not capable of interfacing with the software package used in the automated tests. Officials said that facial recognition vendors are generally familiar with testing requirements, but vendors of other technologies are not. Another way to incentivize testing is to provide support for independent third-party certification of biometric identification technologies. Federal agencies in their roles as technology users could provide funding to the organizations conducting the certification process. They could also encourage development of qualified product lists from which federal agencies and state and local governments could be required or incentivized to purchase biometric identification technologies from a list of certified products.

To address the lack of an agreed-upon approach to evaluating effects on communities, federal agencies in their roles of supporting technology development could encourage additional standards development. One example of standards development is the ISO standard for quantifying biometric system performance variation across demographic groups. An ISO technical committee is drafting the standard, which DHS S&T officials expect to be published in 2024. DHS S&T officials stated that the standard will provide a consistent set of metrics for defining terms such as ethnicity and measuring observable characteristics like skin tone. This standard is one possible metric that could be incorporated into the use of qualified product lists discussed

[45]National Academies of Sciences, Engineering, and Medicine*, Facial Recognition Technology.*

above. The National Academies' study on facial recognition technology recommended that the federal government, together with national and international standards organizations (or an industry consortium with robust government oversight), establish industry-wide standards for evaluating and reporting on the performance—including accuracy and demographic variation—of facial recognition technology products for private or public use.

Another approach to increasing performance evaluation capability for biometric identification technologies is to incentivize technology developers, vendors, and users to adopt risk management strategies like those contained in the NIST AI Risk Management Framework. The NIST framework encourages organizations to think through issues such as the availability of reliable metrics and how measuring risks in a laboratory or controlled environment may differ from risks that may emerge in operational, real-world settings. Dedicating the time and resources to fully consider these issues could help organizations develop ways to overcome challenges that data limitations pose to technology performance evaluations. The National Academies' study on facial recognition technology recommended that the federal government establish a program to develop and refine a risk management framework to help organizations identify and mitigate the risks of proposed facial recognition technology applications with regards to performance, equity, privacy, civil liberties, and effective governance.

OMB's memorandum generally instructs federal agencies to take a risk management approach to managing AI-based technologies. The memorandum requires federal agencies using rights-impacting AI-based technologies, including certain biometric identification technologies, to test those systems for performance in a real-world context and independently evaluate the AI through reviewing relevant documentation to ensure that the system works appropriately. Additionally, the memorandum states that agencies must complete an AI impact assessment and document (1) the intended purpose for the AI and its expected benefit, supported by specific metrics or qualitative analysis; (2) the potential risks of using the AI, as well as any additional mitigations measures the agency will take to reduce the risks; and (3) the quality and appropriateness of the relevant data.

Promoting Transparency

This consideration entails encouraging more widespread sharing of information about the use of biometric identification technologies, both in identifying when and where the technologies are used and in identifying information about the effects of the technologies on communities—including those that have faced historical patterns of disadvantage. This consideration could help address stakeholder concerns related to a lack of transparency about biometric identification technologies.

As discussed above, several stakeholders expressed concern that there is a lack of information about how biometric identification technologies are being used to make decisions. When the public is not provided with sufficient information to understand how and when they are interacting with biometric identification technologies, it can lead to heightened suspicion and a lack of public trust. NIST's Risk Management Framework states that, by promoting higher levels of understanding, transparency increases confidence in biometric identification systems.

One of the key practices in GAO's AI Accountability Framework is that organizations should promote transparency by enabling external stakeholders to access information on the design, operation, and limitations of an AI system. Organizations should consider what type of information about the system is accessible to

external stakeholders, including end users, consumers, and individuals impacted by the use of the AI system. For AI-based biometric identification technologies, that could be achieved by posting information in an easily understandable format on organizations' websites or providing clear notice in places where biometric data are being collected.

The National Academies' study on facial recognition technology recommended that institutions developing or deploying facial recognition technology should take steps to identify and mitigate bias and cultivate greater community trust—with particular attention to minority and other historically disadvantaged communities. These should include, among other things, engaging with communities to help individuals understand the technology's capabilities, limitations, and risks.

OMB's memorandum generally requires federal agencies to provide public notice about their use of rights-impacting AI-based biometric identification technologies. The mechanism for this notice would be an annual inventory of agencies' AI use cases to be documented in plain language and posted on agencies' public websites. The memorandum states that where people interact with a service relying on AI and are likely to be impacted by AI, agencies must provide reasonable and timely notice about the use of AI and a means to directly access any public documentation about it in the use case inventory.

Taking a Risk-Based Approach to Rules, Guidance, and Use

This consideration involves applying a risk-based approach in developing regulation and guidance for biometric technologies that is informed by the severity of the potential risk from a particular technology. This consideration could help address stakeholder concerns related to data security and privacy protections, and systemic inequity.

As discussed above, the effects of biometric identification technologies on individuals and communities varies by use case. For example, we heard from NIST officials that one-to-many matching generally presents a higher risk of errors due to differential performance than one-to-one matching. Moreover, law enforcement use cases, some of which rely on one-to-many matching, can pose a much higher risk to individuals' personal liberty and safety, due to potential consequences such as false arrests and effects on privacy from surveillance and monitoring. Layered on top of these individual risks is the potential to amplify existing inequity, as noted in OSTP's Blueprint for an AI Bill of Rights. NIST's 2022 report on identifying and managing bias in AI states that systemic and implicit biases such as racism and other forms of discrimination can inadvertently manifest in AI, and left unaddressed, these biases can negatively impact individuals and society by amplifying and reinforcing discrimination at a speed and scale far beyond traditional discriminatory practices.[46]

One aspect to managing risk is implementing mitigation strategies for the use of biometric identification technologies. Effective mitigations could take the form of offering an equivalent alternative to using biometrics, including non-biometric pathways to overcome potential barriers, such as false negative match results, or lack of access to the required technology (e.g., reliable internet and smartphones). Other mitigation strategies could include offering instructions in languages other than English, or providing access to opt-out options for technology users. Some use cases for biometric identification technologies that have the highest risk for an individual's personal safety and liberty (e.g., false arrests in the context of domestic law enforcement) may be

[46]National Institute of Standards and Technology, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (Gaithersburg, MD: Mar. 2022).

the least likely to have viable opt-outs. In these cases, policymakers and technology users can consider using other controls—like increased monitoring—to manage risk.

Another approach is for federal agencies to tailor guidance and regulations based on the risk level of different technology use cases. In some cases, the risk, in terms of the social costs relative to the social benefits, may be too great to use biometric identification technologies and agencies may consider banning certain uses of the technologies. Technology users could also consider emerging or potential risks. Because of rapid advancement in modern technologies, not all risks related to biometric identification technologies may be presently realized. For example, biometric data could be used in the future in ways for which they were not explicitly collected. The National Academies study on facial recognition technology noted that an outright ban on all facial recognition technology under any condition is not practically achievable, may not necessarily be desirable to all, and is in any event an implausible policy. However, the study noted that restrictions or other regulations can be appropriate for particular use cases and contexts.

OMB's memorandum requires federal agencies to mitigate emerging risks to rights and safety. Upon identifying new or significantly altered risks to rights or safety through continuous monitoring, periodic review, or other mechanisms, agencies must take steps to mitigate those risks, including, as appropriate, through updating an AI system to reduce its risks or implementing non-technical mitigations, such as greater human oversight. Where an AI system's risks to rights or safety exceed an acceptable level and where mitigation strategies do not sufficiently reduce risk, agencies must stop using the AI system as soon as is practicable.

Instituting Comprehensive Data Privacy Laws or Guidance

Comprehensive privacy laws or guidance can be enacted to address how biometric data can be collected, stored, and used. This consideration could help address stakeholder concerns related to data security and privacy protections, and lack of transparency.

Biometric data are particularly sensitive because they are inherently linked to an individual and cannot be changed. Private companies, state and local governments, and federal agencies that use biometric identification technologies are collecting these data, in some cases without sufficient guidance to ensure that the collection, use, and retention of biometric data is secure, and measures are in place to mitigate privacy and confidentiality risks.

In 2020, we reported that some federal laws are applicable to the commercial use of facial recognition technology, but their scope in addressing privacy concerns is limited.[47] The same is true for other types of biometric identification technologies. In most contexts, federal law does not explicitly address how personal data derived from biometric identification technologies may be used or shared. In 2015, we noted that the privacy issues that have been raised about facial recognition technology and other biometric technologies served as yet another example of the need to adapt federal privacy law to reflect new technologies.[48]

[47]GAO-20-522 (reiterating a 2013 suggestion that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace).

[48]GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015).

Accordingly, we reiterated our 2013 matter for Congress to strengthen the current consumer privacy framework to reflect the effects of changes in technology and the marketplace.[49]

There are examples of state or local policies—several of which have been passed in the last 5 years—that address data privacy concerns, including laws in states such as California, Connecticut, Florida, Illinois, Kentucky, Louisiana, Maryland, Montana, Oregon, Tennessee, Texas, Vermont, Virginia, and Washington.[50] However, these state laws differ in their approach to data retention and company liability. One stakeholder told us that state laws with different requirements create challenges for biometric identification technology vendors because they need to understand and adhere to privacy policies for each state when supplying services nationwide.

Executive Order 14110 states that federal agencies will use available policy and technical tools, including privacy-enhancing technologies where appropriate, to protect privacy and to combat the broader legal and societal risks that result from the improper collection and use of people's data. To pursue this aim, the executive order outlines a number of steps that federal agencies are to begin taking, including directing OMB to evaluate and take steps to identify information procured by agencies, particularly information that contains personally identifiable information and including information procured from data brokers. Within 180 days of the executive order, the director of OMB is to issue a request for information to inform potential revisions to guidance to agencies on implementing privacy impact assessments. The request for information is to seek feedback regarding how the assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI.

Improving Training and Guidance

Providing technology users with additional training and guidance can help them understand how to select and use biometric identification technologies appropriately, including how to monitor performance. This consideration could help address stakeholder concerns related to biased outcomes and technical expertise of users.

As discussed above, some stakeholders are concerned technology users do not have the technical expertise or adequate training to operate biometric technologies appropriately, particularly within the law enforcement use case. For example, there are no federal laws or regulations that require specific training for DHS or DOJ

[49]See GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013). We recommended that Congress consider strengthening the current consumer privacy framework to reflect the effects of changes in technology and the marketplace—particularly in relation to consumer data used for marketing purposes—while also ensuring that any limitations on data collection and sharing do not unduly inhibit the economic and other benefits to industry and consumers that data sharing can accord. As of March 2024, such legislation had not been enacted, although several privacy bills had been introduced, including some that address facial recognition technology.

[50]Example state laws include the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100-1798.199.100 (2020); Connecticut Data Privacy Act, Conn. Gen. Stat. §§ 42-515-42-525 (2022); Florida Digital Bill of Rights, Fla. Stat. §§ 501.701-501.721 (2023); Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1-14/99. (2008); Ky. Rev. Stat. § 61.9305 (2022); Allen Toussaint Legacy Act, 2022 La. Stat. Ann. §§ 51:470.1-51:470.6 (2022); Md. Code Ann., State Gov't §§ 10-1301-10-1308 (2018); Md. Code Ann., Lab. & Empl. § 3-717 (2020); Montana Consumer Data Privacy Act, 2023 Mont. Laws Ch. 681 (eff. Oct. 1, 2024); Oregon Consumer Privacy Act, 2023 Or. Laws Ch. 369; Tennessee Information Protection Act, Tenn. Code. Ann. §§ 47-18-3201-47-18-3213 (2023); the Texas Statute on the Capture or Use of Biometric Identifiers, Tex. Bus. & Com. Code Ann. § 503.001 (2009); Texas Data Privacy and Security Act, Tex. Bus & Com. Code Ann. §§ 541.001-541.205 (2023); the Vermont Data Broker Regulation, Vt. Stat. Ann. tit. 9, §§ 2430, 2433, 2446 and 2447; Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-575-59.1-584 (2021); the Washington Biometric Privacy Law, Wash. Rev. Code §§ 19.375.010-19.375-900 (2017).

employees using facial recognition technology or services to support criminal investigations. Additionally, some agencies at the federal, state, and local level may not have in-house expertise to interpret or assess the outputs from the biometric identification technologies they use. Users of these systems need to understand what a system is claiming (or not claiming).

One approach is for federal law enforcement agencies to establish their own training requirements for using biometric identification technologies. We previously recommended that federal agencies either implement training requirements for their staff or implement a process to periodically monitor whether staff have completed existing training requirements.[51]

Beyond just the law enforcement use case, OMB's memorandum requires agencies to ensure there is sufficient training, assessment, and oversight for operators of an AI system to interpret and act on the system's output and ensure that the human-based components of the system effectively manage risks from the use of AI. The memorandum states that training should be conducted on a periodic basis, determined by the agency, and should be specific to the AI use case, product, or service being operated.

Another approach is for federal guidance that directs technology users to select algorithms that meet minimum standards for accuracy. One stakeholder pointed out that there are analogous minimum standards in other industries—for example, safety standards for vehicles. NIST facial recognition testing is considered the benchmark standard for algorithm testing, but users and the public need to understand how to interpret and use the results. NIST officials told us that they have ongoing efforts to make their evaluation reports more understandable and user-friendly to a wider audience. This could help provide guidance to technology users on selecting the most appropriate algorithm and potentially reduce the number of instances in which NIST report findings are misinterpreted or miscommunicated in the press. Similarly, federal agencies could provide guidance to state and local agencies apprising them of risks inherent in their use of biometric identification for federally funded programs and providing recommendations for risk mitigation. For example, Department of Labor officials told us that after becoming aware of concerns state unemployment agencies were having related to disparate outcomes resulting from the use of biometric identification to complete unemployment insurance applications, the department issued a program letter advising states of the potential equity risks involved and advising them on a series of steps that state agencies could use to monitor potential equity challenges.

Agency Comments and Third Party Views

We provided a draft of this report to Commerce, DHS, DOJ, Education, Labor, Treasury, VA, as well as the FTC, OSTP, and Social Security Administration for review and comment. All 10 agencies provided technical comments, which we incorporated as appropriate. We also provided the stakeholders who participated in our interviews with an opportunity to review key sections of the report. Fifteen stakeholders provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Commerce, Homeland Security, Education; the Treasury, and VA; the Acting Secretary of Labor; the Attorney General; the Chair of the FTC; the Director of OSTP; the Commissioner of the Social Security Administration;

[51]GAO-23-105607.

and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-6888 or wrightc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Candice N. Wright
Director, Science, Technology Assessment, and Analytics

List of Committees

The Honorable Maria Cantwell
Chair
The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Frank D. Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report (1) describes information obtained from relevant literature and interviews with academic researchers and agency officials regarding the accuracy of biometric identification technologies across populations; (2) describes selected stakeholders' perspectives on how, if at all, use of biometric identification technologies affects access to resources or levels of inequality for communities that have faced historical patterns of disadvantage; and (3) identifies key considerations that could help address stakeholder concerns about the use of biometric identification technologies in communities that have faced historical patterns of disadvantage.

To address our objectives, we reviewed academic literature, government reports, and industry documents. We interviewed academic researchers with relevant experience, including federal agency officials, and conducted a series of semi-structured interviews with selected stakeholders, including academics, advocacy groups that represent communities potentially affected by biometric identification, users of biometric identification technologies, and technology developers and vendors.

We worked with a GAO research librarian to conduct a literature review. We identified 140 scholarly articles, conference papers, dissertations, and working papers, published from January 2012 through March 2023, by searching various databases including Scopus, SciTech Premium Collection and SciSearch®. We used search terms such as biometric technology, biometric identification, face recognition technology, etc. We reviewed each of the 140 documents identified for relevance and appropriateness for inclusion in our report. We also reviewed government reports and industry documents that we identified through background research or that were shared with us during our interviews. We used the results of our review to inform our understanding of stakeholders' perspectives on the accuracy and concerns about the use of biometric identification technologies in communities that have faced historical patterns of disadvantage, but we did not independently verify the accuracy of claims made in these reports.

To understand what is known about the accuracy of biometric identification technologies across populations, we interviewed 3 academic researchers with relevant experience that we identified through our review of the academic literature. We also interviewed officials from the National Institute of Standards and Technology and the Department of Homeland Security's Science and Technology Directorate.

To describe selected stakeholders' perspectives and identify key considerations that could help address stakeholder concerns, we reached out to over 185 potential stakeholders across different types of technologies, communities, and use cases. In selecting stakeholders, we prioritized (1) broad inclusion of different communities potentially affected by biometric identification, (2) representation of viewpoints discussing both positive and negative effects of the technologies, and (3) discussion of use cases with the greatest potential to affect communities and individuals. Our selection is not representative of all viewpoints on biometric identification technologies but provides examples of different perspectives and experiences.

We identified the potential stakeholders through multiple sources. One source was respondents to an Office of Science and Technology Policy October 2021 request for information on public and private uses of biometric technologies. We reached out to the respondents who appeared to have information related to communities that have faced historical patterns of disadvantage. We interviewed a total of 44 stakeholders representing technology users, technology developers and vendors, and organizations that represent communities

potentially affected by biometric identification technologies. These stakeholders include private organizations and governments at the federal, state, and local levels. Appendix III lists the stakeholders that we interviewed.

We conducted this performance audit from October 2022 to April 2024 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 any findings and conclusions based on our audit objectives.

Appendix II: Definitions

Communities: “Communities” include: neighborhoods; social network connections (both online and offline); families (construed broadly); people connected by affinity, identity, or shared traits; and formal organizational ties. This includes Tribes, Clans, Bands, Rancherias, Villages, and other Indigenous communities. Biometric identification and other data-driven automated systems most directly collect data on, make inferences about, and may cause harm to individuals. But the overall magnitude of their impacts may be most readily visible at the level of communities.

Equity: “Equity” means the consistent and systematic fair, just, and impartial treatment of all individuals. Systemic, fair, and just treatment must take into account the status of individuals who belong to underserved communities that have been denied such treatment, such as Black or African American, American Indian or Alaska Native, Asian, Hispanic or Latino, Native Hawaiian or Other Pacific Islander, and Multiracial persons; members of religious minorities; women, girls, and non-binary people; lesbian, gay, bisexual, transgender, queer, and intersex (LGBTQI+) persons; older adults; people with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality.

Rights, Opportunities, or Access: “Rights, opportunities, or access” describes the set of: civil rights, civil liberties, and privacy, including freedom of speech, voting, and protections from discrimination, excessive punishment, unlawful surveillance, and violations of privacy and other freedoms in both public and private sector contexts; equal opportunities, including equitable access to education, housing, credit, employment, and other programs; or, access to critical resources or services, such as health care, financial services, safety, social services, non-deceptive information about goods and services, and government benefits.

Underserved Communities: The term “underserved communities” refers to communities that have been systematically denied a full opportunity to participate in aspects of economic, social, and civic life, as exemplified by the list in the preceding definition of “equity.”

Definitions adapted from the Office of Science and Technology Policy’s Blueprint for an AI Bill of Rights, Making Automated Systems Work for the American People, October 2022.

Appendix III: Stakeholder Participation List

Accenture

ACT | The App Association

Action Center for Race and the Economy (ACRE)

Al Otro Lado

Arizona Department of Economic Security

Aware Inc.

Better Identity Coalition

Bipartisan Policy Center

Brooklyn Defender Services

Bureau of Alcohol, Tobacco, Firearms, and Explosives

Center for Democracy and Technology

Center for Law and Social Policy (CLASP)

Center for Policing Equity

Cisco Systems, Inc.

City of Portland

Clearview AI

Council on Islamic Relations (CAIR)

Coworker

Data & Society Research Institute

Data for Black Lives

Dev Technology Group

Digital Benefits Network, Beeck Center for Social Impact + Innovation at Georgetown University

Duke University

Electronic Privacy Information Center (EPIC)

Federal Bureau of Investigation

Fight for the Future

Former Salt Lake City Chief of Police

Georgia Tech Research Institute

Honolulu Police Department

ID.me

International Committee of the Red Cross

iProov

Keough School of Global Affairs, University of Notre Dame

Lawyers' Committee on Civil Rights Under Law

MITRE

National Center for Transgender Equality

New York State Education Department

Oregon Employment Department

Strauss Center for International Security Law

Transportation Security Administration

University of Washington Center for Research and Education on Accessible Technology and Experiences

U.S. Customs and Border Protection

U.S. Marshals Service

U.S. Secret Service

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Candice N. Wright, (202) 512-6888 or wrightc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Chris Murray (Assistant Director), Darnita Akers (Analyst-in-Charge), Dominique Belanger, Jenny Chanley, Philip Farah, Riley Grube, Patrick Harner, John Karikari, Mark Kuykendall, Alice Lin, Joe Rando, Craig Starger, and Carlin Van Holmes made key contributions to this report.

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

A. Nicole Clowers, Managing Director, ClowersA@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