United States Government Accountability Office

Report to Congressional Requesters

July 2020

FACIAL RECOGNITION TECHNOLOGY

Privacy and Accuracy Issues Related to Commercial Uses

GAO-20-522

GAO Highlights

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

July 2020

FACIAL RECOGNITION TECHNOLOGY

Privacy and Accuracy Issues Related to Commercial Uses

Why GAO Did This Study

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

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

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

What GAO Recommends

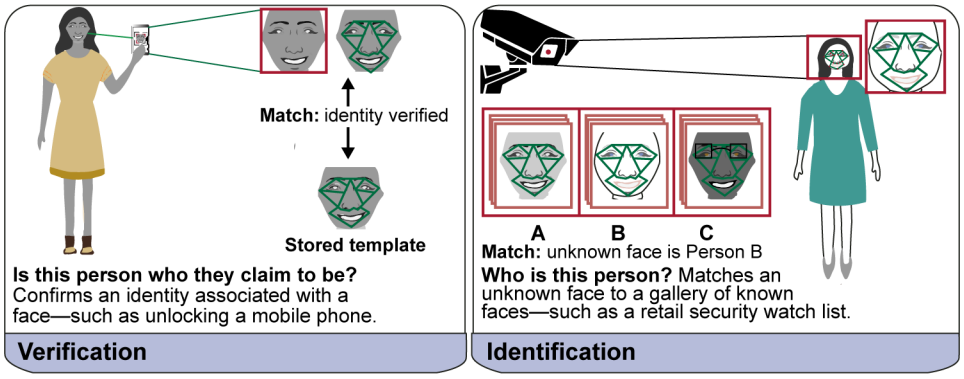
GAO reiterates its previous suggestion from a 2013 report (GAO-13-663) that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace.

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

What GAO Found

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

Functions of Facial Recognition Technology



Source: GAO analysis. | GAO-20-522

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

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

Contents

Abbreviations

APEC	Asia-Pacific Economic Cooperation
COVID-19	Coronavirus Disease 2019
CPC	Cooperative Patent Classification
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
IBIA	International Biometrics +Identity Association
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
USPTO	U.S. Patent and Trademark Office

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

July 13, 2020

Congressional Requesters

Facial recognition technology—which can be used to verify or identify an individual from a facial image—has increasingly been used in commercial settings since our 2015 report on the topic.[1] Most recently, some companies have started using the technology to monitor the spread of Coronavirus Disease 2019 (COVID-19)—such as to identify individuals that came in contact with people displaying symptoms.[2] However, advocacy groups and others have raised privacy and data security concerns about commercial uses of the technology, including its use for responding to COVID-19, particularly when these technologies are being used in the absence of specific guidelines or fully informed and explicit consent. Some of these concerns mirror privacy concerns discussed in our 2015 report, including, among other things, the technology's potential to identify individuals in public without their knowledge or consent and track their locations, movements, and companions. More recently, lawmakers and advocacy groups have expressed concerns that large collections of facial images may be combined with personal information that could be shared or sold. Further, studies have reported that the technology has higher error rates when used to identify individuals

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

[2]The outbreak of COVID-19 was first reported in Wuhan, China, and it has quickly spread around the globe. Under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), GAO has been mandated to periodically report on issues related to the U.S. government's preparedness for, response to, and recovery from the COVID-19 pandemic. An initial report on these efforts was issued on June 25, 2020, with subsequent reporting scheduled for a bimonthly basis. See, GAO, *COVID-19: Opportunities to Improve Federal Response and Recovery Efforts*, GAO-20-625 (Washington, D.C.: Jun. 25,2020).

belonging to certain demographic groups, which could lead to disparate treatment of certain populations. [3]

You asked us to examine the commercial use of facial recognition technology and related accuracy and privacy issues. This report examines (1) current and potential uses of facial recognition technology in the commercial sector, (2) the characteristics of facial image data sets assembled for commercial purposes and any related privacy and data security risks, (3) differences in how accurately the technology performs across demographic groups, and (4) privacy protections under federal and state law applicable to commercial use of facial recognition technology and privacy frameworks developed by private entities. The scope of this report does not include government use of facial recognition technology.[4] Further, this report discusses but does not focus on facial analysis, which interprets facial features to determine characteristics such as gender, race, age, and emotions. Instead, this report primarily focuses on the use of facial recognition technology in private and commercial sectors and how the technology is used to detect, identify, and verify individuals.

For all objectives, we interviewed stakeholders representing federal agencies, privacy advocacy groups, academics, industry associations

[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); 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 (January 2019); John Howard, Yevgeniy Sirotin, and Arun Vemury, "The Effect of Broad and Specific Demographic Homogeneity on the Imposter Distributions and False Match Rates in Face Recognition Algorithm Performance*," IEEE International Conference on Biometrics Theory, Applications, and Systems* (September 2019); and K.S. Krishnapriya, et al., *Characterizing the Variability in Face Recognition Accuracy Relative to Race,* arXiv:1904.07325v3 [cs.CV] (May 8, 2019). We discuss these and other evaluations and studies on the accuracy of facial recognition across demographics later in this report.

[4]We have ongoing work on law enforcement's use of facial recognition technology and expect this report to be issued in early 2021. Additionally, we expect to issue a report in August 2020 on the accuracy of U.S. Customs and Border Protection and Transportation Security Administration facial recognition systems, and whether they incorporate privacy protection principles. Furthermore, we have started work on a comprehensive review of the federal government's use of facial recognition technology. See also GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy,* GAO-16-267 (Washington, D.C.: May 16, 2016).

(representing both the biometrics industry and industries using the technology), vendors, and end-users. Federal agencies included the Federal Trade Commission (FTC) and the Department of Commerce's National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA). We interviewed representatives of six privacy advocacy groups and five industry associations (representing both the biometrics industry and industries using the technology), as well as five academic institutions or researchers. Additionally, we interviewed representatives from the Biometrics Institute and the European Association for Biometrics.[5] We identified these organizations and individuals through suggestions from interviews with agencies, privacy advocacy groups, and others; through reviews of our past work; and based on their participation in government initiatives and industry events.

In addition, we interviewed representatives of eight facial recognition technology vendors, selected because they were identified by agencies and privacy advocacy groups and because they represented a mix of technology developers and service providers. We also interviewed representatives of seven companies that use facial recognition technology in retail, in financial services, or at large venues (such as stadiums). We selected these industries because they were commonly cited in our literature review and among stakeholders we spoke with as current or potential users of facial recognition technology. The companies we selected represent a mix of companies of various sizes in different sectors within the selected industries. We also conducted a literature review of the following topics: commercial facial recognition technology uses (centered in the United States) since 2015; the development and training of facial recognition algorithms; concerns related to privacy; and performance differences for different demographics.

To address our first objective, we reviewed available market research reports on the facial recognition industry. We searched the database of the U.S. Patent and Trademark Office (USPTO) for patents related to facial recognition technologies granted from 2015 to 2019, and we

[5]The Biometrics Institute is a multistakeholder organization whose mission is to promote the responsible and ethical use of biometrics as an independent and impartial international forum for biometric users and other interested parties. Its members include banks, airlines, government agencies, biometric experts, privacy experts, suppliers, and academics. The European Association for Biometrics is a nonprofit organization whose role is to promote the responsible use and adoption of modern digital identity systems. Its members include government agencies, academics, and biometric industry companies.

interviewed USPTO officials. To address our second objective, we interviewed representatives of two data brokers (companies that collect and resell information) and five data consultants (who help companies obtain facial images).[6] We selected the data brokers because they were among the largest and most widely known in their industry, and we selected data consultants that (1) offer data collection services and (2) offer services or show expertise in facial recognition based on our research and suggestions from industry representatives. To address our third objective, we reviewed NIST vendor test reports and four 2019 facial recognition algorithm accuracy evaluations that were commonly cited by NIST vendor test reports and referenced among studies.

For our fourth objective, we reviewed and analyzed federal and state laws that govern the use of biometric information. For comparison purposes, we also reviewed the European Union's General Data Protection Regulation (GDPR) and literature describing its effects. We interviewed current representatives and one former representative from the European Data Protection Supervisor to discuss European Union privacy legislation. We also reviewed facial recognition privacy frameworks issued since 2014 by industry, privacy advocacy groups, and other organizations, which we identified through our literature review and interviews with industry representatives. In addition, we reviewed the privacy policies of 30 businesses that use facial recognition technology, which we selected to represent a diverse set of businesses across various industries identified in our literature review. For more information on our scope and methodology, see appendix I.

We conducted this performance audit from March 2019 through July 2020 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 our findings and conclusions based on our audit objectives.

Background

Facial recognition can be used to verify or identify individuals by their faces. It is one of several biometric technologies, which identify individuals by measuring and analyzing physical and behavioral characteristics such as fingerprints, hands, faces, eye retinas and irises,

[6]Data consultants gather or develop a facial image data set in response to a specific contract, as compared to data brokers, which sell access to already-existing data sets.

voice, and gait. Facial recognition technology converts a photo or video of a person—often called a probe image—into a template, or a mathematical representation of the face. For some facial recognition functions, if the technology detects a face, an algorithm then matches and compares the template to that of another photo and calculates their similarities.[7]

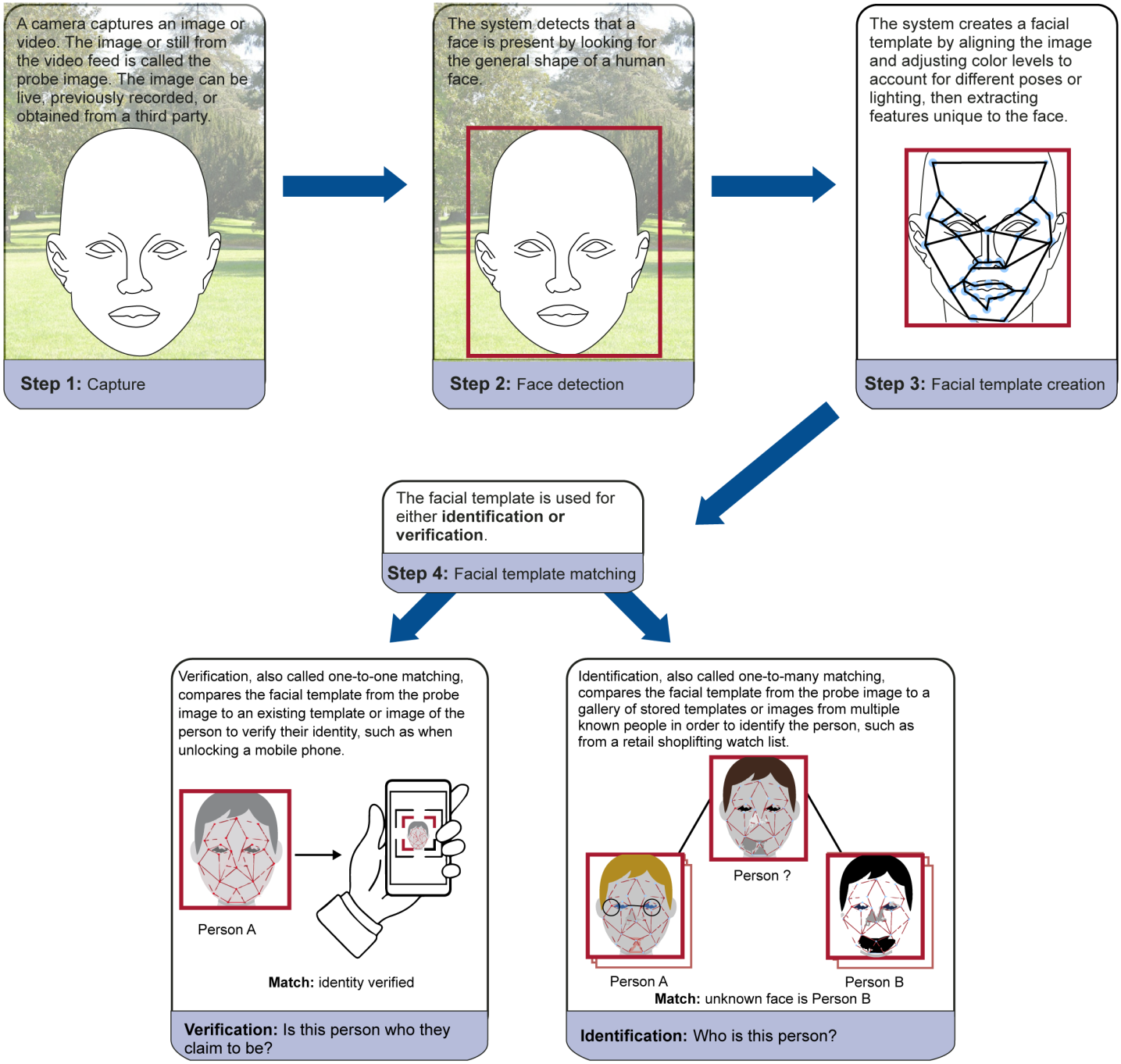
In summary, facial recognition technologies perform three basic functions:

- **Detection:** recognizing that there's a face in an image
- **Verification:** confirming the identity associated with that face
- **Identification:** matching an image of an unknown face to a gallery of known people

As shown in figure 1, facial recognition technology systems follow four steps to perform these functions.

[7]An algorithm is a set of rules that a computer or program follows to compute an outcome.

Figure 1: The Workflow of a Facial Recognition Technology System



Source: GAO analysis. | GAO-20-522

Facial analysis—sometimes also referred to as facial classification or characterization—is a technology distinct from facial recognition. Whereas facial recognition matches a face to a specific identify, facial analysis uses a facial image to estimate or classify personal characteristics such as age, race, or gender.

Modern facial recognition technology systems rely on machine learning, a component of artificial intelligence in which the algorithm uses training data to identify patterns and predict an answer to a question, such as "what parts of this face are important when figuring out who this person is?" Since around 2013, the use of deep neural networks—a type of machine learning algorithm—has led to a dramatic increase in the accuracy of facial recognition technology. In a deep neural network, training data are used to identify patterns and become more accurate as the algorithm "learns."

Parties involved in facial recognition technology for commercial use include the following:

- **Developers:** companies that create facial recognition algorithms
- **Vendors:** companies that leverage facial recognition algorithms that they or others have developed for consumer-facing products or services
- **End-users:** consumers or consumer-facing businesses that use facial recognition technology

Federal Roles and Responsibilities

FTC plays a role in enforcing key privacy and consumer protection laws. In December 2011, FTC hosted a workshop—Face Facts: A Forum on Facial Recognition Technology—that explored privacy issues associated with facial recognition technology. It issued a staff report in October 2012 that synthesized those discussions and recommended best practices for the use of the technology in the context of protecting consumer privacy.[8]

Within the Department of Commerce, NIST and NTIA have played a role in facial recognition technology. NIST conducts evaluations of facial recognition technology, including ongoing Face Recognition Vendor Tests, which test the accuracy of facial recognition algorithms that

[8]Federal Trade Commission, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (Washington, D.C.: October 2012).

developers voluntarily submit.[9] NIST also runs the National Voluntary Laboratory Accreditation Program for biometric testing, which evaluates the technical capability and risk management policies of third-party laboratories that seek accreditation to test biometric products. NTIA is the agency principally responsible for advising the President on telecommunications and information policies, including those related to privacy issues associated with facial recognition technology.

The Facial Recognition Commercial Market Is Expanding Across a Variety of Uses

The Market for Commercial Uses Is Expanding

Market research, patent data, and the growing number of vendors participating in NIST vendor tests all suggest that the number and types of businesses that use facial recognition technology are increasing.

First, market research reports that we reviewed show that from 2016 to 2019, the global facial recognition technology market generated about $3 to $5 billion in revenue. Between 2022 and 2024, revenue is projected to grow to $7 to $10 billion.[10] Market research also shows that more and different types of companies have entered the facial recognition technology market since our report in 2015.[11]

Secondly, as shown in figure 2, our analysis found that the number of patents granted by USPTO associated with facial recognition technology

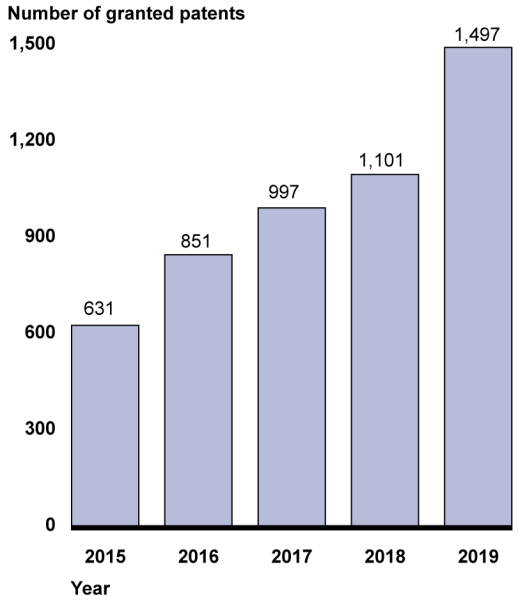
[9]See app. I for more information on the NIST Facial Recognition Vendor Tests we reviewed for this report.

[10]We did not independently verify the global facial recognition market revenues or forecasted revenue estimates. However, we did review information from several market research firms—Allied Market Research, Research and Markets, MarketsandMarkets, Straits Research, Visiongain, Market Research Future, and Variant Market Research—and found that the estimates fell within consistent ranges, with only one outlier.

[11]GAO-15-621.

rose from 631 in 2015 to 1,497 in 2019.[12] These patents were granted to technology, retail, entertainment, insurance, and telecommunications companies, among others.[13]

Figure 2: Number of Granted Patents Associated with Facial Recognition Technology by Year, 2015–2019



Source: GAO analysis of U.S. Patent and Trademark Office data. | GAO-20-522

Finally, the number of participants in NIST's Face Recognition Vendor Tests increased from 16 participants in 2013 to 99 participants in 2019, indicating that more companies are developing facial recognition algorithms.

Several factors appear to have contributed to the growth of facial recognition technology in commercial applications. First, the use of deep neural network technology, noted earlier, has increased the technology's accuracy and speed. Second, the cost of facial recognition technology

[12]A patent for an invention is the grant of an intellectual property right to the inventor, issued by the U.S. Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States.

[13]While some of these companies may not currently use the invention the patent is associated with, the growth in patents shows ongoing interest in the use of facial recognition technology and related applications.

has decreased, which has contributed to its growing use, according to stakeholders we interviewed. For example, systems are increasingly cloud-based, which can reduce end-user cost. Third, some stakeholders stated that the adoption of facial recognition in consumer devices, such as to verify identity on smartphone applications, has made consumers more comfortable with the technology.

Finally, in the financial services sector, according to two payment service providers, wider adoption of facial recognition technology was bolstered, in part, by regulatory changes included in the European Union's payment services regulation. According to both of the payment service providers we spoke with, this regulation requires strong user authentication for payments which includes two-factor authentication—one of which can be biometric, such as face recognition.[14]

While these are indications that the commercial market is growing, privacy and other concerns related to certain facial recognition technology applications may have slowed the adoption in some industries. The *2019 Biometrics Institute Annual Survey* found that 74 percent of respondents agreed that privacy concerns are holding back the market for biometrics.[15] Furthermore, according to some stakeholders we spoke with, privacy and other concerns related to certain facial recognition technology applications may have led some industries or companies—such as retailers—to limit or curb their use of facial recognition technology. For example, representatives from an industry association we spoke with told us that some retail businesses do not want to risk alienating their customers by using facial recognition technology. In addition, one facial recognition technology vendor we spoke with said it had recently experienced a reduced market for retail clients that may be due to negative customer perceptions of the technology. Furthermore, all three retail end-users we spoke with said that they are not using facial recognition as a result of privacy concerns or customer perceptions, but instead are using facial detection or facial analysis for purposes such as understanding customers' foot traffic without identifying them.

[14]*See* Council Directive 2015/2366, 2015 O.J. (L 337) 35.

[15]According to the Biometrics Institute, respondents included Biometrics Institute members and other key stakeholders. Biometrics Institute, *State of Biometrics Report* (October 2019), accessed January 30, 2020, https://www.biometricsinstitute.org/wp-content/uploads/State-of-Biometrics-Report-2019-eBrochure-compressed.pdf.

Facial Recognition Has a Variety of Commercial Applications

Stakeholders and literature we reviewed cited several major types of functions that use facial recognition technology, many of which were similar to those we reported in 2015, such as secure access, safety and security, photo identification and organization, and marketing and customer services. Newer functions of the technology identified by stakeholders and literature included payment processing and attendance tracking and monitoring.

- **Secure access.** Secure access was one of the most commonly cited uses identified by stakeholders and literature we reviewed. Facial recognition technology can be used to control physical access—for example, by using a camera to confirm the user's identity and provide access to a locked door, event venue, or automobile. In addition, facial recognition can be used to control electronic access—for example, to unlock personal computers or smartphones or access online accounts in lieu of a password, which can help prevent fraud. According to a facial recognition technology vendor we spoke with, a 2018 survey it conducted found that 54 percent of Americans either already use a device with facial recognition built in or plan to use one to protect their personal data.[16]
- **Safety and security.** Some retailers, casinos, apartment buildings, and event venues use facial recognition technology for safety and security purposes. The retail industry uses facial recognition technology to deter theft. According to the *2019 National Retail Security Survey*, about 6 percent of stores surveyed had implemented facial recognition across all stores for loss prevention purposes.[17] In addition, some casinos in the United States have been using facial recognition systems to help them identify known or suspected gambling cheaters and members of organized crime networks. Industry representatives told us casinos also allow people with gambling addictions to voluntarily enroll in a program that uses facial recognition technology to recognize them and notify management and prevent them from entering the casino. Venues are also using it for safety at large events, such as to identify fans who have been banned from the venue.
- **Photo identification and organization**. Facial recognition is used by some social media applications to identify and "tag" users' friends.

[16]FaceFirst survey conducted January 4–5, 2018.

[17]National Retail Federation and Richard Hollinger, *2019 National Retail Security Survey* (June, 6 2019), accessed August 27, 2019, https://nrf.com/research/national-retail-security-survey-2019.

Consumers and businesses can also use it to index images and video as a way of organizing content. For example, media companies use it to search their archived video and images. In addition, according to its website, one company partners with summer camps to provide families with access to online photo galleries that use facial recognition software to automatically identify and notify parents when photos of their children are uploaded.

- **Marketing and customer service.** The use of facial recognition technology for marketing and customer services has also expanded in recent years. Retailers and others can use it to identify VIP customers to send them targeted marketing or provide them with a more personalized experience. Hotels and rental car businesses can also use facial recognition to improve customer service by facilitating the check-in process. For example, according to a company press release, two companies partnered to implement integrated facial recognition technology for hotel check-in, including credit card authorization, at 50 hotels in a district in China. Additionally, one rental car company in the United States has partnered with a biometrics provider to implement an optional expedited check-in using facial recognition or an alternative biometric authenticator, such as a fingerprint.
- **Payment.** Some companies have implemented or are exploring using facial recognition for payment processing. For example, two major payment processing companies are exploring ways for consumers to use the technology for purchase, according to company representatives. For example, during checkout in a mobile application, consumers would authorize payment via facial recognition by taking and transmitting a photograph on their phone.
- **Attendance tracking and monitoring.** In the past few years, a new use of facial recognition technology has emerged: tracking attendance of students, employees, or those attending events. For example, some schools and universities use the technology to identify students in the classroom and keep track of their course attendance. In addition, one market research report stated that many educational institutions are using the technology to manage and authenticate the identities of students throughout online sessions, examinations, and certification activities. The technology is used in a similar manner by some companies to track employee time and attendance or to determine who has attended events such as conferences.
- **Other potential uses.** Other current and potential uses for facial recognition technology have been cited in literature we reviewed. Hospitals and other health care providers are exploring the use of

facial recognition technology to verify the identity of a patient and link to that patient's health care data. In addition, some companies are developing applications using facial recognition to track the spread of COVID-19. For example, one company's website describes using thermal imaging cameras to measure building occupants' body temperatures and using facial recognition to identify who may have come into contact with those who displayed fever symptoms. Additionally, some ride-hailing services have used the technology to verify the driver and passenger. Another new use of the technology is to verify voters. In 2018, West Virginia allowed citizens to use a mobile app to vote. First, voters took a photo of their government identification and a self-video of their face using their mobile phone, which was then uploaded to the mobile app to verify their identify. Once approved, they could cast their vote through the mobile app.

In addition, technologies using facial detection and facial analysis—which are distinct from facial recognition—are used in the following applications, according to stakeholders we interviewed:

- **Facial detection.** Facial detection is commonly used to track counts or movements of people without identifying them. For example, the technology can be used to count people in stores, amusement parks, or waiting in lines. Stakeholders told us that one of the more common uses by retailers is to track foot traffic, which can provide useful information to help store operations. For example, one company we spoke with told us that they use facial detection technology because it is critical to understand customer flows, such as peak times, where customers go, and how long they stay.
- **Facial analysis.** One vendor and two retailers we spoke with are using facial analysis to expedite the identification of a customer's age for the purpose of buying controlled substances, such as alcohol. According to some privacy advocacy groups we spoke with, one digital recruiting company is using facial analysis to analyze prospective employees in connection with hiring decisions. Retailers and others can use facial analysis to analyze emotions, gender, and age to deliver targeted signs or billboards. Some stakeholders and a market research report discussed the possibility of analyzing facial features to help detect disease or monitor changes over time.

Facial Image Data Sets Raise Varying Issues about the Use, Security, and Sharing of Personal Information

Privacy and Security Risks Posed by Facial Image Data Sets Can Depend on the Data's Source, Function, and Application

Facial recognition technology is often dependent on the large-scale collection of facial images (facial image data sets). Privacy advocacy organizations, government agencies, academics, and some industry representatives have raised privacy and security issues associated with personal data collected in conjunction with these data sets. Many of these issues mirror concerns about the collection, use, and sharing of personal data more broadly by commercial entities. Among the key data privacy issues that have been raised with regard to facial image data sets are the following:

- **Data security.** Facial image data sets raise the same security concerns as those associated with any personal data—for example, they could be subject to data breaches, resulting in sensitive biometric data being revealed to unauthorized entities.[18] Because a person's face is unique, permanent, and therefore irrevocable, a breach involving data derived from a face may have more serious consequences than the breach of other information, such as passwords, which can be changed.
- **Consumer control over personal information.** As we reported in 2015, one concern is that information that is collected or associated with facial recognition technology could be used, shared, or sold in ways that consumers do not understand, anticipate, or consent to.[19]

Facial image data sets can be built or obtained from a number of different private and public sources, and the nature of the privacy issues related to these data sets can vary depending on the source of the images and the process by which they are collected. Sources for the images in these data sets can include the following:

[18]GAO-15-621, 16–17.

[19]GAO-15-621, 15–16.

- **Company interactions with consumers.** Consumers may provide facial images and identifying information when using a commercial service. For example, a verification photo may be required when signing up for biometric account log-in, or a customer may choose to upload photographs on image-hosting or -sharing platforms, such as social media. Companies have used these images to create their own data sets. In its 2012 report on best practices for the use of facial recognition technology, FTC staff identified and made suggestions to address concerns about the secondary use of facial images.[20] For example, the report states that if a company stores images collected from consumers for purposes of sharing them with third parties, it should explicitly provide consumers with this information before they upload their image. Privacy advocacy groups have expressed concerns that sometimes facial images collected for one use are repurposed for an entirely different use, without clear notice to the people whose face data are collected. For example, a photo storage company shifted its business model to facial recognition and used photos collected from photo storage to train face recognition algorithms, according to some privacy advocacy groups and a representative from the company.
- **Volunteers or paid subjects.** Companies may sometimes collect images—either directly or via third-party consultants—from volunteers or paid subjects who are not necessarily consumers of the company's product. According to a company we spoke with, consent may be explicit in these situations, but subjects may not retain control over how the images are used.
- **Web scraping.** Data brokers, advertisers, or other parties use web scraping—automated software that extracts data from websites—to search the web for information about individuals, and they extract and download bulk information from websites that contain consumer data. In some cases, third parties have been known to use web scraping to collect images that include faces. The source of these images can be, among other things, social media or career networking websites, news articles, or internet search results.

Third parties performing web scraping may not always obtain consent of the individuals in the images. For example, a facial recognition start-up

[20]See Federal Trade Commission, *Facing Facts*, 12. The report states that if the company is storing images for a purpose that is not consistent with the context of the transaction taking place, the company should provide the consumer with information on why they are storing images at a just-in-time point.

company is currently facing a number of lawsuits alleging it used web scraping to amass a data set of 3 billion facial images from millions of websites without obtaining the consent of individuals in the images or the companies whose websites were scraped.[21] While there is no current blanket ban on web scraping, there are various legal restrictions that may be applicable depending on the actions of the company scraping the data, the licenses employed by the data holder, and the way in which the data are used.

- **Public data sets**. There are several facial image data sets that are publicly available. These data sets can be created by academics or other developers or be derived from government sources (as described later in this report). The data sets vary in how the images they contain were assembled, and some include images that were scraped from the web. A few large data sets have been removed from the internet by their creators in response to concerns raised that the data sets lack consent from individuals whose images they contain. However, privacy advocacy groups and researchers have noted that data sets can be copied and shared even after being removed from public access by their creators.

Privacy Considerations Based on the Technology's Function

Not all applications or functions using facial recognition or related technologies collect or store facial images. As a result, the privacy and data security risks can vary according to the function of these technologies.

- **Face detection.** Because this function detects whether a face is present but does not attempt to recognize that face, it generally does not require the collection or storage of identifiable information.[22] Since it is not identifiable or linked to an individual and does not attempt to match identities, it is considered low risk and generally requires less rigorous privacy protections. A more advanced version of face detection can separate each individual face as unique, without identifying it, and track that face with a unique persistent identifier (a temporary identification number) for applications such as preventing

[21] *See eg.* Class Action Complaint, Calderon v. Clearview AI, Inc., No. 1:20-cv-01296 (S.D.N.Y. 2020); Class Action Complaint, Mutnick v. Clearview AI, Inc., No. 1:20-cv-00512 (N.D. Ill. 2020); Class Action Complaint, Hall v. Clearview AI, Inc., No. 20-cv-00846 (N.D. Ill. 2020); Complaint, State of Vermont v. Clearview AI, Inc. (2020 Vt. Sup. Ct. Civ. Div. Chittenden Unit).

[22] Face detection may be used as part of a facial recognition system or it may be a standalone technology used only to determine when a face is present. In this context, we are referring to standalone face detection.

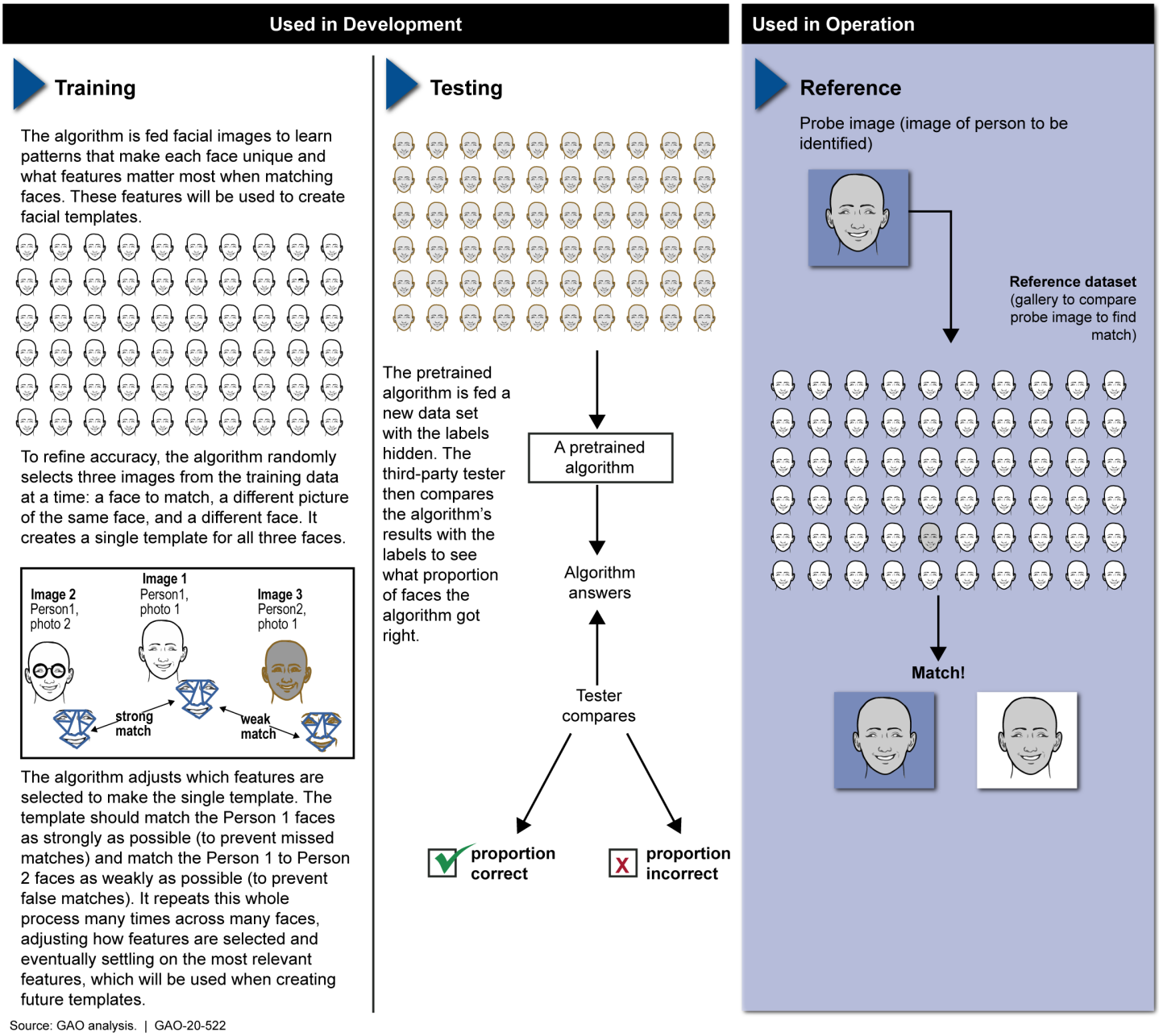
double-counting when analyzing foot traffic in a retail setting. However, because the unique persistent identifier tracks the face, there is a risk of potential future identification if it is linked to other data used to profile or identify the individual.

- **Verification.** Because this function matches a face to a known identity, it typically requires the use of a data set with identifiable information (e.g., facial template, image, name, or other personally identifiable information) to compare to an image. As a result, this function poses greater privacy and security risks than face detection. For example, a data breach of a facial recognition system used for verification could expose both personally identifiable information used to identify a face and the image or template itself.
- **Identification.** Facial recognition systems used for identification typically pose greater privacy and security risks than those used for verification because they contain more personally identifiable data. Systems used for identification compare "one-to-many" (instead of "one-to-one" for verification) and therefore typically have data sets containing more images and individual identities. For example, an application verifying a mobile phone owner's identity will include only the probe image and a stored template for the phone's owner, whereas an application identifying people entering a shop may include a much larger number of images and identities, such as those of suspected shoplifters.

Privacy Considerations Based on Type of Data Set

Facial recognition technology can involve three types of data sets—training, testing, and reference (see fig. 3). The use of these data sets depends on what function the technology performs and what the particular end-user is trying to do with the technology.

Figure 3: The Data Sets Involved in Facial Recognition Technology



Source: GAO analysis. | GAO-20-522

Training and testing data sets. Training and testing data sets are sets of facial images used to develop or assess a facial recognition algorithm. Training data sets are used to "train" modern facial recognition algorithms to identify patterns, such as relevant facial features, in order to improve overall algorithm performance.[23] Testing data sets are used to assess the performance of pretrained algorithms by running new facial images through the algorithm and assessing accuracy, speed, or other outcomes of interest.[24] Some of these training and testing data sets are publicly available and can contain millions of images from a number of sources (see table 1).

Table 1: Selected Large-Scale Publicly Available Facial Image Data Sets

Data set	Year	Number of images	Number of subjects
CASIA WebFace	2014	500,000	10,000
VGGFace	2015	2.6 million	2,500
MS-celeb-1M[a]	2016	10 million	100,000
Megaface	2016	4.7 million	650,000
VGGFace2	2017	3.31 million	10,000
UMDFaces-Videos	2017	22,000	3,000

Source: GAO presentation of data in the European Commission Study on Face Identification Technology, 2019. | GAO-20-522

[a]The largest data set, MS-celeb-1M, was removed from the internet by its creator, but data sets can be copied, shared, or edited even after being removed from public access. We identified at least one copy of MS-celeb-1M that was publicly available for download as of March 10, 2020.

Photographs in some publicly available data sets may have been collected without the knowledge or consent of the individuals included. For example, one researcher reviewed 30 publicly available facial image training data sets released between 2006 and 2018 and found that together they contained 24 million images of approximately 1 million individuals. According to the researcher, those individuals did not provide

[23]Training data sets are particularly important for algorithms that use machine learning, such as deep neural networks.

[24]Testing can happen at multiple stages of an algorithm's development. Developers may test internally during training (also referred to as validation), submit to a third party such as NIST for external testing during development, or submit final commercially available algorithms for external testing. Although publicly available image data sets can be used for training or testing, according to academics, developers, and NIST, a single algorithm should not be trained and tested on the same data since the algorithm would already be familiar with the patterns of the faces being used to test in that scenario.

explicit consent to the use of their images.[25] These images were collected using web scraping, with most of the images obtained from internet search engines or image hosting sites, as well as a smaller number from various websites, closed circuit television, or mugshots.

Another privacy concern is that these data sets may include or reveal personal information beyond the individual's image. Four of the 30 publicly available existing data sets noted above contained images taken from a long-range surveillance camera, closed circuit television surveillance cameras, or a public cafe webcam. The data sets contain information that could potentially be identifiable, because the two surveillance camera data sets included data on the time and day of the week of collection, and the data set titles and publication information also included locations where the images were taken. Several privacy advocacy groups and academics have raised concerns that location and time data could allow individuals in anonymous data sets like these to be identified.

Some training and testing data sets are not publically available and are considered proprietary information. Industry representatives and academics we interviewed said that they mostly collect their own proprietary training and testing data, but sometimes also use publicly available data sets or a combination of both. Stakeholders said that they treat their training and testing data, along with algorithm code, as secrets and do not share them—even with third-party evaluators such as NIST, testing laboratories, or academic evaluators. Similarly, testing data sets assembled by third-party evaluators are not shared with developers whose algorithms will be tested because an evaluation of an algorithm's performance is best done using facial images it has not encountered before.

Additionally, third-party testers may not release test data sets publicly due to privacy concerns. NIST officials told us they cannot publicly release the majority of their testing data because agreements with agencies that provide the source data prohibit their release. As a result, specific characteristics of proprietary training data sets, such as size, facial image content, and any other data stored alongside facial images, are known only to the data set's creator. These creators may report summary characteristics of the facial images within a data set, such as the number

[25]Adam Harvey and Jules LaPlace, "MegaPixels: Origins, Ethics, and Privacy Implications of Publicly Available Face Recognition Image Datasets," last modified April 18, 2019, accessed April 19, 2020, https://megapixels.cc.

of men and women, but they may not report detailed demographic breakdowns that include other characteristics.

Developers and academics said that existing publicly available data sets are not representative and that creating such data sets is challenging.[26] For example, a 2019 review of eight prominent facial image data sets found that six of the eight data sets were comprised of between 81.2 and 94.6 percent lighter-skin individuals.[27] But stakeholders, including several privacy groups, noted that creating a representative data set is challenging due, in part, to the tension between maintaining people's privacy and data security versus creating large and diverse facial image training and testing data sets. For example, in an effort to support more accurate algorithms, a developer publicly released a large data set aimed at providing demographically balanced training data to help reduce algorithm performance differences for underrepresented demographics. However, the developer removed links to the data set from its website after the company was sued under the Illinois Biometric Information Privacy Act.[28]

Reference data sets. Reference data sets are used to verify or identify a face by comparing that face to a stored identity in the reference data set. These data sets, also called galleries, are created and controlled by the end-users of facial recognition technology and hold pre-enrolled facial templates alongside confirmed identities. Examples of reference data sets include a gallery of employee photos used to verify access to a building, a gallery of suspected shoplifters used to compare to live surveillance in a store, or a phone owner's facial template for device unlocking.

Reference data sets are not public but may present privacy and security risks because the facial images or templates they contain generally

[26]As discussed later in this report, the development of more diverse, representative data sets may help to improve the accuracy of facial recognition technology across different demographic groups. Trainable algorithms perform better when they are exposed to more, and more diverse, data. Small or nondiverse data sets may lead an algorithm to identify patterns that are true for that data set but would not hold true for the variety of faces in the real world, leading to decreased accuracy.

[27]Michele Merler, Nalini Ratha, Rogerio Feris, and John Smith, *Diversity in Faces*, arXiv:1901.10436v6 [cs.CV], April 8, 2019.

[28]In January 2020, individuals brought a class action lawsuit under the Illinois Biometric Information Privacy Act against IBM for alleged violations of the act resulting from IBM allegedly collecting, storing, and using individuals' biometric identifiers and biometric information without informed written consent. We discuss the Illinois Biometric Information Privacy Act in more detail later in this report.

include information such as name, date of birth, address, or other identifying information. For example, representatives of one financial institution we spoke with said that they stored member identification numbers with the biometric information linked to their account, and a privacy advocacy group said that location data may also be commonly collected in reference data sets. Privacy advocacy groups and others have expressed concerns about reference data sets because of the personally identifiable information associated with the facial image, and the sensitive nature of the facial images themselves.

Depending on the end-user, facial images for reference data sets may or may not be obtained with explicit consent. For example, an employee whose image is used for building access through facial recognition likely provided consent, whereas an individual whose image is in a reference data set of potential shoplifters likely did not. Privacy advocacy groups have raised concerns that consumers may not know they are in a reference data set and may not have a way to request their removal. This could have adverse consequences if, for example, an individual was unaware they were wrongly included in a data set of suspected shoplifters that was shared among a retailer's locations.

Stakeholders told us there are ways to mitigate some of the privacy and security risks of facial image reference data sets. For example, multiple end-users we spoke with said that personally identifiable information is encrypted and stored separately from facial images or templates for data security purposes.[29] Additionally, some developers and end-users said that end-users could protect the privacy and security of individuals in reference data sets by destroying the images after they are used to create facial templates. However, the subjects whose faces are captured by a system do not have control over whether or not the facial image used to create a template is destroyed. Facial templates are sets of numbers, rather than individuals' images, and multiple vendors and end users told us that it is very difficult, if not impossible, to reconstruct an image from a template. As a result, the inadvertent release of facial templates, such as through a data breach, would likely present less of a privacy concern than release of a full image. In addition, one vendor we spoke with developed a feature that instantly blurs facial images during processing to protect privacy.

[29]Such encryption is generally voluntary and is not universally required by federal law.

Facial Image Data Sets Could Be Sold or Shared, but the Extent to Which They Are Is Unknown

Facial image data sets could be sold or shared by various parties; however, the extent to which such data sets are being sold is unknown. As noted earlier, privacy concerns exist related to the potential for data related to facial recognition technology to be sold or shared—particularly without the knowledge or consent of the affected individuals. These concerns are underscored by the dramatic increase in recent years in the amount of personal data that information resellers and other companies collect and share.[30] Among the potential sellers or sharers of these data sets are data brokers, data consultants, and state departments of motor vehicles.

Data brokers. Data brokers, also sometimes known as information resellers, are companies with a primary line of business that involves collecting, aggregating, and selling personal information to third parties. Two large data brokers we spoke with said that facial images could potentially be added to existing identification and fraud prevention data sets that they sell. One data broker said that facial images could help clients verify customer identities to reduce fraud, but that it would need to analyze industry best practices and regulatory expectations before selling such images. Another data broker noted that it did not have immediate plans to include facial images in its offerings because linking online and offline presence for a customer can be done using other information, such as location data, email addresses, and phone numbers. However, the data broker said that it might add facial images to future offerings to assist clients with verifying identities.

Data consultants. Another potential source of facial images is third-party consultants who assist companies with obtaining images to create new data sets or augment existing company data sets. These consultants assist client companies by identifying data needs, analyzing existing company data, supplementing company data with new data, or creating new data sets for the client. Data consultants may assist with facial images for training, testing, or reference data sets, obtained through methods including data supplied by client companies, existing public data sets, images collected using web scraping, or images obtained from hired individuals. Data consultants we spoke with told us they did not retain or sell images from client to client, and that they operated under contract with each individual client.

[30]For example, see GAO, *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps*, GAO-19-621T (Washington, D.C.: June 11, 2019).

Departments of motor vehicles. Facial image data sets can also be shared or sold by state departments of motor vehicles. Currently, these departments typically sell or share such facial images to law enforcement, courts, or prisons, but the Driver's Privacy Protection Act also lists certain limited permissible uses for specified users, including insurers or insurance support organizations, private investigators or private security services, private employers, researchers, and private toll transportation facilities. Such private or commercial entities could legally purchase facial images from departments of motor vehicles willing to sell them for the purposes of carrying out permissible uses authorized in the Driver's Privacy Protection Act, although in many cases such disclosure requires the express consent of the individual whose image is to be disclosed.[31]

Facial Recognition Performance Differences Exist for Certain Demographics but Could Be Mitigated

Evaluations by NIST and others have found that many facial recognition systems perform differently among demographic groups, which has raised concerns about disparate treatment that may result from the use of this technology. No consensus exists on the exact cause or interaction of multiple causes of these performance differences. To mitigate these differences, stakeholders have suggested larger and more representative data sets, better adherence to image quality standards, and other measures.

While Accuracy Has Improved, Performance Differences Often Exist for Certain Demographics

NIST Performance Tests

NIST's recent evaluations of facial recognition algorithms found significant improvements in the accuracy of facial recognition technology, but they have found that performance differences exist for certain demographic groups.[32] However, a small number of one-to-many identification

[31]*See* 18 U.S.C. § 2721. The law references permissible uses generally for all personal information held by state departments of motor vehicles, which may include photographs or facial images. It is not implied that images are currently being shared with each of the entities listed.

[32]NIST has been evaluating the performance of facial recognition algorithms under different methodologies since 2000 and is noted worldwide for its contributions to the field of biometrics testing.

algorithms among those tested by NIST achieved accurate performance across all demographic groups, with no performance differences among groups.[33]

NIST's evaluations include ongoing Face Recognition Vendor Tests (which we refer to as vendor tests), used for measuring identification (one-to-many identity matching) and verification (one-to-one identity matching).[34] According to NIST's identification vendor test in 2018, facial recognition algorithms have become more accurate since 2013 because of new deep neural network algorithms that use large amounts of training data to identify patterns and become more accurate. NIST described the use of deep neural network algorithms as a revolution that quickly led to massive gains in accuracy. NIST's identification vendor test showed that certain high-performing algorithms had error rates as low as 0.2 percent for good quality photos, which was 20 times better than the error rates recorded in the testing NIST conducted before 2013.

Despite the overall increase in accuracy, NIST's December 2019 vendor test that evaluated variations in accuracy across demographic groups for verification and identification demonstrated performance differences between demographic groups.[35] NIST tested 189 mostly commercial algorithms from 99 developers.[36] These performance differences varied by the algorithms tested, with some performing better than others. In the report, NIST stated that facial recognition algorithms differed in accuracy widely by race, ethnicity, or country of origin, as well as by gender and age.[37] However, differences in false positives across demographic groups

[33]For the purposes of this report, we refer to accuracy when we are discussing the algorithm's ability to match images. We use performance in a broader sense, which can include other elements of a facial recognition system, such as failure to create a facial template in order to perform a match.

[34]NIST Face Recognition Vendor Tests are voluntarily submitted by developers, which include researchers and developers from industry, research institutions, and academia.

[35]NIST Interagency Report 8280. This report was the most recent NIST vendor test at the time of our review.

[36]As noted above, NIST tests algorithms from academics or other noncommercial research institutions in addition to commercial developers.

[37]For purposes of this report we use the term "gender" instead of "sex" because it is more commonly used in the wider literature evaluating both facial recognition and facial analysis. Additionally, all of the facial analysis companies we interacted with used the term "gender" when describing their algorithms developed for gender estimation.

Definitions of Accuracy and Performance for Facial Recognition

Technical literature from the National Institute of Standards and Technology and some academics refer to performance differences between demographic groups processed by a particular algorithm as "differential performance" or "demographic differentials." Demographic performance differentials are measured and reported in a number of ways:

False positive: incorrectly declaring two images to be a match when they are actually from two different people (sometimes called a type I error or false match).

False negative: failing to declare two images to be a match when they are actually from the same person (sometimes called a type II error or false non-match).

Failure to enroll rate: the proportion of facial images where the algorithm is unable to create a facial template, and thus unable to perform verification (one-to-one) or identification (one-to-many) matching.

Source: GAO analysis. | GAO-20-522

were undetectable for a small number of one-to-many identification algorithms. The extent of performance differences varied by the developer, type of error, and quality of the facial images. (See sidebar for definitions of accuracy and performance terminology).

In general, for verification and identification vendor tests, algorithms performed more accurately on white males. White males had the lowest false positive rate—where an algorithm incorrectly finds two images to be a match when they are actually from two different people—while black females had the highest false positive rate. In verification algorithms, false positive rates for white males and black females varied by factors of 10 to more than 100, meaning the lowest-performing algorithm could be over 100 times more accurate on white male faces than on black female faces.[38] Additionally, for verification and identification vendor tests, false positives were higher for women than men.

For verification vendor tests, NIST also found elevated false positive rates for the elderly and children, and these rates increased with increasingly older or younger subjects. NIST also found that false negative rates—where an algorithm incorrectly fails to match two images when they are from the same person—did not vary as widely as false positives and tended to vary more by developer. As discussed earlier, a small number of the one-to-many identification algorithms had no differences when it came to accuracy, regardless of demographics.

Effect of Different Thresholds

Thresholds—the balance between false positives and false negatives at which an algorithm can be set by an end-user or developer—are separate from accuracy. However, thresholds could have an effect on accuracy for certain demographics. Specifically, there is a tradeoff between false positives and false negatives in that lowering one means raising the other, but this tradeoff can vary significantly among algorithms and at different levels at which a threshold can be set. NIST performs some tests of algorithms at a fixed threshold in order to make comparisons between algorithm accuracy on different demographics.

In real-world operation, end-users of a facial recognition system decide on a threshold based on their tolerance for false negatives—missing a match they would have wanted to make—and their willingness to commit resources, such as labor to sift through a large amount of false positive

[38]Prior editions of NIST verification testing found similar trends.

results to prevent a missed identification.[39] However, end-users may not be aware that they have the option to adjust the threshold or may not have received the appropriate training to do so. According to a representative from the Partnership on AI, it is important that developers ensure that end-users understand that they can adjust this threshold to fit their tolerance for false matches. For example, in a low-risk scenario, such as automatic identification of cruise ship passengers in images taken by an onboard professional photographer, a missed match may only result in a missed sale of a photograph. Therefore, an end-user may not want to commit resources, such as staff time, to sifting through false positives. On the other hand, in a high-risk scenario, such as identification of passengers when boarding a cruise ship, a missed match could be costly for an end-user—such as resulting in onboarding a passenger on a watch list. Therefore, the end-user would likely be more willing to commit resources to sift through false positives to prevent such a miss. Figure 4 illustrates the effect of different thresholds on algorithm results.

[39]In a scenario with a low threshold that returns many faces that could include the true face along with a number of false positives, the algorithm results would require a human reviewer to review and determine which candidate is most likely the identity that matches the probe image.

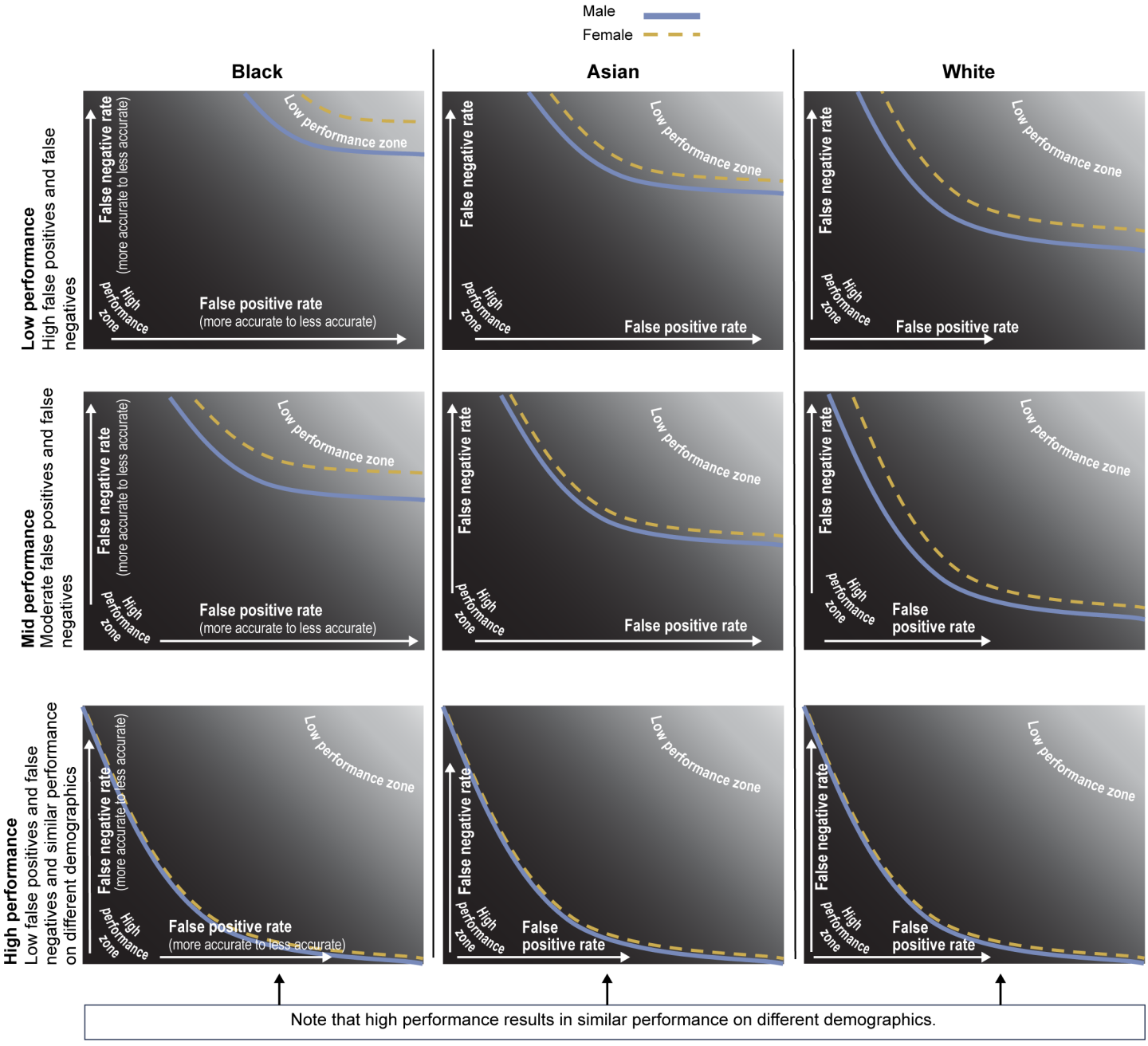
Figure 4: The Effect of Facial Recognition Match Thresholds on Algorithm Results

Source: GAO analysis of Partnership on AI interactive graphic. | GAO-20-522
https://www.partnershiponai.org/facial-recognition-systems

Note: The Partnership on AI is a global nonprofit organization whose mission is to support the responsible development and use of artificial intelligence. Its interactive graphic can be found at https://www.partnershiponai.org/facial-recognition-systems/.

The threshold tradeoff described above is different from an algorithm's overall accuracy. An accurate algorithm can lower both false positives and false negatives. A common way to visualize accuracy is to plot false positive and false negative rates on a chart, with each error rate on each axis of the chart from low to high (see fig. 5). In drawing a line of the algorithm's performance at different false positive rate thresholds on that chart, one can see the tradeoff between false positives and false negatives, as well as the overall accuracy of the system. High-performing algorithms' lines are closer to the bottom left of a chart—representing low false positives and low false negatives—and low-performing algorithms' lines are closer to the upper right of a chart—representing high false positives and high false negatives. These charts are called Detection Error Tradeoff or Receiver Operator Characteristic plots.

Figure 5: Illustrative Representation of How Low-Performing and High-Performing Algorithms Affect Different Demographic Groups



Source: GAO analysis. | GAO-20-522

In addition to NIST, we identified recent academic studies and independent evaluations from 2019 that assessed the accuracy of facial recognition algorithms. These studies, although not as robust as NIST vendor tests, have reported performance trends similar to what NIST found among demographic groups.[40] For instance, four studies on verification algorithms noted that performance was lowest on women, black people, and very young or very old people in comparison to performance on middle-age white men.[41] In addition to the general trends reported across studies, some studies pointed out that results vary based on how algorithm thresholds are set in operation. Results also varied based on whether the focus is on false positives or false negatives. For example, one of the demographic groups, such as females, could perform better on one and worse on the other compared to white males.

Facial Analysis

Although facial analysis is a separate technology that should not be confused with facial recognition testing, discussed above, evaluations of facial analysis algorithms have had similar demographic results. Specifically, these evaluations have found lower performance (i.e., higher error rates) on black females than white men, as well as lower performance on the very young and very old. As discussed earlier, facial analysis algorithms estimate personal characteristics of a facial image, such as age, gender, emotional state, race, or ethnicity. Two academic evaluations of gender classification algorithms from 2018 and 2019 found that performance was lower for black women, and an independent evaluation from 2019 of an age estimation algorithm found that there was

[40]NIST notes that its 2019 Face Recognition Vendor Test report on demographic effects is the first to assess demographic effects in identification (one-to-many) algorithms. Unlike NIST vendor testing, which tested 189 algorithms from 99 developers, most academic and independent evaluations only tested one to four algorithms per study (one independent evaluator looked at 11 algorithms).

[41]Jacqueline Cavazos, et al. *Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias*; Cynthia Cook, et al. "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems"; John Howard and Arun Vemury, "The Effect of Broad and Specific Demographic Homogeneity on the Imposter Distributions and False Match Rates in Face Recognition Algorithm Performance;" and K.S. Krishnapriya, et al. *Characterizing the Variability in Face Recognition Accuracy Relative to Race*.

greater average absolute error for darker-skin females.[42] The 2019 academic evaluation was a follow-up study to the 2018 academic evaluation and found that developers had released updated versions of their algorithms, which had increased accuracy for black women compared to 2018, although it was still lower than accuracy for white men. A NIST gender classification algorithm test performed in 2015 reported similar results regarding gender, with performance for men being higher compared to that for women. However, because of the significant increase in accuracy resulting from modern deep neural network techniques, NIST has cautioned against assuming that results from older tests still apply to modern algorithms.[43]

Consequences of Performance Differences

Some members of Congress, privacy groups, and others have expressed concerns that facial recognition technology's higher error rates for certain demographics could result in disparate treatment, profiling, or other adverse consequences for members of these populations.

The consequences for different demographic groups that result from high error rates depend on the type of error, the algorithm's purpose (e.g., identification, verification, or facial analysis), and in what situation the facial recognition system is being deployed. For verification, consequences could include being blocked from accessing a building or a digital account. For identification, consequences could include being misidentified as a shoplifter when an individual's image is compared against a data set of known shoplifters. With less accurate algorithms that demonstrate performance differences, these negative outcomes would occur more frequently to the demographic groups described above.

For facial analysis, consequences of higher error rates for certain groups could include the inability to purchase age-restricted substances (e.g., alcohol, cigarettes) or rejection from a hiring process that uses facial analysis for screening. For example, facial analysis algorithms may be used for employment screening to assess emotional state, mood, or

[42]Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research,* vol. 81 (2018): pp.1–15; Inioluwa Deborah Raji and Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society (January 2019).*

[43]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT)—Performance of Automated Gender Classification Algorithms,* NIST Interagency Report 8052 (Gaithersburg, Md.: Apr. 20, 2015). We include NIST's 2015 report here because it is the only test NIST has performed on facial analysis.

personality traits. Several privacy advocacy groups expressed concerns that this type of use may lead to biased outcomes, such as the algorithm filtering out candidates who do not look like employees already present in the company or disadvantaging individuals with disabilities such as speech disorders, deafness, or blindness.

No Consensus Exists on the Effect of Factors That Could Cause Performance Differences for Certain Demographics

According to stakeholders we spoke with or literature we reviewed from NIST, academics, independent evaluators, and industry representatives, the performance of a facial recognition technology system depends on physical factors and algorithm factors, as shown in table 2. However, while these groups note factors that may account for performance differences, they have not determined the magnitude of each factor or root causes of performance differences. Additionally, while some factors have been found to apply to all demographics, at least one academic study found that some physical factors, such as illumination and general image quality, have a larger negative effect on certain demographic groups than others. Some studies also note the interaction of various factors together.

Table 2: Potential Causes of Performance Differences in Facial Recognition Technology Systems

Physical factors are related to the intrinsic characteristics of a face and the process of capturing an image of that face and can include the following:

- Pose, illumination, or expression of a face
- Cosmetics, glasses, hair, or other easily changeable characteristics that may cover parts of a face
- General image quality (e.g. because of an uncontrolled environment or camera settings)
- Inherent facial characteristics, particularly skin reflectance or underlying facial structure
- Aging over time (e.g., between reference image and recent image)

Algorithm factors are related to the creation and operation of a facial recognition algorithm and can include the following:

- Algorithm purpose (e.g., identification, verification)
- Algorithm type, such as modern deep neural networks versus older nontrainable algorithms
- Data used to train an algorithm, including how many images are used, the demographic groups represented in the images, and the representation of the physical factors noted above (e.g., images with varying amounts of cosmetics, images of differing quality)
- Operational threshold settings, such as sensitivity to false positives and any differences in the effect of different thresholds on different demographics
- Benchmarking or testing done during development (e.g., to assess the effectiveness or need for additional training data) or operational threshold setting (e.g., to assess appropriate operational threshold setting)

Source: GAO analysis. | GAO-20-522

Note: This table does not differentiate between factors that affect overall accuracy and factors that may specifically affect individual demographic groups.

One reason that there is not consensus over the magnitude or cause of individual physical or algorithm factors is that NIST, academics, and independent evaluators often test commercial algorithms in “black box” fashion, which means they assess algorithm results without looking at algorithm code or algorithm training data. Stakeholders told us that developers consider algorithm code and data used to train algorithms to be proprietary and do not share it with evaluators or the public. For example, NIST evaluations test a large number of algorithms and developers, but NIST explicitly states that it does not determine if or how individual algorithm factors may be affecting the outcome. Independent and academic evaluations of commercial facial recognition algorithms we reviewed also test in “black box” fashion.

Another reason for the lack of consensus is that the purpose and methodologies of evaluations differ. Some evaluations, such as NIST’s, test many different algorithms to investigate their individual performance, while other evaluations, such as by academics or independent evaluators, look at far fewer algorithms to investigate cause and effect of individual performance factors, but no evaluation has covered both. For example, NIST said that its methodology does not analyze cause and effect, so it does not attempt to explain or infer the technical reasons for the results it documents. Academic studies evaluating facial recognition algorithms have often attempted to analyze cause and effect, such as whether race causes greater differences in performance than gender; however, most studies have only looked at between one and four algorithms (one independent evaluator looked at 11 algorithms), which were often a mix of publicly available pretrained algorithms and commercial algorithms. NIST and academics note that findings from such studies may not apply to all algorithms. Multiple studies also note that factors can interact with each other, making it challenging to assign causality or magnitude to each factor’s effect on performance.

Stakeholders Suggested Various Methods That Could Mitigate Performance Differences

In the absence of consensus on the effect of factors or root causes of performance differences between demographics, stakeholders we interviewed and literature we reviewed identified a number of ways to potentially mitigate these differences.

- **Larger and more representative training and testing data sets.** The majority of literature we reviewed and all of the vendors we spoke with said that training data has a large effect on the accuracy of facial recognition algorithms and that larger and more representative data sets are crucial to addressing performance differences. Publicly available facial image data sets can be used for either training or

testing, so larger and more representative data sets could help improve both uses. Additionally, NIST and some academics have said that there are techniques to manipulate large data sets to make them more representative. For example, a data set could be resampled—a technique that randomly removes images from an overrepresented group in the data set or randomly draws additional examples from an underrepresented group, even if it means a sample is used more than once—so that each demographic group is represented by the same number of images compared to the others. This would make the data set more representative with the tradeoff of becoming smaller overall as a result of discarding images from the overrepresented groups or potentially becoming too attuned to the repeated faces.[44]

- **Improved image quality via better control over physical factors and compliance with image quality standards.** Many vendors we spoke with and literature we reviewed said that image quality is very important to algorithm performance. Additionally, NIST and the International Organization for Standardization (ISO), an independent nongovernmental organization composed of representatives from national standards bodies, have established image quality standards for use in facial recognition technology.[45] NIST, ISO, and some academics have suggested that better control over lighting and camera settings could improve image capture, resulting in improved performance. For example, a January 2020 draft of a new ISO image standard for facial image capture notes that improved technology such as face-aware cameras—which detect a face or assess real-time quality factors like lighting or pose—can lead to increased accuracy by providing real-time feedback to allow adjustments to elements that

[44]Another technique suggested by some academics and developers is to use synthetic facial images to train facial recognition algorithms with additional faces that look like those from unrepresented groups. Synthetic facial images are realistic faces of people who do not exist, created from patterns learned from real faces. However, other experts, academics, and developers have said that if the underlying training data for the neural network creating the synthetic faces is not representative, the synthetic faces could also be unrepresentative and not fit for training a facial recognition algorithm.

[45]According to NIST, one of the predominant biometric image standards for facial images is ISO/IEC 39794-5. NIST has also sponsored a related national biometric data standard for law enforcement use, entitled ANSI/NIST ITL 1-2011: Update 2015.

would otherwise lead to poor quality.[46] One academic facial recognition study found that black facial images had a lower rate of compliance with relevant image quality standards, which the study speculated may be the result of poor lighting during image capture.[47] Another facial recognition study performed by independent evaluators showed that lighting and camera sensitivity settings had an effect on performance and that facial recognition performed worse on darker skin, females, and younger subjects.[48] Those studies suggested that lighting or camera settings could be adjusted during image capture for better performance on affected demographics, as suggested in the ISO face-aware camera draft standard. NIST has also highlighted image standards compliance and repeat image capture attempts as effective mitigating techniques.[49]

- **Developers could direct algorithms to achieve equal error rates between demographic groups.** The NIST demographic effects report, some academics, and one facial recognition technology developer suggested that developers should direct algorithms to achieve equal error rates between demographic groups, rather than lowest overall error rates. As discussed earlier, even if an algorithm has an overall low error rate, it may have higher error rates for some demographics. For example, if an algorithm is trained to achieve lowest overall error, it may result in performing very well for the most highly represented group in the training data set (e.g., white men), with poor performance on the least represented group (e.g., black

The "Other Race Effect"

Multiple academic studies have described what has been called the "other race effect," which originated in human perception studies and has also been referred to in facial recognition technology evaluations, including by the National Institute of Standards and Technology. The effect is generally that people, and algorithms, are better at identifying individuals of their own race or ethnicity because of increased exposure to them. Facial recognition technology evaluations have shown that East Asian algorithms on average are better at recognizing East Asian faces and that western algorithms on average are better at recognizing white faces. This is evidence that performance differences are not just a result of certain demographics being inherently harder to recognize. Some academics and at least one developer have suggested that, among other potential solutions, having developers from underrepresented demographics can help mitigate the "other race effect" because of the new ideas they may introduce (e.g., new algorithm approaches or assumptions, such as that a characteristic may be important or function in a certain way).

Source: GAO analysis. | GAO-20-522

[46]*Information Technology – Face Image Quality Assurance – Face Aware Capture Specifications*, Draft International Standard ISO/IEC 24358-1:2020(WD).
[47]K.S. Krishnapriya, *Characterizing the Variability in Face Recognition Accuracy Relative to Race*.

[48]Cynthia Cook, "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems."

[49]In addition to discussing image capture in the 2019 Face Recognition Vendor Test demographic effects report, NIST has published a separate Face Recognition Vendor Test on automated image quality assessment algorithms, used to assess the quality of images inputted into a facial recognition system. National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 5: Face Image Quality Assessment,* Draft NIST Interagency Report (Gaithersburg, Md.: Mar. 6, 2020).

women). If an algorithm is trained to achieve equal error rates between groups, those performance differences would be reduced.[50]

- **Threshold setting in system operations.** Two academic studies reported that setting distinct thresholds for each demographic could reduce performance differences between demographics because a single threshold setting was shown to lead to different accuracy results between demographics. However, NIST noted that the security implications of doing so outweigh the benefits of demographic parity. For example, fraudsters could target demographics known to have a lower threshold and steal their credentials (e.g., steal or forge passports from countries with populations that have darker skin tones), knowing that biometric thresholds are lower and less sensitive to false negatives (i.e., misses) for the faked or stolen credential. NIST also noted that having separate thresholds places the responsibility for demographic parity on end-users rather than on both end-user and developer.[51]
- **Algorithm monitoring.** Developers, vendors, and end-users said that monitoring results and providing feedback to developers allows them to increase accuracy by refining the algorithm with more training data or by changing operational settings, such as thresholds. Two vendors also told us that developing an algorithm in a way that allows end-users to detect or explain differences in performance is important for ensuring accountability in performance on different demographic groups. For example, an algorithm that allows end-users to identify performance differences that arise during a system's operation enables them to adjust settings, such as algorithm thresholds and image capture, without requiring the developer to intervene.
- **Setting performance standards and periodic evaluations of facial recognition algorithms**. Some industry representatives and privacy advocacy groups have suggested addressing performance

[50]One related approach suggested by some academics is to develop facial recognition technology systems that include multiple algorithms, each one trained or fine-tuned to particular demographics, rather than a single algorithm trained to achieve equal error between groups.

[51]This mitigation strategy has been suggested for facial analysis algorithms as well. For example, an independent evaluation of a vendor's age estimation algorithm similarly found that confidence buffers around a result act as a threshold (e.g., setting a system to accept a number of years over or under the target age restriction in order to reduce false positives and false negatives). The evaluator recommended that buffers should be set according to documented performance differences between demographics to avoid discriminatory outcomes.

differences between demographics by setting performance standards for facial recognition technology and making benchmarking and periodic testing through independent entities like NIST mandatory.[52] NIST officials stated they did not have an opinion as to whether evaluations of facial recognition algorithms should be mandatory. However, they said they would not support efforts making NIST's existing voluntary evaluations mandatory because that would adversely affect the dynamic of their ongoing testing and be inconsistent with NIST's independent nonregulatory mission. NIST officials stated that NIST sets standards on how to measure algorithm performance, but it does not intend to play a role in setting standards on what that performance should be. In its December 2019 demographics vendor test report, NIST called for more research into the degree to which differences in accuracy among demographic groups could be tolerated in different settings. Further, according to NIST officials and the U.S. Chamber of Commerce's facial recognition policy principles, the error rate that can be tolerated depends on the end-user's scenario (including the type of facial recognition technology and risk the end-user faces). Some industry representatives also recommended that facial recognition technology companies disclose accuracy results to end-users in a manner that could help them better understand the limitations or issues to consider when setting thresholds of the facial recognition algorithm.

- **Additional research into cause and effect of factors that affect performance.** Stakeholders, including NIST, academics, and independent evaluators, have said that more research and testing would help answer questions regarding the potential causes, magnitudes, and interactions of the different factors. For example, NIST's 2019 vendor test called for research into models of how physical facial features, image quality issues, and algorithms interact. Recent academic evaluations have called for additional research into demographic differences from facial recognition technology that operates on unposed images, the effect of skin reflectance along with different measures of skin tone, or more holistic approaches that investigate multiple potential factors together.

[52]As discussed earlier, NIST runs the National Voluntary Laboratory Accreditation Program for biometric testing, which evaluates third-party laboratories that seek accreditation to test for biometric products (including facial recognition).

Federal and State Laws Provide Limited Privacy Protections, and Voluntary Privacy Guidelines Have Been Developed

Certain Federal and State Privacy Laws Apply to Facial Recognition Technology but Are Limited in Scope

Some federal laws are applicable to the commercial use of facial recognition technology, but their scope in addressing privacy concerns is limited. Some states have adopted laws that either directly or indirectly address facial recognition technology. Outside the United States, laws such as the European Union's 2018 data privacy regulation cover facial and other biometric information.

Federal Law

As we reported in 2015, the United States does not have a comprehensive privacy law governing the collection, use, and sale of personal information by private-sector companies.[53] In addition, no federal law expressly regulates the commercial use of facial recognition technology, including the identifying and tracking of individuals.[54]

Further, in most contexts federal law does not address how personal data derived from facial recognition technology may be used or shared.[55] Federal laws addressing privacy issues in the private sector are generally tailored to specific purposes, situations, types of information, or sectors or entities. In general, these laws, among other things, limit the disclosure of certain types of information to a third party without an individual's

[53]In contrast, a baseline privacy law exists for personal information the federal government maintains—the Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a). The act, among other things, generally prohibits, subject to a number of exceptions, the disclosure by federal agencies of records about an individual without the individual's written consent and provides individuals with a means to seek access to and amend their records.

[54]For additional information on federal privacy law related to commercial entities more broadly, see GAO-19-621T; GAO, *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, D.C.: Feb. 21, 2019); *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GAO-19-52 (Jan. 15, 2019); GAO-15-621; and *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[55]See GAO-15-621.

consent, or prohibit certain types of data collection. Some of these laws also set standards for how certain personal data should be stored and disposed of securely. As seen in table 3, these laws may potentially apply to biometric technologies, including facial recognition.

Table 3: Federal Laws That May Be Applicable to Use of Biometric Information by Commercial Entities

Law	Summary of key biometric requirements
Driver's Privacy Protection Act[a]	Places restrictions and consent requirements on the disclosure and sale of certain personal information collected by state departments of motor vehicles in connection with a motor vehicle record, including a person's photograph or image.
Health Insurance Portability and Accountability Act[b]	Governs the disclosure of individually identifiable health information collected by covered health care entities and sets standards for data security. The act's implementing regulations require that biometric identifiers and full-face photographic images be removed before protected health information is no longer considered individually identifiable health information.
Fair Credit Reporting Act[c]	Governs the collection, disclosure, and use of information contained in consumer credit reports. The Fair Credit Reporting Act's implementing regulations include unique biometric data under the definition for identifying information.
Family Educational Rights and Privacy Act[d]	Governs the disclosure of personally identifiable information from education records. The act's implementing regulations include biometric records under the definition for personally identifiable information.
Computer Fraud and Abuse Act[e]	Prohibits obtaining information from a protected computer through the intentional access of a computer without authorization or exceeding authorized access.
Children's Online Privacy Protection Act[f]	Generally prohibits the online collection of personal information from children under 13 without certifiable parental consent. The act's implementing regulations include a photograph or video containing the child's image under the definition for identifying information.
Section 5 of the Federal Trade Commission (FTC) Act[g]	Prohibits unfair or deceptive acts or practices in or affecting commerce. FTC has interpreted the act to apply to deceptive practices or violations of written privacy policies. This authority could extend to companies that develop or use biometric data.

Source: GAO review of federal laws. | GAO-20-522

[a]18 U.S.C. §§ 2721-25.

[b]See Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); 45 C.F.R. §§ 164.502(d)(2), 164.514(a), 164.514(b)(2)(i)(P)-(Q).

[c]15 U.S.C. § 1681 et seq; 12 C.F.R. § 1022.3(g)(2).

[d]See Pub. L. No. 93-380, Tit. V., § 513, 88 Stat. 57 (1974) (codified as amended at 20 U.S.C. § 122g); 34 C.F.R. § 99.3.

[e]18 U.S.C. § 1030. The Computer Fraud and Abuse Act does not mention biometric data; however, a Department of Justice manual section on the act notes that biometric information should be given high priority for federal prosecution when it is illegally accessed.

[f]See Pub. L. No. 105-277, Div. C, tit. XIII, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501-6506); 16 C.F.R. § 312.2. In July 2019, FTC issued a request for public comment on its implementation of the Children's Online Privacy Protection Act rule. Among the questions asked by FTC, it sought comment on whether it should consider further revision to the definition of "personal information" to expressly include biometric data. See 84 Fed. Reg. 35842, 35844 (July 25, 2019).

[g]15 U.S.C. § 45.

Section 5 of the FTC Act authorizes FTC to take action against unfair or deceptive acts or practices in or affecting commerce—including against companies that use or sell facial recognition technology. FTC has interpreted this authority to apply to deceptive practices or violations of written privacy policies and has often used it to successfully challenge allegedly deceptive statements in privacy policies.

As we previously reported, FTC lacks explicit and comprehensive authority related to privacy issues. However, consumers can submit complaints related to facial recognition technology to FTC.[56] As of the end of February 2020, FTC had received approximately 155 complaints related to facial recognition technology.[57] Complaints included privacy concerns related to social media companies, technology not working, and fraudulent misuse of the technology. According to FTC staff, the total number of complaints for facial recognition was generally low compared to the number of complaints against other types of products.[58]

In addition, FTC has pursued enforcement actions against companies using facial recognition technology under its statutory authority to protect consumers from unfair and deceptive trade practices. In July 2019, FTC imposed a $5 billion penalty on Facebook to settle allegations that, among other things, Facebook violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal

[56]For more information on FTC's authorities and activities, see GAO-19-52.

[57]As we previously reported, FTC's Consumer Sentinel Network is a database of consumer complaints received by FTC, as well as those filed with certain other federal and state agencies and nongovernmental organizations, including the Consumer Financial Protection Bureau and the Better Business Bureaus. See GAO, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*, GAO-17-254 (Washington, D.C.: Mar. 30, 2017). The amount includes all complaints that were in Consumer Sentinel as of February 29, 2020, which according to FTC staff includes 5 years of complaint data.

[58]According to FTC staff, consumer complaint data have limitations and may not indicate the extent of the problems with the product or technology. For example, as we previously reported, not all consumers who experience problems may file a complaint, and not all complaints are necessarily legitimate or categorized appropriately. In addition, a consumer could submit a complaint more than once, or to multiple entities, potentially resulting in duplicate complaints. See GAO-17-254.

information.[59] Specifically, one of FTC's allegations was that Facebook violated the 2012 order by misrepresenting users' ability to control the use of facial recognition technology with their accounts.[60]

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.[61] Accordingly, we reiterated our 2013 suggestion that Congress strengthen the current consumer privacy framework to reflect the effects of changes in technology and the marketplace.[62] For these reasons, we continue to believe that the current privacy framework in commercial settings warrants reconsideration.

State Laws

As seen in table 4, some states have adopted laws that either directly or indirectly address biometric information, including that related to facial recognition technology. Some of these measures address the collection, use, storage, data sale, and security of the information, and some

[59]*See* Stipulated Order for Civil Penalty, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019). In 2012, FTC issued a final consent order that required Facebook to, among other things, avoid misrepresenting the extent to which consumers can control the privacy of their information, including their photos and videos; the steps that consumers must take to implement such controls; and the extent to which Facebook makes user information accessible to third parties. *See In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012).

[60]More specifically, FTC alleged that Facebook implied "to approximately 60 million users that they could 'turn on' facial-recognition technology associated with their posted photos and videos when, in fact that technology was 'on' for those users by default." Plaintiff's Consent Motion for Entry of Stipulated Order, United States of America v. Facebook, Inc., No. 19-cv-2184, 2 (D.D.C. July 24, 2019).

[61]GAO-15-621.

[62]See GAO-13-663. 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 May 2020, such legislation had not been enacted, although several privacy bills had been introduced, including some that address facial recognition technology.

address when consumers must be notified of or consent to the technology's use.[63]

Table 4: Selected State Laws Applicable to Use of Biometric Information by Commercial Entities

Law	Summary of key biometric requirements
Illinois Biometric Information Privacy Act[a]	Places restrictions on how private entities retain, collect, disclose, and destroy biometric identifiers and biometric data. Requires companies to provide notice and obtain consent for collection, capture, purchase, or receipt of such data. Creates a private right of action, so harmed individuals may directly sue offending parties.
Washington Biometric Privacy Law[b]	Prohibits any company or individual from adding certain biometric identifiers to a database for commercial purposes without providing notice, obtaining consent, and providing a mechanism to prevent subsequent use of the identifier for a commercial purpose. Restricts the amount of time a company or individual may retain such biometric identifiers.
The Texas Statute on the Capture or Use of Biometric Identifiers[c]	Prohibits any company or individual from capturing biometric identifiers for a commercial purpose without notice and consent. Restricts the sale, disclosure, and retention of biometric identifiers.
California Consumer Privacy Act[d]	Generally requires companies to disclose the categories of personal information (including biometric information) they collect about a consumer, the business or commercial purpose for collecting or selling such information, and what categories of third parties received it. The law also generally requires companies to allow consumers to opt out of the sale of and request the deletion of personal information.
Vermont Data Broker Regulation[e]	Requires data brokers to register annually and maintain certain minimum security standards, and prohibits the acquisition and use of brokered personal information (including unique biometric data) through fraudulent means or for the purpose of committing certain bad acts.
Various state data breach notification laws	Various states have specifically included biometric data in their data breach notification laws. These laws generally require any company or individual that owns or licenses data containing the private information (including biometric data) of a resident to maintain safeguards for the data and notify the resident of certain instances when the data have been accessed or acquired by a person without valid authorization. States whose laws specifically cover biometric data include Arizona, Arkansas, California, Colorado, Delaware, Illinois, Iowa, Louisiana, Maryland, Nebraska, New Mexico, New York, North Carolina, South Dakota, Washington, Wisconsin, and Wyoming.

Source: GAO review of state laws. | GAO-20-522

Note: Biometric information includes facial images and templates that are a part of facial recognition technology.

[a]740 ILL COMP STAT. 14/1 et seq. (2008).

[b]Wash. Rev. Code § 19.375.010 et seq. (2017).

[c]Tex. Bus. & Com. Code Ann. § 503.001.

[d]Cal. Civ. Code § 1798.100 et seq. (2020).

[e]Vt. Stat. .Ann. tit. 9, §§ 2430, 2433, 2446 and 2447.

[63]According to the National Conference of State Legislators, at least 25 states and Puerto Rico plan to consider legislation related to the regulation of privacy practices of commercial entities, online services, or commercial websites. Proposed legislation covers an array of consumer privacy topics; some proposals are specific to biometrics used in facial recognition technology.

Three states—Illinois, Texas, and Washington—have passed laws requiring that companies let individuals know when they collect certain biometric information, including information used in facial recognition technology. The laws also require companies to obtain consent before collecting biometric information. But these laws differ in their approach to data retention and company liability. The Washington Biometric Privacy Law and Texas Statute on the Capture or Use of Biometric Identification explicitly restrict how long a company can retain collected biometric information.[64] The Illinois Biometric Information Privacy Act provides consumers the ability to sue companies directly for violating the act's provisions.[65]

California passed a comprehensive privacy law in June 2018, which includes protections for biometric information under its definition of personal information. This act went into effect in January 2020. The law requires businesses to inform consumers before personal information is collected, including facial images. California's law also requires businesses to disclose the consumer's rights and options for deleting or opting out of the sale of their information.

Some states provide legal coverage or protection for biometric information, including facial templates, through amendments to existing data breach, data broker, and data protection laws.[66] Under related data breach laws, companies are generally required to notify individuals in the

[64]In March 2020, Washington State also passed a facial recognition law that regulates the development, procurement, and use of facial recognition technology by state and municipal government agencies in Washington State. While this law could affect commercial uses of facial recognition technology, we determined that the law was outside of our scope because of its focus on regulating government use, as opposed to commercial use, of the technology.

[65]The Illinois Biometric Information Privacy Act allows consumers to sue companies directly through a private right of action provision. A private right of action is an individual's right to sue in a personal capacity to enforce a legal claim. In January 2020, Facebook announced a proposed $550 million class-action settlement with plaintiffs who alleged that it violated provisions of the Illinois Biometric Information Privacy Act, including through the use of its facial recognition technology. In addition, in January 2020, individuals brought a class action lawsuit against IBM for alleged violations of the act resulting from IBM allegedly collecting, storing, and using individuals' biometric identifiers and biometric information without informed written consent.

[66]In addition to these state laws, we found municipalities that passed laws or ordinances banning government use of facial recognition technology. While these ordinances could affect the commercial use of the technology, we determined that they were outside the scope of this report because of their focus on regulating government use, as opposed to commercial use, of the technology.

event of a data breach of their unprotected biometric information. For example New York's data breach law requires that companies with data containing residents' private information—including biometric information—must develop, implement, and maintain reasonable safeguards to protect any such data they collect. Vermont established parameters around the acquisition and use of personal information, including biometric information, received through data brokers.

Some industry representatives told us that state laws, such as Illinois's biometric law, have kept companies from testing or offering biometric technologies—including facial recognition technology—in those states. Some industry representatives also expressed concerns about the costs of complying with individual state laws with varying requirements. For example, a few companies noted that they have changed their privacy and data notifications in response to state laws, such as to adhere to California's privacy requirements. Based on our review of 30 companies' privacy policies, 29 of them included information specific to California's privacy law, which detailed the extent to which they collected biometric information, and their policies for protecting and retaining that information. Most industry representatives we interviewed supported a federal approach to regulating facial recognition technology, with some suggesting that regulation should consider the different uses of the technology.

European Union's General Data Protection Regulation

Outside the United States, the European Union's General Data Protection Regulation (GDPR) imposes general data privacy protections and covers the processing of biometric information.[67] According to officials from the European Data Protection Supervisor (the European Union's independent data protection authority), the European Union's GDPR, which became applicable on May 25, 2018, applies to private and public companies that control or process data or offer services to European Union citizens. The officials told us that GDPR jurisdiction is expansive and can cover all

[67]According to our literature review and interviews, Brazil, China, Japan, and Thailand are among the other countries that have adopted significant privacy laws in the past 5 years. See *e.g.,* Brazil's General Data Protection Law (Law No. 13.709/2018); China's GB/T 35273-2017 Information Technology – Personal Information Security Specification; Japan's Act on the Protection of Personal Information (Act No. 57 of 2003; Amendment by Act No. 65 of 2015); and Thailand's Personal Data Protection Act, BE 2562 (2019). In addition, as noted above, according to review of relevant literature and industry interviews, the European Union's Revised Payment Service Directive requires stronger customer authentication procedures for certain electronic transactions, which may include biometric authentication procedures.

entities—including those based in the United States—that process data in the European Union or engage in businesses that affect people within the European Union.[68] Officials with the European Data Protection Supervisor noted that a number of GDPR principles and rules relate to the processing of biometric information, including facial recognition (see text box).

European Union General Data Protection Regulation (GDPR) Principles and Rules Related to Biometric Information

According to the European Data Protection Supervisor—the European Union's independent data protection authority—and other relevant stakeholders and literature, the following are principles and rules of the GDPR that are particularly relevant to the processing of biometric data:

Transparency. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. For example, controllers might use pictograms to explain how the consumer's information was used and then provide the consumer with their data.

Purpose limitations. The purpose limitations principle states that the information is collected with explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In addition, the purpose of the data collection should specified in advance of the collection.

Data minimization. The data minimization principle requires personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Further, it is the company's responsibility to assess how much data are needed and ensure that irrelevant data are not collected, which depends on the use case.

Data accuracy. The data accuracy principle requires companies holding data to ensure that data are kept up to date, and inaccurate data are erased or corrected to ensure accuracy. GDPR's accuracy principles relate to personal data.

Storage limitation. The storage limitation principle means that personal data must be deleted or anonymized as soon as they are no longer needed for the purposes for which they were collected. Further, data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Accountability. The accountability principle requires companies to actively and continuously implement measures to promote and safeguard data protection in their processing activities. Further, companies must be able to discuss and demonstrate their approaches to data privacy as part of their privacy and accountability requirements under GDPR.

Data protection by design and by default. The data protection by design and default principle requires that controllers put in place measures to effectively implement data protection principles and to integrate the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects. In addition, companies must implement appropriate default measures to ensure that only personal data necessary for their purposes will be processed.

Source: Analysis of information and documents from European Data Protection Supervisor and its officials, the European Union Agency for Fundamental Rights, the Council of Europe, and other relevant stakeholder documents and statements. | GAO-20-522

According to European Data Protection Supervisor officials, there have been at least three enforcement actions by European Union member state data protection authorities concerning the use of facial recognition technologies in breach of GDPR. All three examples provided by European Union representatives were related to violations of schools using facial recognition technology to track attendance. The representatives said that the enforcement actions recommended that the

[68]Companies do not need a physical presence in the European Union to be covered under GDPR, according to European Data Protection Supervisor officials. These officials and a former individual with expertise in GDPR said that GDPR would apply to 1) entities that are established in the European Union and 2) entities that do not have a presence in the European Union but offer services or goods to people in the European Union or monitor the data from subjects in the European Union.

schools apply less intrusive measures that did not entail processing sensitive data for tracking attendance.

Industry representatives identified multiple approaches they took to comply with GDPR provisions. Some vendors told us that they provide guidance to end-users for using the technology, including data security and data retention, which are informed by existing standards, including GDPR. Further, some companies issued separate GDPR privacy policies or added specific provisions to existing policies.

Some Stakeholders Have Developed Voluntary Privacy Frameworks

In February 2014, the National Telecommunications and Information Administration (NTIA) convened stakeholders with the goal of developing a voluntary, enforceable code of conduct for industry participants. However, NTIA did not reach its original goal to produce a binding agreement among all stakeholders, in part because several privacy groups withdrew from the process because of their concerns that industry stakeholders were not open to strong privacy protections. NTIA opted to keep working with remaining participants to deliver a best practices document, and in June 2016 it issued its Privacy Best Practice Recommendations for Commercial Facial Recognition Use.[69]

In addition, some industry and privacy groups have developed voluntary privacy frameworks that seek to address privacy concerns, many of which were issued in 2018 and 2019 (see table 5). Some of these frameworks consist of general data privacy principles that would apply to facial recognition technology, while the others are specific to biometrics or facial recognition technology.

[69]National Telecommunications and Information Administration, *Privacy Best Practice Recommendations For Commercial Facial Recognition Use* (Washington, D.C.: June 2016).

Table 5: Selected Organizations That Developed Privacy Frameworks Associated with Facial Recognition Technology

Organization	Description
Asia-Pacific Economic Cooperation (APEC)	APEC is a regional economic forum with 21 member countries. The APEC Privacy Framework was issued in 2015.
Biometrics Institute	The Institute is a nongovernment organization focused on the responsible and ethical use of biometrics. Members represent government, the private sector, and academics from 30 countries. In May 2019, it updated its Privacy Guidelines and in October 2019, it issued Ethical Principles for Biometrics.
Fast Identity Online Alliance	The Alliance is an industry association focused on global authentication standards. Members include technology professionals in the private and government sectors. It issued the Privacy Principles Whitepaper in February 2014.
Future of Privacy Forum	The Forum is a nonprofit organization focused on exploring the challenges posed by emerging technologies, including privacy. Members include private-sector companies and private foundations. In September 2018, it published its Privacy Principles for Facial Recognition Technology in Commercial Applications.
International Biometrics +Identity Association (IBIA)	IBIA is an industry association representing the identification technology industry. In August 2014, IBIA issued its Best Practices Recommendations for Commercial Biometric Use, and in August 2019, it issued its Principles for Biometric Data Security and Privacy.
National Telecommunications and Information Administration (NTIA)	NTIA is a federal agency under the U.S. Department of Commerce that, among other tasks, represents the executive branch in both domestic and international telecommunications and information policy activities. In June 2016, the agency issued its Privacy Best Practice Recommendations for Commercial Facial Recognition Use.
Safe Face Pledge	Safe Face Pledge, created in December 2018, is a joint project of the Algorithmic Justice League and the Center on Privacy & Technology at Georgetown Law. The Algorithmic Justice League is a nongovernment organization focused on the social implications and harms of artificial intelligence. The Center is a think tank focused on privacy and surveillance law and policy.
U.S. Chamber of Commerce	The Chamber is a nongovernment organization representing approximately 3 million businesses. In December 2019, the Chamber released its Facial Recognition Policy Principles.

Source: GAO analysis. | GAO-20-522

Most of these privacy frameworks are consistent with the Fair Information Practice Principles (see table 6).[70] While these principles are not legal requirements, they provide a possible framework for balancing privacy with other interests.

[70]The Fair Information Practice Principles are a set of internationally recognized principles for protecting the privacy and security of personal information. They served as the basis for the Privacy Act of 1974—which governs the collection, maintenance, use, and dissemination of personal information by federal agencies—and for many FTC and Department of Commerce privacy recommendations. See GAO-19-621T.

Table 6: Examples of the Use of Fair Information Practice Principles in Selected Biometrics Privacy Frameworks

Fair Information Practice Principles and description	Examples of application in biometrics privacy frameworks
Collection limitation. The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.	The International Biometrics + Identity Association's Principles for Biometric Data Security and Privacy states that effective notice and consent is to be conveyed with brief written statements, in ordinary language, readily comprehended by the notified or consenting person. Lengthy fine print pro-forma statements, such as most software license agreements, real estate documents, and loan documents do not meet this principle. U.S. Chamber of Commerce Facial Recognition Policy Principles state that transparency should be the cornerstone that governs the use of facial recognition technology. Commercial and government users should be transparent about when and under what circumstances the technology is used as well as the processes and procedures governing the collection, processing, storage, use, and transfer of facial recognition data.
Data quality. Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.	The Future of Privacy Forum Privacy Principles for Facial Recognition Technology in Commercial Applications states that companies should take steps to ensure that facial recognition data and their connections to other personally identifiable information are accurate. Companies should seek to avoid mislabeling by sufficiently testing their systems to identify and eliminate meaningful accuracy disparities, specifically with regard to demographic variances in race, age, and gender.
Purpose specification. The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.	The Future of Privacy Forum Privacy Principles for Facial Recognition Technology in Commercial Applications states that companies should determine whether a prospective use is compatible by considering factors to include the context of collection; a reasonable expectation of how the data will be used; whether facial recognition is merely a feature of a product or service versus integral to the service itself; and how the collection, use, or sharing of facial recognition data will likely impact consumers.
Use limitation. Personal information should not be disclosed or otherwise used for purposes other than a specified purpose without consent of the individual or legal authority.	The Future of Privacy Forum's Privacy Principles for Facial Recognition Technology in Commercial Applications states that companies should commit to collecting, using, and sharing facial recognition data in ways that are compatible with reasonable consumer expectations for the context in which the data were collected. Facial recognition technology should be used in a way that is fair to consumers, including weighing the privacy risks against clear and articulable benefits to consumers and providing opportunities for consumers to make choices to mitigate or avoid risks.
Security safeguards. Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.	The International Biometrics + Identity Association's Principles for Biometric Data Security and Privacy states that for all commercial and civil government applications, the entities should protect the biometric data retained by using biometric one-way template transformation. In addition, it states that companies should encrypt any raw data collected, at rest or in motion, and delete raw biometric data following template transformation. In addition, the association's Best Practices state that it is good practice to maintain a separation between biometric and associated nonbiometric personal information. Fast Identity Online Alliance's Privacy Principles states that biometric data must never leave the user's personal computing environment. This means that all biometric data must be stored locally on the user's device and not transmitted externally to servers or the cloud.

Fair Information Practice Principles and description	Examples of application in biometrics privacy frameworks
Openness. The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.	The Future of Privacy Forum's Privacy Principles for Facial Recognition Technology in Commercial Applications states that companies implementing facial recognition systems should develop and publish privacy policies describing their use of facial recognition systems in clear terms and a detailed description of the data collected. Privacy policies, educational help centers, and other materials are ways to ensure consumers and other stakeholders can understand. According to the Safe Face Pledge (the joint product of an academic and a nonprofit institution), companies taking the pledge should increase public awareness of facial analysis technology use (1) by publishing accessible information on how facial analysis technologies are sold and used, including the types of entities they are sold to and any safeguards taken to mitigate misuse and risks, and (2) by proactively making a public explanation of how the systems work in clear and simple terms so that the people can understand how they work.
Individual participation. Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.	Biometrics Institute's Privacy Guidelines and Ethical Principles for Biometrics state that companies engaged in facial recognition technology should provide citizens the right to have their biometric record amended, if the data are incorrect, or deleted.
Accountability. Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.	The Safe Face Pledge states that companies should ensure compliance with their rules by adopting internal "know your customer" policies and procedures to ensure that their products are not being used for secret government surveillance. In addition, companies should implement internal bias evaluation processes and support independent evaluation by adopting internal systems to evaluate the performance of their products and services.

Source: GAO analysis of selected privacy frameworks. | GAO-20-522

Nearly all selected privacy frameworks discuss the need for companies to notify consumers about the type of information they collect and receive consumer consent; to implement effective data storage and protection measures; and to provide consumers with the opportunity to correct inaccurate information. Most of the selected privacy frameworks note specific recommendations about data retention and disposal practices based on the stated purpose of the data collection, and advocate for a risk-based approach to data retention. About half of the selected privacy frameworks identify the need for end-users to ensure that discussed privacy principles are implemented in the end-users' practices and that accountability measures exist for collected data. Such measures include opportunities for users to seek redress for collection of their data and companies to conduct internal audits of collected data.

Stakeholders we interviewed identified additional activities that companies could improve the use of facial recognition technology. These activities include

- defining the purpose for the technology's use and clearly notifying consumers how companies are using the technology—such as surveillance or marketing;
- identifying risks and limitations associated with using the technology and prohibiting certain uses (e.g., those with discriminatory purposes); and
- providing guidance or training related to these issues.

However, these voluntary privacy frameworks and suggested activities that could help address privacy concerns or improve the use of facial recognition technology are not mandatory. Furthermore, as discussed earlier, in most contexts facial recognition technology is not currently covered by federal privacy law. Accordingly, we reiterate our 2013 suggestion that Congress strengthen the current consumer privacy framework to reflect the effects of changes in technology and the marketplace.[71]

Agency Comments

We provided a draft of this report for review and comment to the Department of Commerce and the Federal Trade Commission. We received technical comments from them, which we incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees and members, the Secretary of Commerce, the Chairman of the FTC, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

[71]GAO-13-663.

Should you or your staff have questions concerning this report, please contact me at (202) 512-8678 or cackleya@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Alicia Puente Cackley
Director, Financial Markets and Community Investment

List of Requesters

The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate

The Honorable Jerrold Nadler
Chairman
Committee on the Judiciary
House of Representatives

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives

The Honorable Cory A. Booker
United States Senate

The Honorable Christopher A. Coons
United States Senate

The Honorable Edward J. Markey
United States Senate

Appendix I: Objectives, Scope, and Methodology

This report examines (1) current and potential uses of facial recognition technology in the commercial sector, (2) the characteristics of facial image data sets assembled for commercial purposes and any related privacy and data security risks, (3) differences in how accurately the technology performs across demographic groups, and (4) privacy protections under federal and state law applicable to commercial use of facial recognition technology and privacy frameworks developed by private entities. The scope of this report does not include government use of facial recognition technology.[1] Further, this report discusses but does not focus on facial analysis, which interprets facial features to determine characteristics such as gender, race, age, and emotions. Instead, this report primarily focuses on the use of facial recognition technology in private and commercial sectors and how the technology is used to detect, identify, and verify individuals.

For all objectives, we interviewed stakeholders representing federal agencies, privacy advocacy groups, academics, industry associations, vendors that develop or provide facial recognition technology, and end-users—companies that use the technology for commercial purposes. The federal agencies include the Federal Trade Commission (FTC) and the Department of Commerce's National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration. We interviewed representatives from six privacy advocacy groups (Electronic Frontier Foundation, Electronic Privacy Information Center, American Civil Liberties Union, Center for Democracy and Technology, World Privacy Forum, and Future of Privacy Forum); five industry associations (the International Biometrics + Identity Association, National Retail Federation, American Association of Motor Vehicle Administrators, Interactive Advertising Bureau, and U.S. Chamber of Commerce); and five academic institutions or researchers.[2] Additionally,

[1]We have ongoing work on law enforcement's use of facial recognition technology and expect this report to be issued in early 2021. Additionally, we expect to issue a report in August 2020 on the accuracy of U.S. Customs and Border Protection and Transportation Security Administration facial recognition systems, and whether they incorporate privacy protection principles. Furthermore, we have started work on a comprehensive review of the federal government's use of facial recognition technology. See also GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[2]The academic institutions or researchers were Georgetown Law Center on Privacy and Technology, Alessandro Acquisti (Carnegie Mellon University), Dr. Erik Learned-Miller (University of Massachusetts Amherst), Dr. Anil Jain, and Dr. Arun Ross (Michigan State University).

we interviewed representatives from the Biometrics Institute and the European Association for Biometrics.[3] We identified these organizations and individuals through suggestions from interviews with agencies, privacy advocacy groups, and others; through reviews of our past work; and based on their participation in government initiatives and industry events.

In addition, we interviewed representatives of eight facial recognition technology vendors, selected because they were identified by agencies and privacy advocacy groups and represented a mix of developers of the technology and service providers. We also interviewed representatives of seven companies that use facial recognition technology in the retail or financial services sectors or at large venues (such as stadiums). We selected these industries because they were commonly cited in our literature review and among industry representatives we spoke with as current or potential users of facial recognition technology. The companies were selected to represent a mix of sizes and industry subsectors.

We also conducted a literature review of the uses of facial recognition technology in the commercial sector (centered in the United States) since 2015; the development and training of facial recognition algorithms; concerns related to privacy; and performance differences for different demographics. Databases searched as part of the literature review included ProQuest, EconLit, Policy Index, and Business Source Corporate Plus. We searched for variations of the term “facial recognition technology.”

To describe current and potential uses of facial recognition technology, we reviewed available market research reports on the industry, including global market revenues and forecasted revenue estimates. We did not independently verify the information in these reports, but our review of seven market research firms found that the estimates fell within consistent ranges, with only one outlier.

[3]The Biometrics Institute is a multistakeholder organization whose mission is to promote the responsible and ethical use of biometrics as an independent and impartial international forum for biometric users and other interested parties. Biometrics Institute membership includes banks, airlines, government agencies, biometric experts, privacy experts, suppliers, and academics. The European Association for Biometrics is a European nonprofit organization whose role is to promote the responsible use and adoption of modern digital identity systems. European Association for Biometrics members include government agencies, academics, and biometric industry companies.

We searched the database of the U.S. Patent and Trademark Office (USPTO) for patents related to facial recognition technologies granted from 2015 to 2019, and we interviewed USPTO officials.[4] We downloaded the data from USPTO's PatentsView, a U.S. patent data visualization and analysis platform. Our analysis included patents within a particular range of Cooperative Patent Classification (CPC) class that are exclusively focused on technologies associated with facial recognition.[5] There are other patents associated with facial recognition that may not be categorized under the CPC class used in our analysis.[6] However, considering that broadening the CPC class might result in patents that are not necessarily related to the facial recognition, we only included the subsets of patents that are exclusive to facial recognition. We assessed the reliability of these data by reviewing supporting documentation, interviewing knowledgeable USPTO officials, and comparing the number of granted patents to other query results provided by patent examiners. We found the data to be sufficiently reliable for the purposes of looking at the general trend of the number of facial-recognition-related patents granted over time.

To describe the characteristics of facial image data sets assembled for commercial purposes and any related privacy and data security risks, we reviewed studies and evaluations published or suggested by academics, privacy advocates, and industry representatives we interviewed. We also reviewed Science.gov using the search terms "facial recognition," "data," and "sale" to identify work citing concerns about the sale of facial image data sets. In addition, we interviewed representatives of two data brokers—companies that collect and resell information on individuals—

[4]Data through December 31, 2019, were the most recent available at the time of our analysis.

[5]The Cooperative Patent Classification System is the result of a partnership between the European Patent Office and the U.S. Patent and Trademark Office in their joint effort to develop a common, internationally compatible classification system for technical documents, which will be used by both offices in the patent granting process. Our analysis focused on patents with CPC class within the following range: G06K 9/00221-00335, which exclusively focus on technologies associated with facial recognition. For example, the description for CPC class G06K 9/00221 is acquiring or recognizing human faces, facial parts, facial sketches, or facial expressions.

[6]For example, there may be patents on facial recognition that are classified under the CPC category G06T: image data processing or generation, in general.

and five data consultants.[7] We selected the data brokers because they were among the largest and most widely known in their industry, and we selected data consultants that (1) offer data collection services and (2) offer services or show expertise in facial recognition based on our research and suggestions from industry representatives.

To address differences in performance across demographic groups, we reviewed NIST Face Recognition Vendor Tests (vendor test) and four additional facial recognition algorithm accuracy evaluations that were commonly cited among NIST vendor test reports and other academic or independent evaluation studies. The NIST vendor test reports we reviewed included two one-to-many identification reports available at the time of our review (published in 2018 and 2019) and a separate demographic effects report published in 2019 that assessed both identification and verification.[8] Additionally, we judgmentally selected a nongeneralizable sample of NIST's ongoing vendor test reports on one-to-one verification published from 2017 to 2019 on a roughly monthly basis.[9] We also reviewed NIST's 2015 gender classification report—which was the only vendor test NIST had performed on facial analysis at the time of our review.[10] Further, we reviewed and selected four facial recognition algorithm accuracy evaluations that were commonly cited by

[7]For purposes of this report, we define data consultants as companies that (1) provide or assist with generating or sourcing data sets for clients to use in facial recognition technology and (2) offer services or show expertise in computer vision applied to faces (of which facial recognition is a subset). The key difference between a data consultant and a data broker is that the data consultant does not sell access to already-existing data sets in the way that broker is usually defined. Instead, they may offer to gather or develop a facial image data set in response to a specific contract.

[8]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 2: Identification,* NIST Interagency Report 8238 (Gaithersburg, Md.: Nov. 26, 2018); *Face Recognition Vendor Test (FRVT) Part 2: Identification*, NIST Interagency Report 8271 (Gaithersburg, Md.: Sept. 11, 2019); and *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency Report 8280 (Gaithersburg, Md.: Dec. 19, 2019).

[9]We selected two reports about 6-months apart from each year beginning in 2017, which was the beginning of NIST's current testing methodology, to 2019. National Institute of Standards and Technology, *Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification,* NIST Interagency Report (Gaithersburg, Md.). The sampled reports include those published on March 23, 2017; August 25, 2017; February 15, 2018; June 21, 2018; April 4, 2019; and September 11, 2019.

[10]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Performance of Automated Gender Classification Algorithms,* NIST Interagency Report 8052 (Gaithersburg, Md.: Apr. 20, 2015).

NIST vendor test reports; were referenced among studies; and were recent (2019), given that older evaluations likely no longer apply due to major advancements in the technology.[11]

To examine privacy protections under federal and state law applicable to commercial use of facial recognition technology, we reviewed and analyzed federal and state laws that govern the use of biometric information. To conduct this analysis, we reviewed previous GAO reports related to privacy and facial recognition technology, statutes, regulations, and legal commentaries using databases such as Westlaw, as well as other documents and information from state government websites and relevant stakeholder groups including the National Conference of State Legislatures.[12] For comparison purposes, we also reviewed the European Union's General Data Protection Regulation (GDPR) and literature describing its effects. In addition to the stakeholders cited earlier, we interviewed current representatives and one former representative of the European Data Protection Supervisor to discuss the European Union's General Data Protection Regulation and other privacy legislation.

To examine privacy frameworks developed by private entities, we reviewed eight facial recognition privacy standards and practices issued since 2014 by industry associations, privacy advocacy groups, and other

[11]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); 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 (January 2019); John Howard, Yevgeniy Sirotin, and Arun Vemury, "The Effect of Broad and Specific Demographic Homogeneity on the Imposter Distributions and False Match Rates in Face Recognition Algorithm Performance," *IEEE International Conference on Biometrics Theory, Applications, and Systems* (September 2019); and K.S. Krishnapriya, et al. *Characterizing the Variability in Face Recognition Accuracy Relative to Race,* arXiv:1904.07325v3 [cs.CV] (May 8, 2019).

[12]See GAO, *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps*, GAO-19-621T (Washington, D.C.: June 11, 2019); *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, D.C.: Feb. 21, 2019); *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GAO-19-52 (Washington D.C.: Jan. 15, 2019); *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (Washington, D.C.: July 30, 2015); and *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

organizations. We identified these documents through our literature review, interviews with industry representatives, and other relevant research.[13] In addition, we reviewed the privacy policies of 30 businesses selected to represent a diverse range of industries identified in our literature review, including the retail, automotive, financial, hospitality, and technology sectors.

We conducted this performance audit from March 2019 through July 2020 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 our findings and conclusions based on our audit objectives.

[13]Some of these privacy standards and practices were broader privacy practices, while others are more specific to facial recognition technology.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Alicia Puente Cackley, 202-512-8678 or cackleya@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Kay Kuhlman (Assistant Director), Verginie Tarpinian (Analyst-in-Charge), Emily Bond, Richard Hung, Dan Luo, Ian P. Moloney, Christine Ramos, William Reeves, Terry Richardson, Jena Sinkfield, Tyler Spunaugle, and Richard Zarrella made key contributions to this report.