United States Government Accountability Office

Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

July 2015

FACIAL RECOGNITION TECHNOLOGY

Commercial Uses, Privacy Issues, and Applicable Federal Law

Accessible Version

GAO-15-621

July 2015

FACIAL RECOGNITION TECHNOLOGY

Commercial Uses, Privacy Issues, and Applicable Federal Law

GAO Highlights

Highlights of GAO-15-621, a report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate

Why GAO Did This Study

Facial recognition technology—which can verify or identify an individual from a facial image—has rapidly improved in performance and now can surpass human performance in some cases. The Department of Commerce has convened stakeholders to review privacy issues related to commercial use of this technology, which GAO was also asked to examine.

This report examines (1) uses of facial recognition technology, (2) privacy issues that have been raised, (3) proposed best practices and industry privacy policies, and (4) potentially applicable privacy protections under federal law. The scope of this report includes use of the technology in commercial settings but not by government agencies. To address these objectives, GAO analyzed laws, regulations, and documents; interviewed federal agencies; and interviewed officials and reviewed privacy policies and proposals of companies, trade groups, and privacy groups. Companies were selected because they were among the largest in industries identified as potential major users of the technology, and privacy groups were selected because they had written on this issue.

What GAO Recommends

GAO makes no recommendations in this report. However, GAO suggested in GAO-13-663 that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace, and facial recognition technology is such a change. GAO maintains that the current privacy framework in commercial settings warrants reconsideration

.

View GAO-15-621. For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

What GAO Found

Facial recognition technology can be used in numerous consumer and business applications, but the extent of its current use in commercial settings is not fully known. The technology is commonly used in software that manages personal photographs and in social networking applications to identify friends. In addition, several companies use the technology to provide secure access to computers, phones, and gaming systems in lieu of a password. Facial recognition technology can have applications for customer service and marketing, but at present, use in the United States of the technology for such purposes appears to be largely for detecting characteristics (such as age or gender) to tailor digital advertising, rather than identifying unique individuals. Some security systems serving retailers, banks, and casinos incorporate facial recognition technology, but the extent of such use at present is not fully known.

Privacy advocacy organizations, government agencies, and others have cited several privacy concerns related to the commercial use of facial recognition technology. They say that if its use became widespread, it could give businesses or individuals the ability to identify almost anyone in public without their knowledge or consent and to track people's locations, movements, and companions. They have also raised concerns that information collected or associated with facial recognition technology could be used, shared, or sold in ways that consumers do not understand, anticipate, or consent to. Some stakeholders disagree that the technology presents new or unusual privacy risks, noting, among other things, that individuals should not expect complete anonymity in public and that some loss of privacy is offset by the benefits the technology offers consumers and businesses.

Several government, industry, and privacy organizations have proposed or are developing voluntary privacy guidelines for commercial use of facial recognition technology. Suggested best practices vary, but most call for disclosing the technology's use and obtaining consent before using it to identify someone from anonymous images. The privacy policies of companies GAO reviewed varied in whether and how they addressed facial recognition technology.

No federal privacy law expressly regulates commercial uses of facial recognition technology, and laws do not fully address key privacy issues stakeholders have raised, such as the circumstances under which the technology may be used to identify individuals or track their whereabouts and companions. Laws governing the collection, use, and storage of personal information may potentially apply to the commercial use of facial recognition in specific contexts, such as information collected by health care entities and financial institutions. In addition, the Federal Trade Commission Act has been interpreted to require companies to abide by their stated privacy policies. Stakeholder views vary on the efficacy of voluntary and self-regulatory approaches versus legislation and regulation to protect privacy. GAO has previously concluded that gaps exist in the consumer privacy framework, and the privacy issues that have been raised by facial recognition technology serve as yet another example of the need to adapt federal privacy law to reflect new technologies.

Contents

Abbreviations

Commerce	Department of Commerce
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration

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

July 30, 2015

The Honorable Al Franken
Ranking Member
Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

Dear Senator Franken:

In recent years, facial recognition technology—which can be used to verify or identify an individual from a facial image—has improved to the point where in some cases its accuracy surpasses that of humans. Experts say that in the future it may be feasible to readily identify by name almost any individual in public places or from unidentified photographs online. Some members of Congress and others have raised privacy concerns related to commercial uses of facial recognition technology. The National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce (Commerce), has an effort under way to address privacy issues associated with this technology that involves convening stakeholders to develop a voluntary, enforceable code of conduct for industry participants.

You asked us to review privacy issues related to facial recognition technology. This report examines (1) the uses of facial recognition technology, (2) privacy issues that have been raised in connection with commercial uses of facial recognition technology, (3) proposed best practices and industry privacy policies for facial recognition technology, and (4) privacy protections under federal law that may potentially apply to facial recognition technology. The scope of this report includes use of the technology by companies and other private entities and does not include use by government agencies.[1] This report covers use of the technology in the United States and not in other countries. It focuses primarily on use of the technology to identify or verify an individual and not on facial detection (which simply detects when a face is present).

[1]We have ongoing work on the Federal Bureau of Investigation's use of facial recognition technology and expect to issue a report on that topic early next year.

To address the first and second objectives, we reviewed the Federal Trade Commission's (FTC) 2012 staff report on facial recognition technology and documents from its 2011 forum, Face Facts: A Forum on Facial Recognition Technology; material from NTIA's multistakeholder process on facial recognition technology; and other reports and documents from industry, academics, and consumer and privacy advocates.[2] We also reviewed testimony and written statements from a congressional hearing on privacy issues related to facial recognition technology.[3] To address the third objective, we reviewed industry codes of conduct and best practices specific to facial recognition technology or to biometrics—which identifies individuals by measuring and analyzing their physiological or behavioral characteristics—that have been proposed by various parties. We also reviewed the privacy policies of selected companies with a large social networking presence, retailers, and casino companies. We selected these industries because they were widely cited among government and industry stakeholders as current or potential users of facial recognition technology, and we selected specific companies because they were among the largest in their respective industries. We also reviewed consumer privacy guidelines that have been issued by federal entities, including the White House and FTC. To address the fourth objective, we reviewed and analyzed relevant federal laws and regulations to determine their potential applicability to commercial uses of facial recognition and other biometric technologies with regard to privacy. We also reviewed two state laws in Illinois and Texas, which we selected because they had been identified as expressly addressing privacy issues raised by biometric technologies. We also reviewed prior work we had conducted on federal privacy law as it relates to commercial entities. To address all four objectives, we obtained documentation from and interviewed representatives of FTC, Commerce's NTIA and National Institute of Standards and Technology (NIST), companies that use or develop facial recognition systems, industry trade organizations, and consumer and privacy advocacy organizations, as well as academic experts.

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

[3]*What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012).

We conducted this performance audit from July 2014 to July 2015 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 technology is one of several biometric technologies, which identify individuals by measuring and analyzing their physiological or behavioral characteristics.[4] Biometric technologies have been developed to identify people using their faces, fingerprints, hands, eye retinas and irises, voice, and gait, among other things. Unlike conventional identification methods, such as a card to gain building access or a password to log on to a computer system, biometric technologies measure things that are generally distinct to each person and cannot easily be changed.

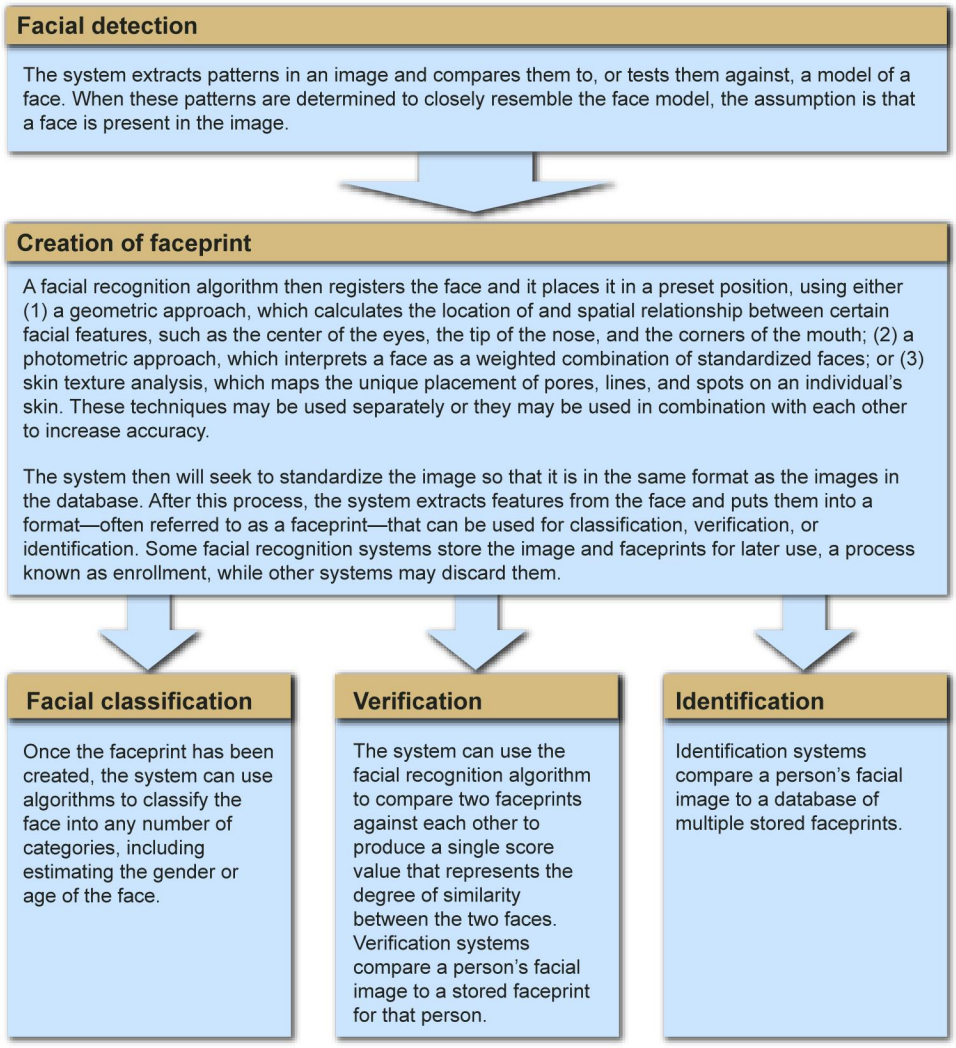
There are generally four basic components to a facial recognition technology system: a camera to capture an image, an algorithm to create a faceprint (sometimes called a facial template), a database of stored images, and an algorithm to compare the captured image to the database of images or a single image in the database.[5] The quality of these components determines the effectiveness of the system. In addition, the more similar the environments in which the images are compared—such as the background, lighting conditions, camera distance, and size and orientation of the head—the better a facial recognition technology system will perform.

[4]We have issued several reports related to biometric technologies, including GAO, *Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies*, GAO-11-276 (Washington, D.C.: Mar. 31, 2011); *Defense Management: DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing*, GAO-09-49 (Washington, D.C.: Oct. 15, 2008); and *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[5]A faceprint or facial template is essentially a digital code that a facial recognition algorithm creates from an image. Faceprints generally are unique to a particular company because different companies use different facial recognition algorithms, according to industry sources.

Facial recognition technologies can perform a number of functions, including (1) detecting a face in an image; (2) estimating personal characteristics, such as an individual's age, race, or gender; (3) verifying identity by accepting or denying the identity claimed by a person; and (4) identifying an individual by matching an image of an unknown person to a gallery of known people. According to FTC staff, academics, and industry experts, most modern facial recognition systems generally follow the steps shown in figure 1.

Figure 1: How Facial Recognition Technology Systems Generally Work



Source: GAO. | GAO-15-621

Facial recognition systems can generate two types of errors—false positives (generating an incorrect match) or false negatives (not generating a match when one exists). NIST has measured the performance of companies' facial recognition algorithms since 1993 and has found that the technology has improved over time. Most recently, NIST's Face Recognition Vendor Test in 2014 found that the error rates continued to decline and algorithms had improved at identifying individuals from images of poor quality or captured under low light.[6] In addition, research supported by the Technical Support Working Group, a federal interagency group, showed that in certain controlled tests, facial recognition algorithms surpassed human accuracy in determining whether pairs of face images, taken under different illumination conditions, were pictures of the same person or of different people.[7]

NTIA is the agency principally responsible for advising the President on telecommunications and information policy issues, including those related to privacy. In February 2014, NTIA began a "multistakeholder process" that has convened various stakeholders to discuss protection of consumer privacy in current and emerging commercial uses of facial recognition technology.[8] This process, which is ongoing, was outlined in a 2012 White House privacy framework, which directed NTIA to convene multistakeholder processes that consist of open, transparent forums in which stakeholders work toward consensus on voluntary, legally

[6]National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms*, NIST Interagency Report 8009 (Gaithersburg, Md.: May 26, 2014).

[7]Alice J. O'Toole, P. Jonathon Phillips, Fang Jiang, Janet Ayyad, Nils Penard, and Hervé Abdi, "Face Recognition Algorithms Surpass Humans Matching Faces over Changes in Illumination," IEEE: Transactions on Pattern Analysis and Machine Intelligence, 29(9), 1642-1646 (September 2007), accessed April 24, 2015, http://www.utdallas.edu/~herve/Abdi-opjapa2007.pdf. The Technical Support Working Group is an interagency group that includes the Departments of Defense, Energy, Homeland Security, and Justice. Its purpose is to support the Department of Defense's Combating Terrorism Technical Support Office.

[8]See National Telecommunications and Information Administration, *Privacy Multistakeholder Process: Facial Recognition Technology,* accessed June 3, 2015, http://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.

enforceable codes of conduct for specific markets or business contexts.[9] The framework also presents privacy principles in the form of a proposed Consumer Privacy Bill of Rights, and states that the codes of conduct developed in NTIA's multistakeholder processes should specify how those principles would apply to different technologies or markets.

FTC is a law enforcement agency that 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.[10]

Facial Recognition Technology Can Be Useful for Many Commercial Applications, but the Extent of Its Use Is Not Fully Known

Facial recognition technology is currently being used in a number of U.S. commercial applications for functions including safety and security, secure access, and marketing and customer service. However the full extent of its present use is not known.

[9]The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C.: Feb. 23, 2012). In February 2012, NTIA requested public comment on the substantive consumer data privacy issues that might be addressed by voluntary codes of conduct. NTIA convened its first multistakeholder process in July 2012, on the topic of mobile application transparency.

[10]Federal Trade Commission, *Facing Facts*.

Facial Recognition Technology Has Applications That Can Be Useful to Consumers and Businesses

Facial recognition technology offers applications beneficial to both consumers and businesses, according to industry representatives and other stakeholders. The International Biometrics & Identification Association has noted that facial recognition and other biometric technologies have until recently been used most prominently by government and law enforcement agencies, such as to protect borders and ports and to identify criminals.[11] However, FTC staff and industry sources have reported that commercial interest and investment in facial recognition technology have grown as the technology has become more accurate and less costly, with new applications being developed for consumers and businesses.[12] The Direct Marketing Association has said that businesses are finding that facial recognition technology can be used as a way to communicate with consumers and provide new tools, products, and services.[13] Industry trade organizations and companies that use and develop facial recognition software have cited four major types of functions that they say do or will benefit from facial recognition technology: photograph identification and organization; safety and security; secure access; and marketing and customer service.

Photograph identification and organization. One of the most well-known current uses of facial recognition technology is photograph identification in social networking applications. For example, some of the top social networking applications use facial recognition technology to identify individuals in photographs. In testimony before Congress, a representative of one such application noted that this allows users to instantaneously link photographs from birthdays, vacations, and other

[11] *The Current and Future Applications of Biometric Technologies: Hearing Before the Subcomm. on Research and Technology of the H. Comm. on Science, Space and Technology*, 113th Cong. 1 (2013) (statement of John Mears, Board Member, International Biometrics & Identification Association). The International Biometrics & Identification Association is a trade association representing providers and users of biometric technologies.

[12] Federal Trade Commission, *Facing Facts*.

[13] The Direct Marketing Association is a global trade association of businesses and nonprofit organizations that use and support data-driven marketing tools and techniques. Its members include retail stores, industrial manufacturers, Internet-based businesses, financial services companies, and publishers, among others.

events with people who participated.[14] In addition, several applications use facial recognition technology to help individuals organize personal photographs stored online or on computer drives. For example, several photograph management software programs can detect individuals, such as family members, which the user has asked to be identified. The programs then automatically add new photographs of these individuals to a photograph album created by the user.

Safety and security. Some retailers, casinos, financial institutions, and apartment buildings use facial recognition technology for safety and security purposes. According to the National Retail Federation, some retailers in the United States are testing systems that use facial recognition technology with closed-circuit television for theft prevention.[15] According to one vendor of such a system with whom we spoke, security cameras in a retail location compare images of individuals who walk into a store against a database of images of known shoplifters, members of organized retail crime syndicates, or other persons of interest. If a match is found, security personnel or management are alerted and provided whatever information is known about the individual. Some casinos in the United States similarly use facial recognition systems to help them identify known or suspected gambling cheaters, members of organized crime networks, or other known persons of concern.[16] Facial recognition technology has also been incorporated into the security systems of some financial institutions to identify robbery suspects or accomplices. According to a vendor of this technology, these systems deter crime and help identify suspects much faster than traditional means, which require staff to spend hours reviewing video recordings. Facial recognition systems have also been used in large apartment buildings to help identify perpetrators of crimes or other known persons of concern who seek to enter the property, according to one software vendor with whom we met.

[14] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 3 (2012) (statement of Robert Sherman, Manager of Privacy and Public Policy, Facebook).

[15] The National Retail Federation is a retail trade association that represents discount and department stores, home goods and specialty stores, grocers, wholesalers, chain restaurants, and Internet retailers from the United States and more than 45 countries.

[16] Outside of the United States, at least one casino in Canada allows people with gambling addictions to voluntarily enroll in a program that uses facial recognition technology to recognize them and notify management if they enter the casino.

Secure access. Facial recognition technology can be used to provide secure physical access control to buildings or other locked areas. For example, some systems unlock a door after a camera confirms the user's identity through facial recognition. In addition, applications exist that allow users to unlock personal computers and smartphones, log into video game consoles, or record workplace time and attendance by recognizing their face, in lieu of using a password or personal identification number. Some systems can distinguish whether an image is live to prevent the use of printed photographs to gain access. Industry representatives have noted that these applications have the benefit of not requiring consumers to remember a password and may eventually become an effective voluntary alternative to the use of passwords to access online transactions.

Marketing and customer service. Industry trade organizations have said they envision retailers and others using facial recognition technology to target marketing and advertising more effectively and improve customer service. The Direct Marketing Association has stated that facial recognition technology has the potential to help businesses provide more customized and improved products and services, conduct market research and product development, provide more tailored and relevant messaging and advertising, and offer a more secure shopping experience. Facial recognition technology is already used in digital signs—usually televisions or kiosks displaying advertisements in stores—with cameras that recognize characteristics of the viewer, such as gender or age range, and target advertisements accordingly. This allows retailers and advertisers to show relevant products and deals in real time, possibly leading to more sales, according to the Digital Signage Federation.[17] In the future, such signs may be used to identify customers by name and target advertising to them based on past purchases or other personal information available about them, according to FTC staff. Facial recognition systems can also be designed to alert staff when known customers enter the store, according to a software vendor with whom we spoke. Representatives of the National Retail Federation told us they could envision retailers using facial recognition systems to track customer movements around the store to provide the customer with a better shopping experience.

[17]The Digital Signage Federation is a trade organization that provides education, networking, and advocacy for the digital signage industry.

Other uses. Several other current or potential uses for facial recognition technology have been cited by industry stakeholders:

- *Facial search engines*. Internet search engines are being developed to allow users to conduct a search using a facial image, or to enter a name to search for images that match the name.
- *Online dating*. Some online dating companies use facial recognition to determine the facial features a user finds most attractive and search their database for individuals with similar features.
- *Memory support*. A memory support application for smartphones assists people with prosopagnosia (face blindness) or other memory-related conditions by confirming the identities and providing the names of family members, friends, caregivers, or others.
- *Hospitality*. Facial recognition technology can be used by hotel and guest services industries to identify guests and enable personalized service without having to ask for a guest name or a room number.

NTIA staff told us that the next major expansion for facial recognition technology could be in mobile applications for consumers. Industry representatives and some experts and privacy advocacy organizations have noted that the technology can be deployed in cell phone applications to compare faces captured by the phone to a database of facial images.[18] Some academics have noted that in the future, these types of applications could be integrated into wearable systems, such as eyeglasses.

The Extent of Commercial Use of Facial Recognition Technology Is Not Fully Known

Facial recognition technology is currently being used in a number of commercial applications in the United States, but the full extent of its present use is not known. The International Biometrics & Identification Association, other industry trade organizations, and FTC staff told us they knew of no comprehensive reliable information on the extent to which U.S. businesses use facial recognition technology. Similarly, our review of literature associated with the technology identified no such data. Representatives of the National Retail Federation and Retail Industry Leaders Association told us that their sense was that retailers are not

[18]*What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 4 (2012) (statement of Brian Martin, Director of Biometric Research, MorphoTrust USA).

using the technology broadly.[19] Several large companies contacted on our behalf by trade associations declined to speak with us about their use of the technology. An industry trade organization representative told us that companies may be reluctant to discuss the technology for competitive reasons.

Two applications in which facial recognition technology appears to now be widely used are photograph identification and management and security access. One large social networking service with more than 1 billion monthly users started using facial recognition technology in 2011 to facilitate "tagging" users' friends in photographs. Other large companies have incorporated the technology into photograph management and social networking applications. Representatives of six other top social networking companies told us that they do not currently use facial recognition technology. Facial recognition technology also has become relatively widely used in providing secure access. For example, versions of one major operating system allow users to unlock devices via facial recognition, as do two of the best-selling home video game systems. Many other companies also offer hardware, software programs, or mobile phone applications using facial recognition technology for photograph management or secure access.

In contrast, our review found that less is known about the current prevalence of facial recognition for marketing and security uses. According to the World Privacy Forum,[20] some companies in Europe and Asia currently use facial recognition technology to enhance marketing and customer service, but such use in the United States is less common.[21] A representative of the National Retail Federation told us that U.S. retailers were exploring facial recognition for such purposes, but were taking a slower approach than their overseas counterparts because of concerns over customer reaction. According to the Digital Signage Federation, some digital signs in the United States, such as video monitors displaying

[19]The Retail Industry Leaders Association is a trade association representing large retail companies, product manufacturers, and service suppliers.

[20]The World Privacy Forum is a privacy advocacy organization that focuses on privacy as it relates to topics including technology, health care, finance, and workplace issues.

[21]For example, one technology services company has developed a facial recognition system for a large European shopping center that can scan up to 15,000 customers per day and generate targeted notifications to known individuals.

advertisements in stores, are used to detect a face or characteristics, such as age and gender for targeted marketing.

Some safety and security applications using facial recognition technology are marketed to retailers, casinos, financial institutions, and other businesses, but the extent of their use is uncertain. A representative of the National Retail Federation said that many retailers were at least in the early stages of looking into facial recognition systems for security purposes, but knew of no data on their current use. A representative of the American Gaming Association told us that facial recognition does not appear to be widely used in U.S. casinos, but that it did not have comprehensive data on such use.[22] Representatives from the American Bankers Association and Financial Services Roundtable told us that they were unaware of any data on the extent of use of facial recognition technology by financial institutions.[23] The American Bankers Association representative said at least one major U.S. bank uses facial recognition technology to identify robbery suspects, but two other major banks stated the technology was not in broad use by financial institutions because of concerns over its accuracy. The International Biometrics & Identification Association told us that some businesses are reluctant to disclose use of the technology because publicizing their specific security practices can diminish their effectiveness.

[22]The American Gaming Association is a trade organization representing the U.S casino industry. Its members include commercial and tribal casino operators, suppliers, and other entities affiliated with the gaming industry.

[23]The American Bankers Association is a trade group representing small, regional, and large banks. The Financial Services Roundtable is a trade organization representing the financial services industry. Its members include banking, insurance, asset management, finance, and credit card companies in the United States.

Stakeholders Have Raised Privacy Concerns Related to the Commercial Use of Facial Recognition Technology

A number of stakeholders—including federal agencies, privacy and consumer groups, and some industry representatives—have identified privacy issues related to commercial use of facial recognition technology. In particular, concerns have been raised by the technology's potential to identify and track individuals in public without their knowledge, and around the collection, use, and sharing of personal data associated with the technology. However, some industry stakeholders have argued that the technology does not present new or unusual privacy risks, or that such risks can be mitigated.

Privacy Concerns Have Been Raised Related to the Ability to Identify and Track Individuals in Public

While acknowledging the potential benefits of commercial use of facial recognition technology, government agencies, privacy advocacy organizations, academics, and others have raised a number of privacy concerns about the technology and its future direction. As noted earlier, facial recognition technology continues to rapidly improve in accuracy. Further, individuals continue to upload billions of pictures to social networking and other Internet sites, creating a vast repository of facial images that are often linked to names or other personal information. The convergence of these two trends may make it technically feasible one day to identify almost any individual in a wide range of public spaces, according to some privacy advocacy organizations and others. Key privacy concerns related to the commercial application of facial recognition technology have generally centered around (1) its effect on the ability of individuals to remain relatively anonymous in public; (2) the capacity to track individuals across locations; and (3) use of facial recognition without individuals' knowledge or consent.

Reduction of Anonymity

During the NTIA multistakeholder process, some participants expressed concern that facial recognition technology could affect personal privacy by reducing individuals' ability to be anonymous when in a public or commercial space, such as a sidewalk or store. The Center for Democracy & Technology[24] has noted that when most individuals are in public, they expect a few people or businesses to recognize their face, but fewer to connect a name to their face, and even fewer to associate their face with Internet behavior, travel patterns, or other profiles.[25]

[24]The Center for Democracy & Technology is a nonprofit organization that advocates for the freedom of expression and privacy protection of Internet users.

[25]Center for Democracy & Technology, *Seeing is Id'ing: Facial Recognition & Privacy* (Washington, D.C.: Jan. 22, 2012).

Commercial use of facial recognition technology for identification purposes, the group states, has the potential to change this dynamic by allowing companies or individuals to collect information on any individual captured by a camera. Privacy advocacy organizations and academics have expressed concern that as being remotely identified in commercial settings becomes more common, some individuals may be uncomfortable visiting certain places, shopping at certain establishments, or assembling in public for a cause they support. Further, the Electronic Privacy Information Center has stated that individuals lose some control over their identity if they are not allowed to choose whether or not they want to remain anonymous in public.[26] The organization has also noted that additional privacy concerns would be raised by use of the technology to identify not just who someone is, but whom they are with.

Tracking

Some participants in the NTIA multistakeholder process and others have expressed concern that facial recognition technology could be used to track individuals' movements in public, which they said could erode personal privacy. Industry sources told us that, at present, facial recognition technology is not used in a commercial context to track consumers on any widespread scale. However, the Center for Democracy & Technology has stated that if use of the technology to identify individuals in public were deployed widely enough in the future, and if businesses shared facial recognition data with one another, the result could be a network of cameras that readily tracked a consumer's movements from location to location. Further, it noted that unlike other tracking methods, facial recognition does not require an individual to wear a special device or tag, which reduces individuals' ability to avoid unwanted tracking. A representative of the World Privacy Forum told us that most consumers would find it invasive of their privacy for security cameras to be used to track their movements for marketing purposes. Likewise, FTC staff have reported that the privacy risks for consumers would increase if companies began using images gathered through digital signs to track consumers across stores. These issues are underscored by concerns consumers have expressed about being tracked in other contexts. For example, a 2009 consumer survey on marketing found that about two-thirds of respondents did not want online advertising targeted

[26]The Electronic Privacy Information Center is a privacy advocacy and research organization that focuses on emerging privacy and civil liberties issues related to digital technology.

to them if it involved having their offline activity tracked.[27] Likewise, a representative of the National Retail Federation told us that customers of a major department store chain reacted negatively after the store posted signs disclosing that customers' movements within the store were being tracked via their mobile phones.

Knowledge and Consent

Another concern that has been raised is the commercial use of facial recognition technology for identification or verification without individuals' knowledge or consent. Unlike other biometrics, such as fingerprint identification, facial recognition technology can be used to capture a face remotely and without the individual's knowledge. In addition, even if consumers are notified and given the option to opt out of the technology, that option may become less feasible as the use of this technology grows. Some industry trade organizations have acknowledged these concerns and expressed caution over deploying the technology in certain contexts without consumer notification and consent. For example, the Software & Information Industry Association said that firms may need to obtain consent prior to deploying the technology in digital signs to identify individuals and record their interests and preferences. The Computer and Communications Industry Association stated that firms' use of facial recognition technology to match individuals' names and other biographical information with their faces should be transparent and provide individuals the ability to opt out.

Some Stakeholders Believe Facial Recognition Technology Raises Issues about the Use and Security of Personal Data

Privacy advocacy organizations, government agencies, academics, and some industry representatives also have raised privacy and security issues associated with personal data collected in conjunction with commercial use of facial recognition technology. Many of these issues mirror concerns about the collection, use, and sharing of personal data more broadly by commercial entities.[28] Key data privacy issues that have

[27]Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It* (Sept. 29, 2009), accessed March 2, 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[28]We discuss privacy issues associated with private-sector companies' collection, use, and sale of personal information for marketing and individual reference services in GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

been raised with regard to facial recognition technology in particular include the following:

- **Consumer control over personal information.** Some privacy advocacy organizations and others have reported that, like other forms of personal data, 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. Commenters to the FTC Face Facts Forum noted that the proliferation in recent years of information resellers, and of data sharing among third parties, raises questions about whether faceprints and associated personal data may one day be sold or shared. Facial recognition data may be particularly valuable to marketers because they potentially could link a person's online presence and offline presence, according to two experts we spoke with. One privacy expert told us that risks to consumer privacy would increase if retailers were to develop relationships with social networking sites, which typically possess consumers' facial images and detailed personal information that could be used for marketing. As we concluded in our September 2013 report on information resellers, consumers generally do not have the right to prevent their personal information from being collected, used, or shared for marketing purposes.[29]

- **Data security.** Industry trade organizations, government agencies, and privacy advocacy organizations have noted that commercial use of facial recognition technology raises the same security concerns as those associated with any personal data. Participants in the NTIA multistakeholder process noted that facial recognition data could be subject to data breaches that result in sensitive biometric data being revealed to unauthorized entities. Because a person's face is unique, permanent (absent surgery), and therefore irrevocable, a breach involving data derived from or related to facial recognition technology may have more serious consequences than the breach of other information, such as passwords or credit card numbers, which can be changed. The Electronic Privacy Information Center has stated that the risk of theft of data associated with the technology could increase the possibility of identity theft, harassment, and stalking. The International Biometrics & Identification Association has said that faceprints, when stored with other identity data, should be considered

[29]GAO-13-663.

personally identifiable information and provided all the security and privacy protections bestowed upon these personal data. At the same time, industry representatives have noted that security concerns are mitigated, to some extent, because at present faceprint algorithms are specific to a vendor and of little use outside that vendor's system if obtained through a breach.

- **Misidentification.** Industry and other stakeholders have said that facial recognition technology may generate more matching errors than other forms of biometric identification because facial recognition technology systems are currently less accurate than other biometrics. Representatives of the Electronic Privacy Information Center have expressed concern that if someone's image is captured and misidentified, adverse information—such as an incorrect identification of an individual as a shoplifter—could propagate in the long-term throughout different commercial systems, sometimes without the individual's knowledge.

- **Disparate treatment.** Some stakeholders in the NTIA multistakeholder process expressed concerns about disparate treatment for certain groups based on information derived from facial recognition systems. They also noted that individuals who declined to consent to a retailer's request for facial recognition could be denied access to certain products or services. The World Privacy Forum expressed the view that digital signage networks have the potential to create a new form of marketing surveillance that it believes raises the possibility of unfairness, discrimination, and abuses of personal information. In addition, the Center for Democracy & Technology has expressed concerns about the use of facial recognition technology for classification purposes, such as to detect gender, race, and age range. The organization expressed the view that this could lead to profiling—the use of personal characteristics or behavior patterns to make generalizations about a person—that could lead to, for example, price discrimination for certain groups.

Other Stakeholders Believe That the Technology Does Not Present New or Unusual Privacy Risks

In contrast, some industry representatives have argued that commercial use of facial recognition technology does not present new or unusual privacy risks, that risks that do exist can be mitigated, and that any potential loss of privacy should be weighed against the benefits the technology confers. In position papers, other written materials, or in interviews we conducted, some industry stakeholders have expressed the following views:

- **Individuals should not expect complete anonymity in public.** The National Retail Federation and the International Biometrics & Identification Association have argued that individuals effectively give up some of their anonymity when they make their faces public. The latter has contended that privacy and anonymity are not the same and that losing complete anonymity is not tantamount to a surrender of privacy. Further, the organization has argued that capturing a facial image or faceprint in public does not necessarily remove an individual's anonymity because it does not directly reveal a name, Social Security number, or any other personal information.

- **Surveillance is already part of our daily life.** The International Biometrics & Identification Association has noted that commercial entities already routinely have security cameras and that facial recognition does not increase their use. Further, it says that privacy advocacy organizations may have overstated the capabilities of facial recognition technology systems, noting that cameras generally are not interconnected and that it is not practical to conceive of a commercial application that would use multiple cameras to track individuals' movements.

- **Consumers have shown a willingness to give up some privacy for the benefits technology offers.** Industry stakeholders have generally noted that there are inherent trade-offs between some loss of privacy and the benefits that new technologies confer to consumers and businesses, and to economic growth in general. As we noted in our September 2013 report on information resellers, representatives of the marketing and information technology industries, among others, have argued that consumers' expectations and notion of privacy have changed in an era of innovative technologies.[30] For example, they said, consumers have shown they are willing to share private information in public settings—such as by posting to social networking sites in order to gain such benefits as photograph sharing and management.

- **The need for consent should depend on the context.** Industry trade organizations including the Software & Information Industry Association, Computer and Communications Industry Association, and National Retail Federation have stated that the need for

[30]GAO-13-663.

consumer consent should depend on the context under which facial recognition technology is used. For example, two of the trade organizations say that businesses that use the technology for security may not need to obtain consent before using the technology, as opposed to social networking sites that have repositories of facial images to identify individuals more broadly.

- **Facial recognition technology should not be singled out.** Some industry representatives have stated that the privacy issues associated with facial recognition technology are largely the same as those for any biometric technologies—particularly for emerging technologies like voice or gait recognition, which also can identify individuals from afar without their knowledge. Several facial recognition technology companies have said that policymakers should focus on protecting personal information, which would include all biometrics, not just facial recognition technology.

Several Stakeholders Have Suggested Privacy Guidelines, and Company Privacy Policies Vary in Addressing Facial Recognition

Several government, industry, and privacy organizations have proposed or are developing suggested privacy guidelines for commercial use of facial recognition technology. Firms may describe how they collect, use, and store data in published privacy policies, and the policies we reviewed varied in whether and how they addressed facial recognition technology.

Privacy Guidelines Have Been Proposed by Several Organizations

Several different groups, including a government agency, industry trade organizations, and a privacy advocacy organization have proposed, or are in the process of developing, privacy guidelines or best practices for commercial use of facial recognition technology. Most of these guidelines are based at least to some extent on the Fair Information Practice Principles, a set of internationally recognized principles for balancing the

privacy and security of personal information with other interests.[31] Our review found some areas of agreement in the different organizations' recommended practices—for example, all recommended that users of facial recognition technology publish a privacy policy describing their data collection practices. However, the guidelines differed in other key areas, such as if and when firms should obtain individuals' consent prior to using the technology to identify them.

NTIA Multistakeholder Process

As of June 2015, NTIA's multistakeholder process for facial recognition was ongoing. As noted previously, the goal of the process is to develop a voluntary, enforceable code of conduct for facial recognition technology that incorporates privacy principles outlined in the 2012 White House privacy framework. Once the process is complete, companies for which the code is relevant may commit to abide by the code, and that company's adherence to the code, after having made such a commitment, is enforceable by FTC.

The process is open to the public and has involved a series of meetings held in Washington, D.C., with remote access via teleconference and webcasting. At the 11 meetings that NTIA had convened as of June 2015, stakeholders have discussed the privacy and technical issues related to current and potential uses of facial recognition technology, and how a code of conduct might address those issues.[32] Topics of discussion have included issues to be considered in drafting a code of conduct, who its provisions should apply to, the circumstances under which informed consent should be obtained from consumers, and the impact of a code of conduct. The participants with whom we spoke had mixed views on the

[31]The Fair Information Practice Principles were first proposed by a U.S. government advisory committee in 1973, and the Organisation for Economic Co-operation and Development developed a revised version in 1980 that has been adopted by many organizations and governments. The principles address the collection and use of personal information, data quality and security, and transparency, among other things, and have served as the basis for many of the privacy recommendations federal agencies have made. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Paris, France: Sept. 23, 1980).

[32]NTIA noted that the meetings have included panel discussions and presentations by representatives of individual biometric technology companies, trade organizations for the biometrics and interactive advertising industries, privacy advocacy groups, consumer groups, academics, technical experts, government agencies, and international partners. Representatives of other organizations, such as social networking companies, have attended meetings but not made formal presentations.

process. One industry participant said that the meetings had provided a good forum for discussing concerns about the technology, while other participants expressed concern that the process was moving slowly or that any resulting code of conduct would not be widely adopted or provide real privacy protections. Some participants expressed disappointment that there has not been greater involvement by social networking services, given that they are major users of the technology and possess large numbers of faceprints. In June 2015, nine privacy and consumer groups issued a joint statement announcing that they were withdrawing from the multistakeholder process, stating that the process was unlikely to yield a set of privacy rules that offers adequate protections for the use of facial recognition technology.[33] Other stakeholders decided to continue the discussions toward a code of conduct, and the next meeting was scheduled for July 28, 2015.[34]

International Biometrics & Identification Association

In August 2014, the International Biometrics & Identification Association released "Privacy Best Practice Recommendations for Commercial Biometric Use," which it also submitted as part of the NTIA process.[35] Key elements of these recommendations for businesses include the following:

- Users of biometric technologies, which include facial recognition technology, should publish privacy policies, which should specify the types and purposes of the biometric data captured, the nonbiometric data that are being associated with the biometric data, and the amount of time that biometric data will be stored.
- When using biometrics to detect or classify an individual, businesses should post a general notice. When using biometrics to identify an

[33]The statement was signed by representatives of the American Civil Liberties Union, Center for Democracy & Technology, Center for Digital Democracy, Center on Privacy & Technology at Georgetown Law School, Common Sense Media, Consumer Action, Consumer Federation of America, Consumer Watchdog, and Electronic Frontier Foundation, and can be accessed at https://www.democraticmedia.org/sites/default/files/field/public/2015/privacy_advocates_statement_on_ntia_facial_recognition_process_-_final.pdf (accessed July 21, 2015).

[34]National Telecommunications and Information Administration, Notice of Open Meeting, Multistakeholder Process To Develop Consumer Data Privacy Code of Conduct Concerning Facial Recognition Technology, 80 Fed. Reg. 41,486 (July 15, 2015).

[35]International Biometrics & Identification Association, *IBIA Best Practice Recommendations for Commercial Biometric Use* (Washington, D.C.: August 2014), accessed June 22, 2015, https://www.ibia.org/resources/.

individual, whether to provide notice depends on the context; for example, universal notification may be impractical, the association said, if the technology is used to identify every person entering an office building.

- Firms should use good cybersecurity practices to protect any information collected or retained; provide a mechanism for consumers to obtain a record of data maintained on them and have that data corrected if necessary or removed; restrict third-party access to biometrics unless that access is disclosed as a purpose of the data collection; and maintain an appropriate audit trail for accountability.

The International Biometrics & Identification Association does not currently track implementation of these recommendations and refers to them as "general guidelines." It also says that it leaves it to those using the technology to determine what is most appropriate given the application and its purpose, the risk and consequence of abuse, and the nonbiometric data used. The American Civil Liberties Union and the Center for Digital Democracy have been critical of these best practices, objecting, for example, to the statement that it is impractical to obtain consent for use of facial recognition from consumers entering buildings.[36]

American Civil Liberties Union

The American Civil Liberties Union issued "An Ethical Framework for Facial Recognition" in May 2014, and provided it for discussion during the NTIA multistakeholder process.[37] The framework recommends stricter standards for use, notice, and consent than those recommended by the International Biometrics & Identification Association, including that users of facial recognition technology should

- not use the technology to determine an individual's race, color, religion, sex, national origin, disability, or age;
- prominently notify individuals when facial recognition is in operation;

[36]The American Civil Liberties Union is an advocacy organization that focuses on issues related to individual rights and liberties. The Center for Digital Democracy is a consumer protection and privacy organization that conducts research, public education, and advocacy focusing on issues related to technology.

[37]American Civil Liberties Union, *An Ethical Framework for Facial Recognition* (May 2014), accessed August 4, 2014, http://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf.

- obtain specific consent from an individual before storing a photograph or faceprint of that person or sharing any facial recognition data with a third party;
- allow individuals to access, correct, and delete their faceprint information; and
- consider what special precautions might be needed when using a facial recognition system with teenagers.

Digital Signage Federation

In February 2011, the Digital Signage Federation issued privacy standards for its members that it developed in collaboration with the Center for Democracy & Technology.[38] Among other things, the standards state that companies should

- disclose in privacy policies the data collected by digital signs and the purpose of the data;
- obtain affirmative consent before using facial recognition to identify an individual;
- notify consumers at the physical location of the sign when using facial recognition (or other means) to collect other information about an individual, such as age range or gender;
- not share data for any uses incompatible with those specified in the privacy policy; and
- allow consumers to submit complaints and request to access their data.

The Digital Signage Federation has a process to certify that member firms are abiding by these standards, and the federation reported that 28 of its 221 member firms had been certified as of May 2015.[39]

Federal Trade Commission

FTC issued a staff report in October 2012 that included recommended best practices for commercial uses of facial recognition technology to protect consumer privacy.[40] The report synthesized the discussions and comments from FTC's December 2011 Face Facts Forum to explore advances in facial recognition technologies, current and possible future commercial uses, ways consumers can benefit from these uses, and

[38]Digital Signage Federation, *Digital Signage Privacy Standards* (February 2011), accessed May 2, 2015, http://www.digitalsignagefederation.org/standards.

[39]Digital Signage Federation, *DSF Seal of Professional Excellence (SPE),* accessed May 2, 2015, http://www.digitalsignagefederation.org/dsf_seal.

[40]Federal Trade Commission, *Facing Facts*.

privacy and security concerns.[41] FTC staff said the best practices are intended to provide guidance to commercial entities that are using or plan to use facial recognition technologies in their products and services, while promoting innovation. The best practices were based on core principles outlined in FTC's March 2012 report on consumer data privacy.[42] These principles included providing consumers with meaningful choices about use of their data at a relevant time and context, ensuring that practices related to information collection and use are transparent, and building in privacy protections during product development. Among the best practices recommended for companies using facial recognition technology were

- obtaining individuals' affirmative consent before identifying them in anonymous images to someone who could not otherwise identify them;
- providing clear notice to individuals when using facial recognition to detect demographic characteristics;
- providing individuals with a choice about whether any data collected with facial recognition technology are shared with third parties; and
- implementing a specified retention period for personal data and disposing of stored images once they are no longer necessary for the purpose for which they were collected.

One FTC commissioner issued a dissenting statement with the staff report, stating there was little evidence that facial recognition technology was likely to cause tangible injuries to consumers in the near future, and that following the staff report's recommendations would create a burden on businesses in many contexts. Representatives of several privacy advocacy organizations told us they believed the FTC staff report provided a good summary of the issues but had not resulted in noticeable changes in industry practices.

Privacy by Design

In addition to best practices and codes of conduct, some stakeholders have advocated addressing consumer privacy through "privacy by design"—the practice of building in consumer privacy protections at every

[41]See archived webcasts of the Federal Trade Commission's Face Facts: A Forum on Facial Recognition Technology at https://www.ftc.gov/news-events/events-calendar/2011/12/face-facts-forum-facial-recognition-technology.

[42]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington D.C.: March 2012).

stage of product development. For example, FTC staff and the Privacy Rights Clearinghouse have both noted that systems can be designed to ensure that data collected by facial recognition technology are not used beyond specified purposes, either by automatically deleting the data after they are used, or ensuring the data cannot be repurposed.[43] The International Biometrics & Identification Association has cited the need for systems that block "web-crawlers," which seek to surreptitiously gather images and other information from websites containing facial images and other personal data.[44] Firms that develop facial recognition technology also told us that some measures can be taken to build privacy controls into facial recognition systems. These include segregating biometric data from other personal data, as well as encrypting data, which can be especially important for entities that possess large numbers of photographs matched with other identifying information. However, some representatives of industry and privacy advocacy organizations have argued that privacy by design has limitations. Industry representatives noted that facial recognition technology systems generally are built to be flexible and provide users with the option to choose among different levels of privacy protection. This may allow users to bypass privacy protections, such as a data retention time frame, that have been included in the system's design.

Some Companies Address Facial Recognition Technology in Their Privacy Policies

We reviewed the written privacy policies, as of May 2015, of selected businesses in three industries—social networking, retail, and gaming—to identify whether and how these policies expressly addressed facial recognition technology.[45] In published privacy policies, firms may describe the data they collect, their uses for these data and circumstances under

[43]Federal Trade Commission, *Facing Facts*. The Privacy Rights Clearinghouse is a privacy advocacy organization that focuses on raising consumers' awareness on how technology affects personal privacy.

[44]International Biometrics & Identification Association, *Comments Submitted to Face Facts: A Forum on Facial Recognition Technology—Project No. P115406* (Jan. 31, 2012), accessed June 4, 2015, https://www.ftc.gov/policy/public-comments/comment-00074-3.

[45]As previously discussed, we selected these industries because they were widely cited among government and industry stakeholders as current or potential users of facial recognition technology, and we selected specific companies because they were among the largest in their respective industries. While we identified whether and how the privacy policies addressed facial recognition technology specifically, we did not conduct a broad evaluation or assessment of these policies more generally.

which they may be shared with third parties, and how these data are stored. Firms that publish a privacy policy may not be required to describe their use of facial recognition technology, if any. Therefore, some firms may be using facial recognition technology even if they do not address the technology in their privacy policies. However, because we were unable to determine whether most companies we selected used facial recognition technology, their failure to mention it in their privacy policies could also mean that they do not use the technology.

Two companies operating social networking applications that use facial recognition technology expressly address how they use the technology in their privacy policies and associated documents.[46] One of these companies automatically uses facial recognition technology to facilitate tagging a user's friends in photographs unless the user opts out. The user can turn off the facial recognition feature, at which time the user's facial templates are deleted. Users can also "untag" themselves in photographs. Company representatives told us that the firm's approach to privacy is to provide multiple opportunities for users to exercise control over their data—for example, through privacy settings and tools that allow users to select who can see their personal information and content. Company representatives told us that the firm has no plans at this time to share facial recognition faceprints with third parties and that personal information associated with facial recognition technology would not be shared without user consent.

In contrast, the second company requires users to approve the use of its face tagging feature before it is enabled, which company representatives told us is in accordance with the FTC staff report's suggested best practices. That company told us it does not share and has no plans to share personal information associated with facial recognition technology without user consent, except in very limited circumstances as described in its privacy policy (i.e., with domain administrators, for external processing by company affiliates or trusted parties, or for legal reasons).

This company has also developed a digital eyeglass product. In a June 2013 letter to a Member of Congress, the company said it would not provide facial recognition capabilities for that product, or allow third-party

[46]Representatives of six other top social networking companies told us that they do not currently use facial recognition technology.

developers to do so, until it had strong privacy protections in place.[47] The letter also stated that the company would prohibit developers from disabling a feature that would alert the public when the digital eyeglass product was being used to take a photograph or video. The firm also stated that the product was covered by the company's privacy policy and that no changes were contemplated for its privacy policy to specifically address the product.

The five major retail chains and four large casino companies that we selected did not expressly address facial recognition technology in their written privacy policies, although as indicated earlier, we were unable to determine whether these firms use the technology.[48] A representative from the National Retail Federation told us that retailers' privacy policies are written broadly enough to address facial recognition technology, even if they do not expressly mention it. The privacy policies of three of the five retailers we reviewed did address their stores' use of video cameras (which can be a component of facial recognition systems). All three policies specified that the cameras are used for security purposes or to measure store traffic, while one policy noted that the cameras were used for collecting information about their customers. None of the five policies made reference to the use of digital signs, which, as noted earlier, can incorporate facial recognition technology. Similarly, none of the privacy policies of the four large U.S.-based casino companies we reviewed made reference to the use of facial recognition technology in the United States.[49]

[47]Letter from Susan Molinari, Vice President, Public Policy and Government Relations, Google, Inc., to Representative Joe Barton, Texas (June 7, 2013). This letter was publicly released by Congressman Joe Barton on his website http://www.joebarton.house.gov/images/user_images/gt/Google_Glass_Response_2013_Letter.pdf.

[48]We selected the five largest U.S. retailers based on sales and the four largest U.S.-based casino companies based on revenues.

[49]One of the casino companies disclosed in its privacy policy the use of facial recognition technology at its Canadian casinos for a self-exclusion program that problem gamblers can voluntarily enroll in.

Some Federal Laws May Potentially Apply to Facial Recognition Technology, but Do Not Fully Address Stakeholder Privacy Issues

Some federal laws may potentially be applicable to the commercial use of facial recognition technology, but these laws do not fully address the privacy concerns that have been raised about facial recognition technology by some stakeholders. Views differ on the need for additional legislation.

Federal Law Does Not Expressly Regulate the Commercial Use of Facial Recognition Technology, but Some Laws May Potentially Apply in Certain Circumstances

The United States does not have a comprehensive privacy law governing the collection, use, and sale of personal information by private-sector companies.[50] In addition, we did not identify any federal laws that expressly regulate commercial uses of facial recognition technology in particular. However, there are three areas in which certain federal laws that address privacy and consumer protection may potentially apply to commercial uses of facial recognition technology: (1) the capture of facial images; (2) the collection, use, and sharing of personal data; and (3) unfair or deceptive acts or practices, such as failure to comply with a company's stated privacy policies.

Capture of Facial Images

Generally, individuals can take pictures while on public property and in commercial spaces open to the public unless prohibited by the business or property owner. We did not identify federal laws that generally restrict the capture of facial images. One federal law, the Video Voyeurism Prevention Act of 2004, prohibits the taking of certain types of pictures in limited circumstances.[51] The act makes it a crime to intentionally capture an image of a "private area" of an individual without his or her consent, or to knowingly do so under circumstances in which that individual has a

[50]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 entities 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.

[51]Video Voyeurism Prevention Act of 2004, Pub. L. No. 108-495, 118 Stat. 3999 (2004) (codified at 18 U.S.C. § 1801).

reasonable expectation of privacy.[52] While the definition of a private area does not include a person's face, the act could affect the specific placement of cameras in certain parts of commercial spaces, such as retail stores' dressing rooms.

Collection, Use, and Storage of Personal Information

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 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. These laws may potentially apply to facial recognition technology in two ways. First, they may potentially limit some firms' ability to share data collected with facial recognition technology, such as a person's image and faceprint, or a person's location at a given time. Second, these laws may potentially limit firms' access to personal information that could be used in connection with the technology, such as a person's photograph, name, age, address, or purchase history. As shown in table 1, the general applicability of these laws depends on some combination of the source of the data, the means of collection, the entity collecting the data, the type of data being collected, and the purpose for which the data are being used. For additional details on these federal laws and their potential applicability to facial recognition technology, see appendix II.

Table I: Federal Laws Specifically Addressing the Collection, Use, and Storage of Personal Information

Federal law	Applicability to collection, use, and storage of personal information
Driver's Privacy Protection Act [Note A]	Addresses the use and disclosure of personal information contained in state motor vehicle records.
Gramm-Leach-Bliley Act [Note B]	Governs the disclosure of nonpublic information collected by financial institutions, and sets standards for data security.

[52]The act defines "circumstances in which that individual has a reasonable expectation of privacy" as, in part, circumstances in which a reasonable person would believe that their private area would not be visible to the public, regardless of whether that person is in a public or private place. 18 U.S.C. § 1801(b)(5).

Federal law	Applicability to collection, use, and storage of personal information
Health Insurance Portability and Accountability Act [Note C]	Governs the disclosure of individually identifiable health information collected by covered health care entities, and sets standards for data security.
Fair Credit Reporting Act [Note D]	Governs the disclosure of personal information collected or used for eligibility determinations for such things as credit, insurance, or employment.
Family Educational Rights and Privacy Act [Note E]	Governs the disclosure of personally identifiable information from education records.
Children's Online Privacy Protection Act [Note F]	Generally prohibits the online collection of personal information from children under 13 without verifiable parental consent.
Electronic Communications Privacy Act [Note G]	Prohibits the interception and disclosure of electronic communications by third parties unless a specified exception applies.
Computer Fraud and Abuse Act [Note H]	Prohibits obtaining information from a protected computer through the intentional access of a computer without authorization or exceeding authorized access.

Source: GAO review of federal laws. | GAO-15-621

Note A: Pub. L. No. 103-322, Tit. XXX, 108 Stat. 2099 (1994) (codified as amended at 18 U.S.C. §§ 2721-2725).

Note B: Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

Note C: Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

Note D: Pub. L. No. 91-508, Tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

Note E: Pub. L. No. 93-380, Tit. V, § 513, 88 Stat. 57 (1974) (codified as amended at 20 U.S.C. § 1232g).

Note F: Pub. L. No. 105-277, Div. C, Tit. XIII, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501-6506).

Note G: Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

Note H: Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030).

Unfair or Deceptive Acts or Practices

Section 5 of the Federal Trade Commission Act (FTC Act) authorizes FTC to take action against unfair or deceptive acts or practices in or affecting commerce.[53] Although the act does not explicitly grant FTC the authority to protect privacy, FTC has interpreted it to apply to deceptions or violations of written privacy policies.[54] For example, if a retailer has a written privacy policy stating it does not use facial recognition technology to identify customers and later breaches the policy by doing so, FTC staff have stated the agency could prosecute the retailer if it determined such violation constituted a deceptive practice. Likewise, FTC staff told us that the act could apply if firms violate written privacy policies on how they use or share personal information that was collected in conjunction with facial recognition technology. In addition, according to FTC staff, the FTC Act's "unfairness" authority could apply even in the absence of a privacy policy, in situations where an act or practice causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[55] FTC staff told us that as of June 2015, the agency had not taken any enforcement actions on privacy issues specifically with regard to the use of facial recognition technology or other biometrics. However, more generally, the agency had brought more than 40 cases related to privacy, and more than 50 cases related to data security, against companies that had engaged in unfair or deceptive practices.

[53]38 Stat. 717, § 5 (1914) (codified as amended at 15 U.S.C. § 45). The FTC Act further provides that an act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). The act does not provide a standard of what constitutes a "deceptive" act or practice, but FTC has issued guidance stating that it will find deception where there is "a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." *See* FTC Policy Statement on Deception, October 14, 1983.

[54]According to FTC staff, federal law does not require all firms to post a privacy policy. Several laws require covered entities to provide certain types of privacy policies or notices. For example, the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act require covered entities to provide a privacy policy. *See* 15 U.S.C. §§ 6502(b)(A), 6803; 16 C.F.R. § 312.3(a). Rules implementing the Health Insurance Portability and Accountability Act require covered entities to provide notice of how protected health information they collect is used and shared. *See* 45 C.F.R. § 164.520(a)(1).

[55]*See* 15 U.S.C. § 45(n).

Selected State Laws

Two states—Texas[56] and Illinois[57]—have adopted privacy laws that expressly address commercial uses of biometric identifiers, including scans of face geometry such as those gathered through facial recognition technology.[58] A report by a committee of the Texas House of Representatives noted that there were concerns that biometric data were increasingly becoming a target of identity theft and needed to be safeguarded.[59] Similarly, the Illinois General Assembly noted that use of biometrics was growing in the business and security screening sectors and that the ramifications of this technology were not fully known.[60] Both the Texas and Illinois laws

- require that before collecting a biometric identifier of an individual, a private entity must obtain that individual's consent;
- prohibit an entity in possession of a biometric identifier from sharing that person's biometric identifier with a third party, unless the disclosure meets an exception, such as for law enforcement or to complete a financial transaction that the individual requested or authorized; and
- govern the retention of biometric records, including requirements for protecting biometric information and destroying such information after a certain period of time.

In addition, according the National Conference of State Legislatures, most states have general privacy laws applicable to personal data, which may also potentially apply to information collected with, or otherwise connected to, facial recognition technology. As of January 2015, according to the organization, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands had enacted legislation requiring companies to notify residents if their personal information in the

[56]TEX. BUS. & COM. CODE ANN. § 503.001.

[57]740 ILL. COMP. STAT. 14/1-99.

[58]We did not conduct a comprehensive review of all state privacy laws. We selected the Illinois and Texas laws because they had been identified as expressly addressing privacy issues raised by biometric technologies.

[59]McCall, B. (2009). Bill Analysis. Business & Industry Committee Report. 81R 32595, accessed May 12, 2015, http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=81R&Bill=HB3186.

[60]*See* 740 Ill. Comp. Stat. 14/5.

companies' custody was compromised.[61] Further, at least 32 states and Puerto Rico have enacted laws that require entities to destroy, dispose of, or otherwise make personal information unreadable or undecipherable after it is no longer being used or after a specified amount of time, according to the National Conference of State Legislatures.[62]

Federal Laws Do Not Fully Address Stakeholder Privacy Concerns about Facial Recognition Technology, but Views Differ on the Need for Additional Legislation

Federal laws do not fully address the privacy issues that stakeholders have identified with commercial uses of facial recognition technology. As previously discussed, no federal law expressly regulates commercial use of facial recognition technology. This means that federal law does not expressly regulate the circumstances under which facial recognition technology may be used by commercial entities to identify and track someone with whom they have no prior relationship. Further, federal law does not expressly regulate whether and when firms should notify consumers of their use of facial recognition technology, or seek an individual's consent prior to identifying them, which has been an area of concern to privacy advocacy organizations and others.

Certain federal laws do address the collection, use, and sale of personal information by private-sector companies, as discussed earlier. These laws could potentially restrict, in certain circumstances, the collection of facial images, which are used to build a database for use with facial recognition technology. For example, provisions in the Driver's Privacy Protection Act restrict state motor vehicle bureaus from selling drivers' license photographs and associated information to private parties. In addition, the Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability Act potentially could restrict the ability of banks and health care providers to share data collected with facial recognition technology if those data were to fall within the laws' definitions of protected information. However, the reach of these laws is limited because they generally apply only for specific purposes, in certain situations, to certain sectors, or to certain types of entities. As a result, they do not comprehensively address how commercial entities other than

[61]See National Conference of State Legislatures, Security Breach Notification Laws, accessed May 12, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[62]See National Conference of State Legislatures, Data Disposal Laws, accessed May 12, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

those explicitly covered by the specific laws may collect, use, or share personal data in conjunction with facial recognition technology.

Additionally, depending on the context, federal law does not require firms that collect personal information to follow detailed standards for verifying the accuracy of data developed through computer matching.[63] As noted earlier, facial recognition algorithms may misidentify individuals and may not be as accurate as other forms of biometric identifiers because of technological challenges in accurately matching photographs and because users typically can adjust settings for the degree of accuracy required for a match. In a 2012 report, FTC stated that measures to ensure the accuracy of the consumer data that companies collect and maintain should be scaled to the intended use and sensitivity of the information.[64] One privacy expert we met with stated that in some commercial contexts facial recognition technology is used to identify criminals, such as shoplifters. As such, misidentifying an innocent individual could be detrimental. In most contexts, federal law may not provide consumers with the right to correct or delete inaccurate personal information collected by commercial firms.[65]

Some privacy advocacy organizations have argued for new legislation or regulation to address privacy issues associated with facial recognition technology. The American Civil Liberties Union has contended that government intervention and statutorily created legal protections are

[63]In contrast, the federal government must comply with certain requirements for information used in computer matching, which is governed by the Computer Matching and Privacy Protection Act of 1988. Pub. L. No. 100-503, 102 Stat. 2507 (1988) (codified as amended at 5 U.S.C. § 552a). Federal agencies are generally prohibited from taking adverse action, such as denying a benefit, unless they have taken one of several steps, such as independently verifying the information. 5 U.S.C. § 552a(p). The House Report on the Computer Matching and Privacy Protection Act stated that the purpose of the independent verification requirement was to provide assurance that the rights of individuals are not determined automatically by computers without human involvement and without checking that the information relied upon is accurate, complete, and timely. H.R. REP. NO. 100-802, at 34 (1988), *reprinted in* 1988 U.S.C.C.A.N. 3107, 3140.

[64]Federal Trade Commission (2012), *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington D.C.: March 2012).

[65]For information covered under Fair Credit Reporting Act, consumers have the right to dispute incomplete or inaccurate information held by firms, to have a claim investigated, and to have any errors deleted or corrected. 15 U.S.C. § 1681*i*.

needed to protect against the negative effects of this technology.[66] In testimony before the Senate in 2012, the Electronic Frontier Foundation stated that because of the risk that faceprints will be collected without individuals' knowledge, rules should define clear notice requirements to alert people that a faceprint has been collected and include information on how to request that data collected on them be removed.[67] One academic has argued specifically for legislation that would require individuals' explicit consent before a company could capture or use their faceprint, and would require companies to provide individuals with information about the uses of their biometric data.[68] The Center for Digital Democracy has urged FTC to recommend new safeguards for adolescents relating to facial recognition.[69] The Center for Democracy & Technology has stated that the technology poses complex privacy issues that do not fit squarely with present laws because these laws apply only indirectly to facial recognition and offer consumers no real choices with regard to the technology.

Views vary on the approach that additional privacy legislation or regulation, if any, should take to address these issues. The Center for Democracy & Technology argues that current federal privacy law is a confusing patchwork targeting discrete economic sectors with different rules. Therefore, it contends that Congress should not pass privacy legislation for facial recognition technology alone, but rather as a comprehensive framework that protects all personal information. One industry representative told us he believed that federal privacy legislation could benefit firms by clearly defining acceptable practices, but that any

[66]American Civil Liberties Union, *An Ethical Framework for Facial Recognition*, accessed May 13, 2015, http://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf.

[67]*What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. 24 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation). The Electronic Frontier Foundation is an advocacy organization that focuses on issues related to privacy, free speech online, surveillance, and technology.

[68]Y. Welinder, "A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks," *Harvard Journal of Law & Technology,* vol. 26, no. 1 (2012).

[69]Center for Digital Democracy (2012). Comments Submitted to Face Facts: A Forum on Facial Recognition Technology—Project No. P115406, accessed June 4, 2015, https://www.ftc.gov/policy/public-comments/comment-00076-3.

legislation should focus comprehensively on personal data rather than a specific technology. In February 2015, the White House proposed draft legislation to establish baseline protections for individual privacy in the commercial arena.[70] However, one academic privacy expert told us he believed that legal protections specific to facial recognition technology are needed because, as a practical matter, comprehensive privacy legislation is unlikely to be enacted in the foreseeable future. In comments submitted to FTC, several industry groups noted that facial recognition technology should not be regulated in a "one size fits all" manner. One company also noted that the privacy issues that arise from using facial recognition to surreptitiously identify a person in public are very different from the issues involved in using the technology to organize personal photographs, and that privacy regulations should be designed with respect to these different uses.[71]

However, most industry representatives have argued that new legislation or regulation is not necessary to address privacy issues associated with facial recognition technology, contending that self-regulation—such as voluntary codes of conduct and best practices—and privacy by design are effective alternatives. Industry trade organizations have urged caution in expanding privacy law in general, arguing that absent any identifiable harm in the marketplace, privacy issues are best addressed through industry self-regulatory programs and best practices.[72] In a 2012 Senate Committee hearing, a representative of the Digital Advertising Alliance said that industry self-regulation is flexible and could adapt to rapid changes in technology and consumer expectations, whereas legislation and government regulation could be inflexible and quickly become

[70]The White House, *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015* (Feb. 27, 2015), accessed May 27, 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[71]Facebook, *Comments Submitted to Face Facts: A Forum on Facial Recognition Technology—Project No. P115406* (Jan. 31, 2012), accessed May 13, 2015, https://www.ftc.gov/policy/public-comments/comment-00081-2.

[72]For example, see U.S. Chamber of Commerce, *Multi-industry Letter on Changes to Privacy Law* (June 29, 2011), accessed May 13, 2015, https://www.uschamber.com/letter/multi-industry-letter-changes-privacy-law.

outdated in an era of rapidly evolving technologies.[73] Specifically with regard to facial recognition technology, the industry association TechAmerica has contended that self-regulation based on the Fair Information Practice Principles, coupled with privacy by design, has provided consumers with the necessary privacy protections.[74] The National Retail Federation and others have argued that it may be too early to consider additional regulation of facial recognition technology because the technology is still in the early stages of development and thus the privacy issues raised are mostly speculative.[75] The group argued that such regulation could inhibit innovation and deny businesses and consumers beneficial products, while protecting against harms that might never have occurred.

In contrast, some consumer and privacy advocacy organizations have argued that self-regulation is not sufficient to fully address privacy concerns because it may be limited in scope, limited in coverage to those entities that choose to participate, and subject to change. For example, a study of industry privacy self-regulatory programs from 1997 through 2007 by the World Privacy Forum argued that these programs often lacked a meaningful ability to enforce their own rules or maintain memberships, and covered only a fraction of an industry or an industry subgroup.[76] The Center for Digital Democracy questioned the effectiveness of the NTIA's multistakeholder process for developing voluntary industry standards, contending that a previous process covering mobile applications did not lead to any significant changes in that industry's privacy practices. One former industry representative told us

[73] *The Need for Privacy Protections: Is Industry Self-Regulation Adequate?: Hearing Before the S. Comm. On Commerce, Science, and Transportation*, 112th Cong. 2 (2012) (statement of Robert Liodice, President and Chief Executive Officer, Association of National Advertisers, Inc. on behalf of the Digital Advertising Alliance). The Digital Advertising Alliance is an industry trade organization that establishes and enforces privacy practices across the online advertising industry.

[74] TechAmerica, *Comments Submitted to Face Facts: A Forum on Facial Recognition Technology—Project No. P115406* (Jan. 31, 2012), accessed May 13, 2015, https://www.ftc.gov/policy/public-comments/comment-00079-2.

[75] National Retail Federation, *Comments Submitted to Face Facts: A Forum on Facial Recognition Technology—Project No. P115406* (Jan. 31, 2012), accessed June 4, 2015 at https://www.ftc.gov/policy/public-comments/comment-00069-4.

[76] R. Gellman and P. Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States* (World Privacy Forum, 2011), 4-8.

that firms using facial recognition technology would not abide by voluntary codes of conduct if those codes damaged their commercial interests. In contrast, he believes that privacy legislation can provide firms with a financial incentive to abide by privacy principles because of the reputation risk caused by a public violation of privacy law. The White House framework for consumer data privacy, while supporting industry-wide codes of conduct, also suggested that Congress enact legislation to provide FTC with the ability to enforce the Consumer Privacy Bill of Rights independently. Similarly, in its 2012 report on protecting consumer privacy, FTC noted that while it has supported self-regulatory efforts, privacy self-regulation had not gone far enough and that Congress should consider enacting baseline privacy legislation.[77]

In our September 2013 report on personal information collected for marketing purposes, we suggested that Congress consider strengthening the consumer privacy framework to reflect the effects of changes in technology and the marketplace, a suggestion that is underscored by the privacy issues associated with facial recognition technology.[78] We identified how advances in technology and marketplace practices had resulted in vast changes in the amount and type of personal information collected. We also found that gaps existed in federal privacy law because it had not adapted to new technologies. As of July 2015, Congress has not passed legislation addressing our 2013 suggestion.

Concluding Observations

Facial recognition technology may be employed in a wide range of useful commercial applications, but the future trajectory of the technology raises questions about consumer privacy. Federal law does not expressly address the circumstances under which commercial entities can use facial recognition technology to identify or track individuals, or when consumer knowledge or consent should be required for the technology's use. Further, in most contexts federal law does not address how personal data derived from the technology may be used or shared. NTIA's multistakeholder process to develop a voluntary code of conduct is a positive step toward incorporating privacy considerations into the development and use of facial recognition technology. However, views

[77]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington D.C.: March 2012).

[78]GAO-13-663.

vary on the efficacy of voluntary and self-regulatory approaches versus legislation and regulation to protect privacy. The privacy issues stakeholders have raised about facial recognition technology and other biometric technologies serve as yet another example of the need to adapt federal privacy law to reflect new technologies. As such, we reiterate our 2013 suggestion that Congress strengthen the current consumer privacy framework to reflect the effects of changes in technology and the marketplace.

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. We also provided relevant excerpts of the draft for technical review to selected private parties cited in our report, and included their technical comments as appropriate.

We are sending copies of this report to Commerce, FTC, appropriate congressional committees and members, and other interested parties. The report also is available at no charge on the GAO website at http://www.gao.gov.

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 III.

Sincerely yours,

Alicia Puente Cackley
Director
Financial Markets and
Community Investment

Appendix I: Objectives, Scope, and Methodology

This report examines (1) the uses of facial recognition technology for consumers and businesses, (2) privacy issues that have been raised in connection with commercial uses of facial recognition technology, (3) proposed best privacy practices and industry privacy policies related to facial recognition technology, and (4) privacy protections under federal law that may potentially apply to facial recognition technology. The scope of this report includes use of the technology by companies and other private entities and does not include use by federal, state, or local government agencies. This report covers use of the technology in the United States and not in other countries. It focuses primarily on use of the technology to identify or verify an individual and not on facial detection (which simply detects when a face is present).

To address the first two objectives, we identified and reviewed relevant studies and reports, congressional testimony, position papers, and other documents from industry stakeholders, privacy and consumer advocacy organizations, federal agencies, and academic and industry experts. These included, among others, the Federal Trade Commission's (FTC) 2012 staff report on facial recognition technology;[1] transcripts and written comments stemming from FTC's 2011 facial recognition technology forum; agendas, meeting summaries, and documents submitted by participants from the Department of Commerce's (Commerce) National Telecommunications and Information Administration's (NTIA) multistakeholder process on facial recognition technology in 2014 and 2015; and testimony and written statements from a 2012 congressional hearing on facial recognition technology.[2] In addition, we reviewed product information and marketing material from selected companies that develop and sell products using facial recognition technology. We conducted a literature search to identify academic and trade articles on commercial applications of facial recognition technology, as well as privacy issues raised by the technology. We used these articles to corroborate information we obtained from industry stakeholders, privacy and consumer advocacy groups, and federal agencies. In conducting this search, we generally obtained information from various online research

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

[2]*What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012).

sources such as Proquest, Nexis, and Dialogue. We also used Internet search techniques and key word search terms to identify additional sources and types of available information about how facial recognition technology works, how it is used in commercial applications, and what privacy issues are raised by its use.

To address the third objective, we reviewed the Fair Information Practice Principles and White House Consumer Privacy Bill of Rights, as well as privacy guidelines and best practices with specific application to facial recognition and biometric technologies issued by the American Civil Liberties Union, Digital Signage Federation, FTC staff, and the International Biometrics & Information Association.[3] We also reviewed the privacy policies of selected companies in the social networking, retail, and casino industries, which we obtained from company websites. We chose those industries because they were widely cited among government and industry stakeholders as among the most significant users, or potential users, of facial recognition technology. Specifically, we reviewed the privacy policies of (1) two U.S. companies that currently use facial recognition technology and are ranked number one and number five, respectively, of the most popular social networking websites, based on estimated unique monthly visitors as of December 2014; (2) the five largest retail companies in the United States based on 2013 retail sales; and (3) the four largest U.S. casino companies, based on worldwide revenue in 2013.[4] We reviewed each privacy policy and relevant supporting documents for key words such as “facial recognition technology,” “photos,” “video,” and “surveillance cameras” to determine whether and how they addressed the use of facial recognition technology. While we identified whether and how the privacy policies addressed facial recognition technology specifically, we did not conduct a broad evaluation or assessment of these policies more generally because that was outside the scope of this engagement. We also met with representatives of two

[3]The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C.: Feb. 23, 2012). The framework presents a Consumer Privacy Bill of Rights, describes a stakeholder process to specify how the principles in that bill of rights would apply, and encourages Congress to provide FTC with enforcement authorities for the bill of rights.

[4]We did not review the privacy policies of six other top social networking companies because representatives of these firms told us that they do not currently use facial recognition technology.

companies that provide social networking applications to discuss, among other things, how facial recognition technology was addressed in their privacy policies. We also inquired with trade organization representatives about meeting with major retailers and casinos to discuss facial recognition technology, but the trade organizations told us that these companies declined to speak to us.

To examine privacy protections under federal law that may potentially apply to commercial uses of facial recognition technology, we reviewed and analyzed relevant federal laws and regulations to examine their potential applicability to the commercial use of facial recognition or other biometric technologies. We then reviewed laws, as well as relevant agency regulations, in terms of their general purpose and potential applicability to facial recognition or other biometric technologies. We also reviewed prior work we had conducted on federal privacy law as it relates to commercial entities.[5] We also reviewed state laws in Illinois and Texas that expressly addressed privacy issues related to commercial use of facial recognition technology or other biometric identifiers. We selected these laws for review because Illinois and Texas were the two states we identified as having such laws, based on our interviews and a review of relevant law review articles and information from the National Conference of State Legislatures. This review was intended to provide illustrative examples and was not exhaustive, and thus may not have identified all state laws that may exist addressing privacy and biometrics. In addition, we reviewed the previously mentioned congressional testimony, comments submitted to FTC's 2011 forum, and documents submitted to NTIA's multistakeholder process that addressed the applicability of federal law to facial recognition technology.

To address all four objectives, we conducted interviews with, and obtained documentation from, representatives of federal agencies, including FTC and Commerce's NTIA and National Institute of Standards and Technology; companies that use facial recognition technology; companies that develop facial recognition products; trade associations, including the American Bankers Association, American Gaming Association, Interactive Advertising Bureau, National Retail Federation, and Retail Industry Leaders Association; privacy or consumer advocacy

[5]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

organizations, including the American Civil Liberties Union, Center for Democracy & Technology, Electronic Frontier Foundation, Electronic Privacy Information Center, and World Privacy Forum; and two academics who have participated in the FTC FaceFacts Forum or NTIA multistakeholder process and who have studied these issues. We also interviewed the International Biometrics & Information Association and conducted a group interview with seven of its member companies that it had invited to participate.

We conducted this performance audit from July 2014 to July 2015 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.

Appendix II: Federal Laws Specifically Addressing the Collection, Use, and Storage of Personal Information

This appendix describes the federal laws that specifically address the collection, use, and storage of personal information by private entities, and these laws' potential applicability to commercial uses of facial recognition technology.

Driver's Privacy Protection Act.[1] Enacted in 1994, the Driver's Privacy Protection Act generally prohibits the use and disclosure of certain personal information contained in state motor vehicle records for commercial purposes, with some exceptions. The act's definition of personal information includes the driver's license photograph, as well as any other information that identifies an individual, including Social Security number, driver identification number, name, address (except 5-digit zip code), telephone number, and medical or disability information.

Gramm-Leach-Bliley Act (GLBA).[2] Enacted in 1999, the Gramm-Leach-Bliley Act contains provisions that restrict, with some exceptions, the disclosure of nonpublic information by entities that fall under GLBA's definition of a "financial institution" or that receive nonpublic personal information from such a financial institution.[3] GLBA generally requires financial institutions to provide notice and an opportunity for consumers to opt out before sharing their nonpublic information with nonaffiliated third parties, other than for certain purposes such as processing a financial service authorized by the consumer. Regulations implementing GLBA do not specifically cite facial images or biometric identifiers—which are used by some financial institutions to verify customers—in the definition of nonpublic personal information.[4] However, the definition does include personally identifiable financial information, which is defined to include any information that financial institutions obtain about a consumer in connection with providing a financial product or service to that consumer,

[1]Pub. L. No. 103-322, Tit. XXX, 108 Stat. 2099 (1994) (codified as amended at 18 U.S.C. §§ 2721-2725).

[2]Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

[3]15 U.S.C. § 6802. GLBA defines a "financial institution" as any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)). 15 U.S.C. § 6809(3)(a). Such activities include lending, providing financial or investment advice, and insuring against loss.

[4]*See* 12 C.F.R. § 1016.3(p).

such as the fact that an individual is a consumer or customer of a particular financial institution.

Health Insurance Portability and Accountability Act.[5] Enacted in 1996, the Health Insurance Portability and Accountability Act establishes a set of national standards for the protection and safeguarding of individually identifiable health information. With some exceptions, rules implementing the act require an individual's written authorization before a covered entity—a health care provider that transmits health information electronically in connection with covered transactions, health care clearinghouse, or health plan—may use or disclose that individual's individually identifiable health information, including for commercial purposes.[6] The rules also give individuals the right to have a covered entity amend their protected health information if it is not accurate and complete.[7] Additionally, the rules include full-face images and biometric identifiers among the personal identifiers that must be removed before protected health information is no longer considered individually identifiable health information and therefore generally can be disclosed.[8]

Fair Credit Reporting Act.[9] The act, which was enacted in 1970, protects the security and confidentiality of personal information collected or used for eligibility determinations for such products as credit, insurance, or employment. The Fair Credit Reporting Act applies to those meeting the definition of "consumer reporting agency" under the act, which includes the three nationwide consumer reporting agencies (commonly called credit bureaus) and other businesses that collect or

[5]Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[6]45 C.F.R. § 164.508(a)(3).

[7]45 C.F.R. § 164.526(a).

[8]45 C.F.R. §§ 164.502(d)(2), 164.514(a), (b)(2)(i)(P)-(Q).

[9]Pub. L. No. 91-508, Tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

disclose information for consumer reports for use by others.[10] The act limits the use and distribution of personal data collected for consumer reports to permissible purposes specified in the act and also gives consumers certain rights to opt out of allowing their personal information to be shared for certain marketing purposes. The act also allows individuals to access and dispute the accuracy of personal data held on them and imposes safeguarding requirements for such data.

Children's Online Privacy Protection Act.[11] Enacted in 1998, the Children's Online Privacy Protection Act requires covered website and online service operators to obtain verifiable parental consent before collecting personal information from children under 13, with certain exceptions. Regulations implementing the act define "personal information" to include a photograph or video containing a child's image, as well as other information such as full name and e-mail address.[12] In its 2013 final rule amending its regulations implementing the act, FTC expressly addressed facial recognition technology in the discussion of its decision to incorporate photographs of a child under 13 into the definition of "personal information," noting the inherently personal nature of photographs and the possibility of them being paired with facial recognition technology.[13]

[10]The Fair Credit Reporting Act defines a consumer reporting agency as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f). The act defines a consumer report as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [of the act]," subject to certain exclusions. 15 U.S.C. § 1681a(d).

[11]Pub. L. No. 105-277, Div. C, Tit. XIII, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501-6506).

[12]*See* 16 C.F.R. § 312.2.

[13]78 Fed. Reg. 3972, 3981 (Jan. 17, 2013).

Electronic Communications Privacy Act.[14] Enacted in 1986, this act prohibits the interception and disclosure of electronic communications by third parties unless an exception applies, such as one of the parties to the communication having consented to the interception or disclosure. For example, unless an exception applies, such as customers having given their consent, the act would prohibit an Internet service provider from selling the content of its customers' e-mails and text messages—which could include facial images—to a third party.

Family Educational Rights and Privacy Act.[15] Enacted in 1974, the act generally prohibits federal funds from being made available to any school or institution that has a policy of releasing students' education records or personally identifiable information contained in such records without the prior written consent of the parent or eligible student, with certain exceptions. The Department of Education's regulations implementing the Family Educational Rights and Privacy Act include biometric records—including facial characteristics—in the definition of personally identifiable information.[16]

Computer Fraud and Abuse Act.[17] Enacted in 1986, the Computer Fraud and Abuse Act prohibits obtaining information from a protected computer through the intentional access of a computer without authorization or through exceeding authorized access.[18] Some courts have held that using a website for a purpose in violation of the site's terms of use or terms of service exceeds authorized access and therefore violates the act.[19] Other courts, however, have read the act more

[14]Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

[15]Pub. L. No. 93-380, Tit. V, § 513, 88 Stat. 57 (1974) (codified as amended at 20 U.S.C. § 1232g).

[16]34 C.F.R. § 99.3.

[17]Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030).

[18]Specifically, the Computer Fraud and Abuse Act states that "Whoever… intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains… information from any protected computer… shall be punished as provided [in this section of the Act]." 18 U.S.C. § 1030(a)(2)(C).

[19]*See, e.g.*, *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003); *Southwest Airlines Co. v. Farcase, Inc.*, 318 F.Supp.2d 435, 439-440 (N.D. Tex. 2004); *Am. Online, Inc. v. LCGM, Inc.*, 46 F.Supp.2d 444, 450 (E.D. Va. 1998).

narrowly, holding that it prohibits the unauthorized procurement of information rather than its misuse.[20] To the extent that the collection of images online related to facial recognition technology is found to constitute obtaining information from a protected computer through access without authorization or exceeding authorized access, such collection may be a violation of the Computer Fraud and Abuse Act.

[20]*See, e.g.*, *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2011); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009); *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D. Ariz. 2008).

Appendix III: 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, Jason Bromberg (Assistant Director), José R. Peña (Analyst-in-Charge), William R. Chatlos, Jeremy Conley, Richard Hung, Patricia Moye, and Jennifer Schwartz made key contributions to this report.

Appendix IV: Accessible Data

Accessible Text

Accessible Text for Figure 1: How Facial Recognition Technology Systems Generally Work

1. **Facial detection:**
   The system extracts patterns in an image and compares them to, or tests them against, a model of a face. When these patterns are determined to closely resemble the face model, the assumption is that a face is present in the image.

2. **Creation of faceprint:**
   A facial recognition algorithm then registers the face and it places it in a preset position, using either (1) a geometric approach, which calculates the location of and spatial relationship between certain facial features, such as the center of the eyes, the tip of the nose, and the corners of the mouth; (2) a photometric approach, which interprets a face as a weighted combination of standardized faces; or (3) skin texture analysis, which maps the unique placement of pores, lines, and spots on an individual's skin. These techniques may be used separately or they may be used in combination with each other to increase accuracy.
   The system then will seek to standardize the image so that it is in the same format as the images in the database. After this process, the system extracts features from the face and puts them into a format—often referred to as a faceprint—that can be used for classification, verification, or identification. Some facial recognition systems store the image and faceprints for later use, a process known as enrollment, while other systems may discard them.

   a. **Facial classification:**
      Once the faceprint has been created, the system can use algorithms to classify the face into any number of categories, including estimating the gender or age of the face.

   b. **Verification:**
      The system can use the facial recognition algorithm to compare two faceprints against each other to produce a single score value that represents the degree of similarity between the two faces. Verification systems compare a person's facial image to a stored faceprint for that person.

   c. **Identification:**
      Identification systems compare a person's facial image to a database of multiple stored faceprints.

Source: GAO. GAO-15-621