ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Daniel Castro

Vice President

Information Technology and Innovation Foundation

Before the

House Committee on Oversight and Reform

Hearing on

"Facial Recognition Technology (Part III):

Ensuring Commercial Transparency & Accuracy"

January 15, 2020

2154 Rayburn House Office Building

Washington, DC

Chairwoman Maloney, Ranking Member Jordan, and members of the committee, thank you for the opportunity to appear before you to discuss the use of facial recognition technology by the private sector and the opportunities for better oversight of this technology.

I am the vice president of the Information Technology and Innovation Foundation (ITIF). ITIF is a non-profit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity. I am also the director of the Center for Data Innovation, an ITIF-affiliated research institute focusing on the intersection of data, technology, and public policy.

In my testimony today, I would like to give an overview of facial recognition technology, discuss some of its potential commercial uses, the level of public support for the technology, and steps Congress can take to improve oversight and accountability.

## OVERVIEW OF FACIAL RECOGNITION TECHNOLOGY

There are a variety of technologies that process images of faces, including facial detection, facial analysis, and facial recognition.

Facial detection refers to technology that detects the presence and location of a face in an image. For example, many cameras use facial detection to locate faces in a scene and then automatically adjust the focus, exposure, and flash to optimize the photograph. Search engines may use facial detection to return photos with images of a face, and video software may use face detection to keep a face in frame.

Facial analysis describes technology that identifies specific characteristics about faces in images. For example, some facial analysis software estimates an individual's age, gender, or emotional state based on an image of their face, or answers questions such as whether a face has a beard, hat, or glasses. Retailers, for example, may use facial analysis to create metrics about the demographics of their customers. Researchers have also begun to experiment with integrating facial analysis into wearable technology to help children with autism understand the emotions of others.[1] Some health care providers also use facial analysis software to screen for certain congenital and neurodevelopmental disorders.[2]

Facial recognition refers to technology that compares faces automatically, either by searching for similar faces in a database (one-to-many matching) or by verifying the degree to which two faces match (one-to-one matching). In the former case, facial recognition tries to answer the question "who is this person?" and in the latter, it tries to answer the question "is this person who they say they are?" Facial recognition works by creating a mathematical representation of an image of a face based on its unique characteristics and by comparing that representation to others.

There are different types of facial recognition technology. One of the most common types of facial recognition uses two-dimensional images created by standard cameras. For example, in Google Photos, users can group together photos that contain the same faces.[3] Another type of facial recognition uses infrared or near-infrared technology to create a three-dimensional map of an individual's face. Smartphone companies such as Apple, Huawei, and Oppo use infrared technology to allow individuals to unlock their phones using their face. For example, Apple's iPhone X contains a flood illuminator that shines infrared light to detect a user and an infrared dot projector to create a dot pattern on the user's face that the phone's built-in infrared camera uses to map the user's face.[4] The benefit of infrared technologies is that they work even in low-light conditions.

Many facial recognition systems, especially those used for security purposes, also use methods to distinguish between a live image of a face and a photo of a face to prevent imposters from misusing someone's identity. While attackers have defeated some of these methods, researchers continue to improve on these techniques.

While facial detection, facial analysis, and facial recognition may sometimes be used together, they are each designed for different purposes. Moreover, characteristics about one technology do not necessarily apply to another. For example, the accuracy rates of facial analysis algorithms are different than those for facial recognition, and the privacy implications of facial detection are different than those of facial recognition. Unfortunately, some news articles conflate these technologies, which may create misperceptions about the risks associated with these technologies.[5]

## HOW THE PRIVATE SECTOR USES FACIAL RECOGNITION TECHNOLOGY

There are many existing and emerging uses of facial recognition technology in the private sector.

Social networks are using facial recognition to increase convenience, security, and accessibility for users. For example, users who enable facial recognition on Facebook can have the social network automatically identify them in photos uploaded by their friends and alert them if someone creates a fake profile using their face. Facebook also uses facial recognition to make its platform more accessible by automatically adding descriptive text to photos to explain who is in a photo.[6] Users who are blind or have low vision can use screen readers that read aloud this text so they can better understand the photos from their friends and family.[7]

Airlines are using facial recognition to allow travelers to get through the airports faster and more easily. For example, travelers at the international terminal in the Atlanta airport can use facial recognition to check in at self-service kiosks, drop their checked baggage, identify themselves at the TSA checkpoint, and board their flights.[8] And JetBlue has partnered with U.S. Customs and Border Protection to launch a biometric self-boarding gate for international flights that verifies passengers' identities using facial recognition.[9] In a test at the Los Angeles international airport, facial

recognition expedited processing so that 350 passengers could board a plane in less than 20 minutes—half the time it usually takes.[10]

Financial institutions are using facial recognition to improve security. Credit card companies like Visa and Mastercard have launched services that allow customers to verify the authenticity of online purchases by taking selfies.[11] In addition, some banks are using facial recognition to verify their customers' identity—online, in-person at a physical branch, and at ATMs.[12] Banks can also use the technology to improve on-premise security, such as by ensuring that only authorized staff have access to restricted areas like bank vaults.

The hospitality industry is exploring how to use facial recognition to provide guests a more personalized experience. For example, the restaurant chain CaliBurger (also known for hiring Flippy, the hamburger-flipping robot, in 2018) has built a self-service kiosk with technology company NEC that uses facial recognition to identify customers who have registered for its loyalty program and automatically pulls up their favorite orders.[13] Cruise ships, amusement parks, stadiums, and other venues are also considering how to use facial recognition as a substitution for traditional ticketing, allowing guests to come and go more easily and create VIP experiences. For example, one hotel uses facial recognition so that guests can avoid check-in: instead they go straight to an elevator that recognizes them and takes them to the correct floor; they can then unlock their hotel room door via facial recognition.[14] Casinos can also use facial recognition technology to prevent gambling addicts from placing bets.[15]

Retailers similarly are using facial recognition to enable customers to make purchases with just their face, speeding up the checkout process.[16] Retailers also use facial recognition to identify known shoplifters, with some stores reporting the technology has reduced theft by 30 percent.[17]

In addition to mobile devices, companies are integrating facial recognition into many other products. The X One electric bike allows the owner to unlock it using facial recognition.[18] This feature may soon come to cars too. BMW recently unveiled its Vision M Next concept car that the driver can unlock using facial recognition.[19] And the Chinese electric vehicle startup Byton has already debuted an SUV equipped with facial recognition technology that not only unlocks the door when it recognizes its driver, but also automatically adjusts the seats, mirrors, and climate control to the driver's personal preferences.[20] Many companies also sell home security cameras with facial recognition capabilities. Residents can use these cameras to identify who is at their door and alert them of someone who should not be at their home. These systems can provide necessary evidence to police to investigate low-dollar crimes, such as car break-ins and package thefts from doorsteps, which often go unaddressed.

Facial recognition can help protect children. If a facial recognition system identifies a potentially dangerous individual at a school or childcare facility—such as a suspended student, a sex offender, or

a drug dealer—security personnel can respond accordingly.[21] In addition, online casinos are using facial recognition to verify their players' identity, keeping out underage users.[22] Finally, companies are developing biometric storage safes so that cannabis users and gun owners can store their property securely, keeping dangerous items safely out of the hands of children who might otherwise find a hidden key or learn a combination.[23]

Health care facilities are also exploring the use of facial recognition. For example, the Parker Adventist Hospital in Colorado has begun using facial recognition technology to confirm the identities of cancer patients to ensure the right patient receives the right treatment.[24] The goal of this initiative is to prevent patient misidentification, which can result in serious medical errors.

Finally, facial recognition can help people with prosopagnosia, or "face blindness," to remember faces. For example, one mobile app allows users to upload photos of people they know and link these to their personal notes about them, which the app can then automatically display when the user encounters that individual in the future.[25]

## THE PUBLIC GENERALLY SUPPORTS FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology has become very common—as of 2020, there are likely more than one billion smartphones with some form of facial recognition.[26] Indeed, most Americans (86 percent) have heard about facial recognition, according to a 2019 Pew Research Center survey.[27]

Although a handful of cities such as San Francisco, California, Oakland, California, and Somerville, Massachusetts have recently made headlines by passing a ban on government use of facial recognition technology, the public generally opposes such extreme measures.

In a poll from December 2018, ITIF's Center for Data Innovation found that only one in four Americans (26 percent) think government should strictly limit the use of facial recognition technology—and that support drops even further if it would come at the expense of public safety.[28] Fewer than one in five Americans (18 percent) would agree with strictly limiting the technology if it came at the expense of public safety, while a solid majority (55 percent) would disagree.

Similarly, only 20 percent of Americans say government should strictly limit use of facial recognition if it would mean airports cannot use the technology to speed up security lines, while a majority (54 percent) would disagree with such a limit. And just 24 percent want strict limits if it would prevent stores from using the technology to stop shoplifting, while 49 percent would oppose such a tradeoff.

The survey also asked respondents whether government should limit surveillance cameras, since they are integral to many applications of facial recognition technology. Overall, Americans were more likely to support limiting surveillance cameras (36 percent) than facial recognition technology (26

percent). If it would come at the expense of public safety, then just 18 percent of Americans would agree with limiting surveillance cameras and the same percentage would agree for facial recognition. These findings suggest that what little support there is for limiting facial recognition technology is related to existing support for limiting the use of surveillance cameras.

Other recent surveys have found similar results. For example, a poll conducted in August 2019 for NetChoice, a business trade association, found that the majority (64 percent) of Massachusetts residents believe facial recognition can make society safer.[29] And a May 2019 survey by Reservations.com found that 43 percent of Americans approve of facial recognition technology in airports, compared to only 33 percent who disapprove.[30]

Finally, a 2018 survey by the facial recognition company FaceFirst found that most Americans (56 percent) believe facial recognition should be used in retail environments to safeguard stores against serial shoplifters, thieves, and dangerous criminals.[31] This survey also found that a majority of Americans (56 percent) would use facial recognition to protect their homes if cost was not an issue.[32]

As with technologies that came before it, as the average American becomes more familiar with the benefits of facial recognition technology, their level of acceptance of the technology will likely grow.

## FACTS ABOUT RACE AND GENDER BIAS IN FACIAL RECOGNITION HAVE BEEN MISCONSTRUED

While multiple polls show that the public generally supports facial recognition technology when it increases safety and convenience, there have been alarming claims about potential racial or gender bias in the technology. Concerns about racial or gender bias should always be taken seriously. In this case, however, the headlines often do not accurately represent the facts.

First, there are many different facial recognition systems on the market, and the accuracy and error rates of these systems vary. Some systems perform much better than others, including in their accuracy rates across race, gender, and age.[33]

Second, the most accurate algorithms have little to no bias. The most recent report from the National Institute of Standards and Technology (NIST) on the accuracy rates of facial recognition technology across different demographic groups found that the most accurate one-to-one algorithms have error rates below 1 percent "for almost all countries and demographic groups."[34] Similarly, NIST found that for one-to-many algorithms "some developers supplied highly accurate identification algorithms for which false positive differentials are undetectable."[35]

Third, many of the claims that have been made in the past about racial bias, especially those citing a study from the MIT Media Lab, conflate facial analysis with facial recognition.[36] As described previously, these are different technologies, and the accuracy rates of one do not relate to the

accuracy rates of the other. Moreover, the accuracy rates of these technologies need to be evaluated in the context of specific applications. In some situations, accuracy is paramount; however, in others it may not be as important or there may be appropriate controls in place to mitigate errors.

Fourth, many of the critiques about racial bias in facial recognition algorithms refer to older technologies. Newer versions of these facial recognition systems perform more accurately, and the technology continues to improve over time.[37]

Fifth, the accuracy of facial recognition systems depends on a range of variables, including the quality of the images used and the confidence thresholds for determining matches. Some of the critiques have focused on facial recognition systems that use low thresholds, thereby artificially inflating error rates. For example, an oft-cited ACLU study used Amazon's facial recognition service to compare photos of members of Congress to a mug shot database and found multiple false positives. However, the ACLU used a lower confidence threshold than recommended.[38] The ACLU used a confidence threshold of 80 percent, which may be suitable for some uses, but Amazon recommends using a 99 percent threshold when higher levels of accuracy are necessary, such as in law enforcement. Indeed, Dr. Matt Wood, who oversees machine learning at Amazon Web Services, says that the ACLU's reported error rate would drop from 5 percent to zero at this higher confidence level.[39]

Finally, many critiques overlook the fact that humans are often more biased in recognizing faces than computers are, particularly when they are looking for people of different races than themselves, and facial recognition technology can mitigate some of these human biases.[40]

## PRIVATE SECTOR INITIATIVES TO ENSURE RESPONSIBLE DEVELOPMENT AND USE OF FACIAL RECOGNITION

The private sector has taken many steps to ensure the safe and responsible deployment of facial recognition technology.

First, some of the industries that have been early adopters of the technology have been at the forefront of voluntary self-regulation. For example, in 2011, the digital signage industry adopted a set of voluntary privacy and transparency guidelines for the use of facial recognition and facial analysis.[41] This standard offers detailed guidance for how to provide clear and meaningful notice to consumers and under which conditions consumers should be able to opt in or opt out of data collection. In addition, in February 2014, the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce launched a multi-stakeholder process on commercial use of facial recognition. In June 2016, a group of stakeholders reached a consensus on a set of best practices which offered guidelines for protecting consumer privacy.[42]

Second, many of the technology companies that make facial recognition technology have published their own principles for developing and using the technology. For example, Microsoft's president Brad Smith has outlined six principles—fairness, transparency, accountability, non-discrimination, notice and consent, and lawful surveillance—that will guide how Microsoft develops and deploys facial recognition technology.[43] Amazon likewise has developed guidance for its facial recognition customers, created an acceptable use policy, and published its own recommendations for federal legislation.[44] Indeed, many of the leading facial recognition technology vendors, including Google, RankOne, and Trueface, have released similar principles.[45] More recently, the U.S. Chamber of Commerce's Technology Engagement Center (C_TEC), whose members include facial recognition vendors, developers, users, and other stakeholders, drafted a set of policy principles for facial recognition that called for a single national regulatory framework that would promote beneficial uses of the technology while mitigating risks.[46]

## STEPS TO IMPROVE OVERSIGHT AND ACCOUNTABILITY

Recent calls for bans or moratoriums on facial recognition are misguided and, if implemented, would have negative economic and social consequences. As such, Congress should avoid any bans on facial recognition. Even narrow bans can have unintended consequences given the widespread integration of facial recognition technology into many products and services. For example, after San Francisco banned government use of facial recognition technology the city later realized it had unintentionally banned city employees from using their iPhones.[47] Similarly, a number of companies have blocked residents of Illinois from using their products and services because the state unintentionally banned them with the Illinois Biometric Information Privacy Act.[48]

Instead of bans or moratoriums, Congress should focus on steps to improve oversight and accountability of commercial use of facial recognition technology.

First, Congress should pass legislation to create a national privacy framework that streamlines regulation, preempts state laws, establishes basic consumer data rights, and minimizes the impact on innovation.[49] Federal data privacy legislation should address the collection and use of biometric data, such as specifying how to provide notice and choice to consumers, but it should be technology-neutral and not treat facial recognition differently than other biometrics. While it may be appropriate to require opt-in consent for certain sensitive uses, such as in health care or education, this should not be applied to all scenarios. Opt-in consent is not always feasible, such as when historians are using facial recognition to identify soldiers in Civil War-era photographs, when non-profit organizations are using facial recognition to find sex trafficking victims, or when individuals are using security cameras with facial recognition to alert them of stalkers, domestic abusers, or sex offenders.[50] In addition, a federal law should not establish a private right of action as this would significantly raise costs for businesses, which would eventually be passed on to consumers.[51] Indeed,

after the Illinois Supreme Court ruled that plaintiffs do not have to show harm to sue companies for violations of the state's biometric law, there has been a surge in class action lawsuits.[52]

Second, Congress should direct NIST to expand its evaluation of commercial facial recognition systems. In particular, NIST should include cloud-based facial recognition systems in its tests. Currently, all algorithms must be submitted as pre-compiled software libraries, which means many cloud providers do not participate in these evaluations. Expanding to include cloud-based providers would be useful as many commercial systems use these services. NIST should also expand its tests to reflect more real-world commercial uses. Independent public testing of these facial recognition systems will encourage more competition in the market and accelerate improvements in existing systems, since integrators will likely be able to switch easily to the best performing cloud-based providers. Finally, NIST should include race, gender, and age diversity metrics as part of its regular testing protocol in the future.

Third, Congress should direct NIST to develop a diverse set of training and evaluation data of facial images. By funding the creation of additional and more diverse training and evaluation datasets for facial recognition, Congress can spur developers to further reduce any differences in accuracy across different demographics and reduce concerns about bias.

Fourth, Congress should direct the General Services Administration to work with NIST to set performance standards for any facial recognition technology procured by the federal government, including for accuracy and error rates by age, race, and gender. Since the same technology is used by both the federal government and the private sector, by setting a performance standard for the federal government, Congress can promote better accuracy rates across all sectors of the economy. This will also ensure federal agencies do not waste tax dollars on ineffective systems or ones with significant performance disparities.

Fifth, Congress should fund federal agencies to deploy facial recognition systems where appropriate within government. By having government become an early adopter of the technology, the federal government can accelerate the rate of innovation of the technology. For example, federal buildings can use facial recognition to improve building security and expedite entry into building for federal government workers.

Sixth, Congress should continue to support federal funding for research to improve the accuracy of facial recognition technology as part of the government's overall commitment to investing in artificial intelligence (AI). One of the key areas of fundamental AI research is computer vision, and the U.S. government should continue to invest in this technology. China is investing heavily in AI, and it is beginning to outperform the United States in some metrics.[53] As NIST found, a number of algorithms developed in China outperform algorithms developed in the United States on East Asian faces.[54]

Seventh, Congress should consider legislation to uphold civil liberties, in particular to guard against the risk that law enforcement may request access to private-sector databases that contain detailed geolocation data about individuals derived from facial recognition systems. To address this risk, policymakers should establish a warrant requirement to track the movements of individuals by any means, including with facial recognition systems, mobile phones, GPS trackers, or license plate readers. By addressing this broader risk, Congress can mitigate many concerns about facial recognition that are not actually related to the use of this particular technology but about broader surveillance by the government. In addition, Congress should call for states to eliminate laws banning wearing masks in public. While the average person is not likely to wear a mask to avoid facial recognition, this should still not be illegal, yet it is in many states.[55] Instead, states should only make it illegal to wear masks in public to commit a crime.

Finally, Congress should continue to pursue broad oversight of appropriate law enforcement activity. For example, Congress should clarify the appropriateness of police surveillance of political protests, regardless of the type of technology used for surveillance. And it should continue to provide oversight of racial bias in law enforcement and the criminal justice systems, especially racial disparities in police use of force among communities of color. In addition, Congress should direct the Department of Justice and the Department of Homeland Security to develop best practices on government use of facial recognition technology, including operational guidance and oversight protocols. The National Institute of Justice should also create best practices for state and local law enforcement to improve their use of facial recognition technology. This guidance should include recommendations for how to publicly disclose when law enforcement uses the technology, the types of data sources used for images, and data retention policies.

## CONCLUSION

It is always important for Congress to consider the impact of new technologies and ensure there are proper guardrails in place to protect society's best interests. In the case of facial recognition technology, there are many clearly beneficial opportunities to use the technology. Congress should therefore pursue opportunities to establish policies that support positives uses of facial recognition technology, but limit potential misuse and abuse.

Thank you again for this opportunity to appear before you today.

## REFERENCES


[1] "Google Glass helps kids with autism read facial expressions," Stanford Medicine, August 2, 2018, https://med.stanford.edu/news/all-news/2018/08/google-glass-helps-kids-with-autism-read-facial-expressions.html.

[2] "AI face-scanning app spots signs of rare genetic disorders," *Nature*, January 7, 2019, https://www.nature.com/articles/d41586-019-00027-x.

[3] "Search by people, things & places in your photos," Google Photos Help, n.d., https://support.google.com/photos/answer/6128838 (accessed January 12, 2020).

[4] "Apple's Face ID [The iPhone X's facial recognition tech] explained," *ComputerWorld*, November 1, 2017, https://www.computerworld.com/article/3235140/apples-face-id-the-iphone-xs-facial-recognition-tech-explained.html.

[5] Daniel Castro, "Note to Press: Facial Analysis Is Not Facial Recognition," Information Technology and Innovation Foundation, January 27, 2019, https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition.

[6] "What is the face recognition setting on Facebook and how does it work?" Facebook, n.d., https://www.facebook.com/help/122175507864081 (accessed January 12, 2020).

[7] "Facebook's new facial recognition efforts help blind users know exactly who's in photos," *Mashable*, December 19, 2017, https://mashable.com/2017/12/19/facebook-facial-recognition-blind-users-photos/.

[8] "Delta unveils first biometric terminal in U.S. in Atlanta; next stop: Detroit," Delta, December 13, 2018, https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.

[9] Evie Carrick, "JetBlue is Expanding its Use of Facial Recognition Technology," *Travel and Leisure*, April 29, 2019, https://www.travelandleisure.com/airlines-airports/jetblue/jetblue-airline-facial-recognition-technology.

[10] "Facial-recognition scanners at airports raise privacy concerns," *Washington Post*, September 15, 2018, https://www.washingtonpost.com/local/trafficandcommuting,/facial-recognition-scanners-at-airports-raise-privacy-concerns/2018/09/15/a312f6d0-abce-11e8-a8d7-0f63ab8b1370_story.html.

[11] "Fighting fraud with a smile," Visa, n.d., https://usa.visa.com/visa-everywhere/security/fighting-fraud-with-a-smile.html (accessed January 12, 2020) and "Mastercard and BMO make Fingerprint and 'Selfie' Payment Technology a Reality in North America," Mastercard, October 24, 2016, https://newsroom.mastercard.com/press-releases/mastercard-and-bmo-make-fingerprint-and-selfie-payment-technology-a-reality-in-north-america/.

[12] Harmon Leon, "How AI and Facial Recognition are Impacting the Future of Banking," *Observer*, November 12, 2019, https://observer.com/2019/11/trueface-artificial-intelligence-facial-recognition-future-banking/.

[13] "CaliBurger's new kiosk uses facial recognition to take orders," Engadget, December 21, 2017, https://www.engadget.com/2017/12/21/caliburger-face-scan-ordering-kiosk/.

[14] "Facial recognition is coming to hotels to make check-in easier—and much creepier," *Fast Company*, April 1, 2019, https://www.fastcompany.com/90327875/facial-recognition-is-coming-to-hotels-to-make-check-in-easier-and-much-creepier.

[15] Casino.org Staff Writer, "Japanese Government Wants Facial Recognition Technology Used at Casinos, Racetracks," *Casino.org*, Marcy 7, 2019, https://www.casino.org/news/facial-recognition-technology-to-be-used-at-japanese-casinos/.

[16] "SnapPay Launches Facial Recognition Payment Technology in North America," *Business Wire*, October 16, 2019, https://www.businesswire.com/news/home/20191016005225/en/SnapPay-Launches-Facial-Recognition-Payment-Technology-North.

[17] Leticia Miranda, "Thousands of Stores will Soon Use Facial Recognition, and They Won't Need Your Consent," *BuzzFeed News*, August 17, 2018, https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at.

[18] "X One electric bike with facial recognition, in-built touchscreen computer available for pre-order," BiometricUpdate.com, November 17, 2019, https://www.biometricupdate.com/201911/x-one-electric-bike-with-facial-recognition-in-built-touchscreen-computer-available-for-pre-order.

[19] "BMW Vision M Next: An autonomous car for people who love driving," *Engadget*, June 25, 2019, https://www.engadget.com/2019/06/25/bmw-vision-m-next-autonomous-concept-unveil/.

[20] Jeff Plungis, "Car Companies Show Off Facial Recognition and High-Tech Cockpit Features," *Consumer Reports*, January 8, 2018, https://www.consumerreports.org/cars-driving/car-companies-show-off-face-recognition-and-high-tech-cockpit-features/.

[21] Lucas Ropek, "Facial Recognition Software on the Rise in U.S. Schools," *Government Technology*, October 17, 2019, https://www.govtech.com/products/Facial-Recognition-Software-on-the-Rise-in-US-Schools.html.

[22] Ed Silverstein, "New Konami Casino Facial Recognition Technology Could Rival Reward Cards," *Casino.org*, October 22, 2019, https://www.casino.org/news/new-konami-casino-facial-recognition-technology-could-rival-reward-cards/.

[23] "KEEP Smart Storage," CES 2020 Innovation Award Product, n.d., https://www.ces.tech/Innovation-Awards/Honorees/2020/Honorees/K/KEEP-Smart-Storage.aspx (accessed January 12, 2020) and "Biometric Gun Safe – Protecting Your Children From Your Own Guns," Biometric Security Devices, https://www.biometric-security-devices.com/biometric-gun-safe.html (accessed January 8, 2020).

[24] "Facial recognition technology used in cancer treatment at Parker Adventist Hospital," KDVR, June 26, 2019, https://kdvr.com/2019/06/26/facial-recognition-technology-used-in-cancer-treatment-at-parker-adventist-hospital/.

[25] "New App Helps People Remember Faces," *Scientific American*, January 1, 2019, https://www.scientificamerican.com/article/new-app-helps-people-remember-faces/.

[26] "More than one billion smartphones to feature facial recognition in 2020," Counterpoint, February 7, 2018, https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/.

[27] "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly," Pew Research Center, September 5, 2019, https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

[28] Daniel Castro and Michael McLaughlin, "Survey: Few Americans Want Government to Limit Use of Facial Recognition Technology, Particularly for Public Safety or Airport Screening," (Center for Data Innovation, January 7, 2019), https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/.

[29] "Massachusetts Polling Study," Savanta, August 2019, http://netchoice.org/wp-content/uploads/MA-Facial-Recognition-Polling.pdf.

[30] "Survey: 43% of Americans Approve, 33% Disapprove of Facial Recognition Technology in Airports," Runaway Suitcase, June 2019, https://www.reservations.com/blog/resources/facial-recognition-airports-survey/.

[31] Jesse Davis West, "New Survey Finds Americans Favor Face Recognition to Combat Rising Retail Theft and Violence," Face First, January 31, 2018, https://www.facefirst.com/blog/new-survey-finds-americans-favor-face-recognition-combat-rising-retail-theft-violence/.

[32] Ibid.

[33] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT), Part 1: Verification," National Institute of Standards and Technology, April 12, 2019, https://www.nist.gov/sites/default/files/documents/2019/04/15/frvt_report_2019_04_12.pdf.

[34] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects," National Institute of Standards and Technology, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[35] Ibid.

[36] Daniel Castro, "Note to Press: Facial Analysis is Not Facial Recognition," Innovation Files, January 27, 2019, https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition.

[37] Ibid.

[38] Daniel Castro and Michael McLaughlin, "Banning Police Use of Facial Recognition Would Undercut Public Safety," (Information Technology and Innovation Foundation, July 30, 2018), https://itif.org/publications/2018/07/30/banning-police-use-facial-recognition-would-undercut-public-safety.

[39] Matt Wood, "Thoughts on Machine Learning Accuracy," AWS Machine Learning Blog, July 27, 2018, https://aws.amazon.com/blogs/machine-learning/thoughts-on-machine-learning-accuracy/.

[40] See, for example, Daniel Wright, Catherine Boyd, and Colin Tredoux, "Inter-facial contact and the own-race bias for face recognition in South Africa and England," Applied Cognitive Psychology, March 14, 2003, https://onlinelibrary.wiley.com/doi/abs/10.1002/acp.898.

[41] "Digital Signage Privacy Standards," Digital Signage Federation, February 2011, https://www.digitalsignagefederation.org/wp-content/uploads/2017/02/DSF-Digital-Signage-Privacy-Standards-02-2011-3.pdf.

[42] "Privacy Best Practice Recommendations For Commercial Facial Recognition Use," n.d., https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf (accessed January 12, 2020).

[43] "Six principles to guide Microsoft's facial recognition work," Microsoft, December 17, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/.

[44] Michael Punke, "Some Thoughts on Facial Recognition Legislation," AWS Machine Learning Blog, February 7, 2019, https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

[45] "Our approach to facial recognition," Google, n.d., https://ai.google/responsibilities/facial-recognition/ (accessed January 12, 2020); "Facial Recognition Code of Ethics," Rank One Computing, November 22, 2019, https://blog.rankone.io/2019/11/22/facial-recognition-code-of-ethics/; "The Way Forward: Responsibly Deployed Facial Recognition," Medium, November 20, 2018 https://medium.com/trueface-ai/the-way-forward-responsibly-deployed-facial-recognition-65bf5cc9ed03.

[46] "U.S. Chamber Facial Recognition Policy Principles," C_TEC, December 5, 2019, https://www.uschamber.com/issue-brief/us-chamber-facial-recognition-policy-principles-0.

[47] "San Francisco is changing its facial recognition ban after it accidentally made the iPhones it gave to city employees illegal," *Business Insider*, December 19, 2019, https://www.businessinsider.com/san-francisco-amended-its-facial-recognition-ban-2019-12.

[48] "Now Your Groceries See You, Too," *The Atlantic*, January 25, 2019, https://www.theatlantic.com/technology/archive/2019/01/walgreens-tests-new-smart-coolers/581248/.

[49] Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America," Information Technology and Innovation Foundation, January 2019, https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america.

[50] "The Computer Scientist Who Wants to Put a Name to Every Face in Civil War Photographs," *Smithsonian Magazine*, March 19, 2019, https://www.smithsonianmag.com/innovation/computer-scientist-who-wants-to-put-name-to-every-face-in-civil-war-photographs-180971754/; "How Facial Recognition Is Fighting Child Sex Trafficking," *Wired*, June 19, 2019, https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/.

[51] Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law," Information Technology and Innovation Foundation, August 5, 2019, https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

[52] "Biometric Privacy Class Actions By The Numbers: Analyzing Illinois' Hottest Class Action Trend," Lexology, June 28, 2019, https://www.lexology.com/library/detail.aspx?g=4e1ddca6-229b-4760-8c0e-a44ad8e96293.

[53] Daniel Castro, Michael McLaughlin and Eline Chivot, "Who Is Winning the AI Race: China, the EU or the United States?" Center for Data Innovation, August 19, 2019, https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

[54] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects," National Institute of Standards and Technology, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[55] "12 US states and 7 countries that have barred protesters from wearing masks," *Business Insider*, October 7, 2019, https://www.businessinsider.com/countries-states-where-protesters-cant-wear-masks-2019-10.