ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

**Testimony of**

**Michael McLaughlin**

**Research Analyst**

**Information Technology and Innovation Foundation**

**Before the**

**California State Assembly Privacy and Consumer Protection Committee and the Assembly Select Committee on Emerging Technologies and Innovation**

**Hearing on**

# "Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges"

March 10, 2020

127 California State Capitol,

Sacramento, California

Chairman Chau, Vice-Chair Kiley, and members of the committee, thank you for the opportunity to appear before you to discuss the current legal framework and the potential need for government regulation of facial recognition technology.

I am a research analyst at 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.

In my testimony today, I would like to discuss the benefits of facial recognition technology, the current frameworks governing the use of the technology, and additional steps the California State Legislature can take to improve oversight and accountability.

## THE BENEFITS OF FACIAL RECOGNITION

Facial recognition technology compares images of faces to determine their similarity, which the technology represents using a similarity score. The technology often performs one of two types of comparisons. The first comparison is known as a one-to-many or identification search, in which the technology uses a probe image to search a database of images to find potential matches. The second comparison is known as a one-to-one or verification search as the technology compares two images to determine the similarity of the faces in them. In many cases, the faces in images are considered a match if their similarity score meets or exceeds the match threshold, a number the operator assigns that represents a minimum acceptable similarity score.[1] The technology has rapidly improved in recent years and is providing numerous benefits to society.

First, facial recognition has increased public safety.[2] For example, in April 2019, a California law enforcement officer saw a Facebook post about a missing young girl. The officer used facial recognition technology to find online sex trafficking advertisements that featured the missing girl. These matches led to more traditional police work, and within weeks, the recovery of the child.[3] Facial recognition has also helped identify individuals committing crimes ranging from shoplifting and check forgery to armed robbery and murder.[4] In addition, the technology can help law enforcement avoid arresting individuals for minor infractions of the law. For example, the San Diego Police Department must issue a citation to an individual that has violated a local ordinance or state law. If that person cannot confirm their identification, the department arrests the individual and runs their fingerprints. Between 2012 and 2019, however, the department used mobile facial recognition and fingerprint scanning devices, which allowed the department's officers to quickly identify an individual, and thus avoid booking an individual for failing to identify themselves.[5]

It is important to remember that without facial recognition, police must try to identify witnesses, suspects, and other persons of interest in a crime manually, such as by combing through mugshot photos or asking the public to help identify someone. These processes are slow, inaccurate, and expensive, particularly compared to using facial recognition.[6] Indeed, facial recognition will make it much more feasible to investigate low-dollar crimes, such as car break-ins and package thefts from doorsteps, which often go unaddressed.

Second, facial recognition has increased convenience for consumers. 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.[7] In addition, airlines are using facial recognition to allow travelers to get through 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] 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.[9]

Third, businesses are using the technology to improve security in several ways. For example, credit card companies like Visa and Mastercard have launched services that allow customers to verify the authenticity of online purchases by taking selfies.[10] In addition, some banks are using facial recognition to verify their customers' identity—online, in-person at a physical branch, and at ATMs.[11] Lastly, retailers also use facial recognition to identify known shoplifters, with some stores reporting the technology has reduced theft by 30 percent.[12]

Fourth, facial recognition has increased the accessibility of services for disabled individuals. For example, Facebook uses facial recognition to make its platform more accessible by automatically adding descriptive text to photos to explain who is in a photo.[13] 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.[14]

## EXISTING PROTECTIONS FROM FACIAL RECOGNITION ABUSES

Californians are protected from possible abuses of facial recognition technology in several ways, including by state law, the U.S. Constitution, and self-regulatory efforts by industry.

First, the newly enacted California Consumer Privacy Act provides Californians numerous privacy rights concerning the collection, use, and sharing of personal data of biometrics, including imagery of the face.[15] For example, businesses that have annual gross revenues greater than $25 million or hold identifying data for 50,000 or more people must inform consumers if they are collecting personal data.[16] Consumers also have the right to know the reason why a business is collecting data, and if the business is selling the data and to whom. In addition, consumers have the right to request access to the data and for an organization to delete it, unless the data is necessary for several purposes, such as detecting security incidents or preventing illegal activity.[17] The act also provides consumers the right to block businesses from selling their data. Furthermore, businesses cannot sell the personal data of an individual under the age of 16, unless they receive opt-in consent from a parent or guardian for children under 13 or opt-in consent from a child between 13 and 16.[18] Businesses also cannot discriminate against an individual that exercises their privacy rights, such as charging a higher price or offering a lower quality of service, unless the difference is related to the value of the consumer's data.[19] Collectively, these rights increase the transparency of the use of facial recognition by private actors and limit potential abuses, such as the unwanted sale of facial recognition data.

Second, the Body Camera Accountability Act (AB 1215) prohibits law enforcement from using a facial recognition system to analyze data collected from an officer camera. The law sunsets in 2023.[20] While there are many beneficial applications of using facial recognition with policy body cameras, such as helping law

enforcement quickly identify individuals on a watch list at a public event, the law makes it much harder to achieve these benefits.[21]

Third, the U.S. Constitution likely protects Californians from law enforcement abusing the technology. For example, the Supreme Court ruled in *Carpenter v. United States* that the government violated an individual's Fourth Amendment rights by receiving cellphone data that revealed a person's location over time without a search warrant.[22] As such, the use of facial recognition technology to surveil an individual for an extended period without a search warrant is likely a violation of the U.S. Constitution. Nonetheless, the Supreme Court ruling in *Katz v. United States* suggests that the government's use of facial recognition using public systems to identify individuals on a limited basis does not violate the Fourth Amendment because an individual's face is open to the public.[23] In short, the U.S. Constitution sets reasonable limits on the use of facial recognition by law enforcement, and these limits are one reason that fears about the U.S. adopting China-style surveillance measures are unwarranted.

Fourth, the standard of probable cause to make an arrest protects Californians from adverse outcomes that result from the technology falsely matching an individual. For example, the Federal Bureau of Investigation (FBI) has stated it uses the Next Generation Identification System, which includes facial recognition capabilities, for investigative purposes only. The FBI stated it does not use possible matches as the sole basis for an arrest.[24]

Finally, industry has developed voluntary self-regulation and principles to foster the responsible use of the technology. 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.[25] 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 2012, the U.S. Federal Trade Commission (FTC) published a staff report that recommended a series of best practices for business use of facial recognition technology. The report, which was the result of a workshop and eighty public comments, identified numerous best practices, including that companies should establish "appropriate retention and disposal practices for the consumer images and biometric data that they collect." The FTC's recommendations also included that businesses should provide clear notices that they are using facial recognition, provide consumers the opportunity to opt-out of facial recognition use, and that companies should not use the technology to identify anonymous images of an individual without their consent. For example, a company should not use the technology to identify an individual walking to work to learn their identity without the individual being aware.[26]

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 that offered guidelines for protecting consumer privacy.[27] Many of the technology companies that make facial recognition technology have also 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.[28] Amazon likewise has developed guidance for its facial recognition customers, created an acceptable use policy, and published its recommendations for federal legislation.[29] Indeed, many of the leading facial recognition technology vendors, including Google, RankOne, and Trueface, have released similar principles.[30] 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.[31]

## STEPS TO IMPROVE OVERSIGHT AND ACCOUNTABILITY

Because of the significant benefits of facial recognition, the potential for police to misuse the technology does not mean government should halt law enforcement's use of it. Instead, it means government should improve oversight of law enforcement's behavior and enact rules where necessary.[32] Indeed, the goal of any new facial recognition laws should be to prevent harms, not stop the technology's use.[33] The California State Legislature can and should take the following steps to improve oversight and accountability of facial recognition use by government.

First, the state legislature should require that law enforcement agencies publicly disclose it is using the technology.[34] While law enforcement agencies should not need to seek approval before using new technology, by publicly disclosing when they are using facial recognition they can alleviate concerns that law enforcement is using the technology without any public knowledge.

Second, the state legislature should require that the California Department of Justice or another relevant agency establish the following policies:

- Performance standards for the facial recognition systems law enforcement procures.[35] These standards could include both overall accuracy rates for facial recognition systems and specific ones for different genders, races, and age groups. Setting minimum performance standards would not only ensure that law enforcement does not procure ineffective technology, but it would also help promote the use of more accurate technology in the private sector.
- Policies for when the government, including law enforcement, can use facial recognition in sensitive environments, such as at protests, schools, and abortion clinics.
- Policies how state government agencies, and their contractors, can acquire and share photos used for facial recognition. The agency should also establish limits on how long images from government-owned camera systems, such as surveillance cameras and body cameras, can store images.[36] These policies can address privacy concerns.

Third, the state legislature should require that law enforcement obtain a warrant to use facial recognition or any technology, such as mobile phones or license plate readers, to track the location of an individual over an extended period of time.[37] For example, Sen. Mike Lee (R-Utah) and Chris Coons (D-Del) proposed the

Facial Recognition Technology Warrant Act of 2019, which requires that a government agency obtain a court order to use facial recognition technology to track the movements of an individual for more than 72 hours.[38] Similarly, the legislature should require that law enforcement obtain a warrant to access any database that contains detailed geolocation data about individuals.[39] These requirements can alleviate concerns that law enforcement will use facial recognition technologies to engage in mass surveillance.

Fourth, the legislature should require that state and local law enforcement entities have written policies on how they will use the technology. These policies could include who will have access to the technology, how the entity trains individuals on using the technology, and how and when and it will decide to use the technology.[40] Law enforcement could also detail in its policies how it adds an individual to a state or local watch list, the types of data sources used for images, and data retention policies.[41] Establishing best practices on the types of images law enforcement will use can reduce concerns that law enforcement will use low-quality data that increases the possibility of false matches.[42] In addition, the policies could include an overview of how the law enforcement entity will set confidence thresholds for facial recognition searches. The policies should also detail how the entity will log its searches and how it will track metrics on the success rate of the technology, including the number of times a facial recognition system helped lead to an arrest.[43] In combination, these policies can help ensure law enforcement uses the technology appropriately.[44]

Fifth, the legislature can establish guardrails for the use of live facial recognition systems, which attempt to match faces in real-time images, such as from closed-circuit television (CCTV) cameras. In such scenarios, the legislature can require that law enforcement only match faces against a database of specific groups of individuals, such as lost children or individuals with outstanding arrest warrants for felonies.[45] These guardrails could limit the potential that law enforcement uses the technology for widespread surveillance. Law enforcement's written policies on facial recognition could also include a policy for the circumstances under which it would use live facial recognition.

Finally, the legislature should fund training to teach law enforcement how to properly use the technology as well as encourage law enforcement to pilot the technology before implementing it. This training could include educating law enforcement about how to maximize effectiveness, such as by choosing appropriate confidence thresholds and using high-quality reference images. For example, 1-to-many algorithms often make a series of 1-to-1 comparisons against a large number of images in a database. As such, users of the technology may need to employ higher confidence thresholds for 1-to-many searches compared to 1-to-1 searches to reduce the likelihood of falsely matching any two images.[46] In addition, piloting the technology would help law enforcement learn a particular facial recognition systems' strengths and weaknesses and evaluate how it performs in their own communities. For example, law enforcement can use the pilots to learn the appropriate confidence thresholds for different applications depending on the desired false-positive and false-negative rates.

## WHY CALIFORNIA SHOULD NOT IMPLEMENT A BAN ON FACIAL RECOGNITION

There are numerous reasons why the California State Legislature should adopt targeted legislation to ensure appropriate and effective use of facial recognition, rather than overreacting by banning the technology, either temporarily or permanently.

First, many critics calling for bans cite misleading research to bolster their claims. For example, the American Civil Liberties (ACLU) has produced two misleading reports that incorrectly suggest facial recognition systems are inaccurate.[47] In the first report, the ACLU used Amazon's Rekognition service to compare mugshot images of criminals to photos of members of the U.S. Congress. The ACLU said that the system had a false-positive rate of five percent.[48] The ACLU performed a similar test using images of California lawmakers, finding that the system falsely matched 20 percent of California lawmakers with criminals.[49] However, in each instance, the ACLU set artificially low confidence thresholds for matching faces to create these results so that many false positives were allowed.[50] Indeed, Amazon has noted that the ACLU's error rates for matching members of the U.S. Congress would have dropped to zero if it had used an appropriate confidence threshold of 99 percent.[51] The ACLU repeated its test for California lawmakers even after Amazon had publicly clarified its position on the appropriate confidence thresholds. Moreover, ACLU has refused to release the data or code used to produce its reports which has allowed its claims to avoid legitimate scrutiny.

Critics also frequently cite studies from MIT Media Lab that tested gender classification systems, rather than facial recognition systems, to imply the latter technology is inaccurate. However, the technologies are different, and the accuracy of one has no bearing on the other, and there are no reports of law enforcement using gender classification systems.[52] Indeed, gender classification tools attempt to classify a person's gender, not match faces. *The New York Times* published an article with the headline blaring "Amazon Is Pushing Facial Technology That a Study Says Could Be Biased" about the MIT Media Lab study.[53] Unfortunately, this confusion has led to critiques of facial recognition by prominent figures. For example, Sen. Ed Markey (D-MA) tweeted that the "Adoption of flawed facial recognition technologies by law enforcement could literally hardwire racial and gender bias into police depts" while linking to *The New York Times* article.[54]

Second, the National Institute of Standards and Technology (NIST) has found that the best facial recognition systems are extremely accurate. For example, NEC-2, the best 1-to-many algorithm NIST tested in a 2019 report, failed to rank the correct candidate as the most likely match only 0.12 percent of the time when performing a search of a database containing images of 3 million individuals.[55] If an individual used the algorithm to perform 25,000 searches, it would have failed to list the correct individual as the most likely match only 30 times.[56]

Third, the best facial recognition systems have no or little bias. For example, a recent NIST report reveals that the most accurate 1-to-many algorithms have "undetectable" differences between demographic groups and that the most accurate 1-to-1 algorithms have low-false positive rates and false-negative rates across most demographic groups.[57] For example, NIST's testing shows that several algorithms maintained true positive and true negative accuracy rates greater than 99 percent for all races and sexes.[58]

Nonetheless, many of the facial recognition algorithms NIST tested did have higher false-positive rates for minorities and women than white males. However, NIST tested nearly 200 algorithms from vendors and labs around the world—it allows anyone to submit an algorithm for testing, including those from labs in China

that are on the Entity List, which prohibits U.S. firms from selling technology to companies on the list without government approval.[59] As such, it found a wide variance in performance between different algorithms. It is also true that most 1-to-1 algorithms had higher false-negative rates for women than men. But NIST notes that this "is a marginal effect—perhaps 98 percent of women are still correctly verified—so the effect is confined to fewer than 2 percent of comparisons where algorithms fail to verify."[60] Most importantly, however, NIST's testing demonstrated the accuracy and lack of bias of the best-performing algorithms. As such, California's government agencies do not have to procure biased technology.

Fourth, bans can have unintended consequences. For example, San Francisco's ban on government agencies using facial recognition accidentally made it illegal for the city's employees to use city-issued iPhones, which used facial recognition.[61]

Fifth, the fear of facial recognition technology that has led to calls for bans is similar to claims about other technologies that have not had their fears realized. For example, in the 1960s, many people feared transistors would spell the end of privacy, with miniature electronics used to eavesdrop on private conversations.[62] In the early 2000s, privacy advocates called for bans of radio frequency identification (RFID) chips, which use radio waves to transmit data, in several use cases, including on government identification documents.[63] These advocates warned that stores, governments, and even terrorists would use RFID to track the movements of individuals. For example, the Electronic Frontier Foundation (EFF) argued that a 2005 U.S. State Department proposal to require RFID chips in passports would turn passports into "terrorist beacons," stating "that's precisely what they'll become if we allow the State Department to move ahead with this plan."[64] The fears of stores, governments, or terrorists tracking individuals with RFID never materialized. Moreover, just as transistors did not give rise to widespread eavesdropping, neither will facial recognition lead to pervasive surveillance.[65]

Finally, bans or moratoriums limit the positive uses of facial recognition. Facial recognition has already helped find missing individuals, identify individuals who committed serious crimes, such as armed robbery, and prevent potentially dangerous people, such as sex offenders, from entering school facilities.[66] A ban or moratorium not only limits negative uses of facial recognition but positive uses as well.

## REFERENCES


1. Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist," (Information Technology and Innovation Foundation, January 27, 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

2. "Should Government Halt the Use of Facial-Recognition Technology?" *The Wall Street Journal*, February 23, 2020, https://www.wsj.com/articles/should-government-halt-the-use-of-facial-recognition-technology-11582513260.

3. Tom Simonite, "How Facial Recognition Is Fighting Child Sex Trafficking," Wired, June 19, 2019, https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/.

4. Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *The New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html; Face Facts: Dispelling Common myths Associated with Facial Recognition Technology," Security Industry Association, accessed March 5, 2020, https://www.securityindustry.org/report/face-facts-dispelling-common-myths-associated-with-facial-recognition-technology/.

5. DJ Pangburn, "San Diego's Massive, 7-Year Experiment With Facial Recognition Technology Appears to Be a Flop," Fast Company, January 9, 2020, https://www.fastcompany.com/90440198/san-diegos-massive-7-year-experiment-with-facial-recognition-technology-appears-to-be-a-flop.

6. Chris Adzima, "Using Amazon Rekognition to Identify Persons of Interest for Law Enforcement," AWS Machine Learning Blog, June 15, 2017, https://aws.amazon.com/blogs/machine-learning/using-amazon-rekognition-to-identifypersons-of-interest-for-law-enforcement/.

7. "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/; http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

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. "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-privacyconcerns/2018/09/15/a312f6d0-abce-11e8-a8d7-0f63ab8b1370_story.html.

10. "Fighting fraud with a smile," Visa, n.d., https://usa.visa.com/visa-everywhere/security/fighting-fraud-with-asmile.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/mastercardand-bmo-make-fingerprint-and-selfie-payment-technology-a-reality-in-north-america/; Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy,"

(Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

11. 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/; Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

12. 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-testingout-facial-recognition-at; Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

13. "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).

14. "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/.

15. California Consumer Privacy Act of 2018, Senate Bill No. 1121, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

16. California Consumer Privacy Act of 2018, Senate Bill No. 1121, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121; "How the New California Privacy Law (CCPA) Handles Facial Recognition," *Calrip*, accessed March 3, 2020, https://www.clarip.com/data-privacy/california-privacy-law-facial-recognition/.

17. California Consumer Privacy Act of 2018, Senate Bill No. 1121, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121; "How the New California Privacy Law (CCPA) Handles Facial Recognition," *Calrip*, accessed March 3, 2020, https://www.clarip.com/data-privacy/california-privacy-law-facial-recognition/.

18. California Consumer Privacy Act of 2018, Senate Bill No. 1121, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121; "How the New California Privacy Law (CCPA) Handles Facial Recognition," *Calrip*, accessed March 3, 2020, https://www.clarip.com/data-privacy/california-privacy-law-facial-recognition/.

19. California Consumer Privacy Act of 2018, Senate Bill No. 1121 (2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121; "How the New California Privacy Law (CCPA) Handles Facial Recognition," *Calrip*, accessed March 3, 2020, https://www.clarip.com/data-privacy/california-privacy-law-facial-recognition/.

20. The Body Camera Accountability Act, Assembly Bill No. 1215 (2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

21. Daniel Castro and Michael McLaughlin, "Banning Facial Recognition in Policy Body Cameras Will make Californian's Less Safe," Information Technology and Innovation Foundation, September 10, 2019, https://itif.org/publications/2019/09/10/banning-facial-recognition-police-body-cameras-will-make-californians-less.

22. Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?," American Bar Association, accessed March 3, 2020, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/; *Carpenter v. United States,* 138 S. Ct. 2206 (2018).

23. Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?," American Bar Association, accessed March 3, 2020, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/; *Katz v. United States*, 389 U.S. 347 (1967).

24. Kristine Hamann and Rachel Smith, "Facial Recognition Technology: Where Will It Take Us?," American Bar Association, accessed March 3, 2020, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

25. "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.

26. "Facing Facts: Best Practices for Common Uses of Facial recognition Technologies," (Washington, DC: U.S. Federal Trade Commission, October 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

27. "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_facia l_recogntion.pdf (accessed January 12, 2020); Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

28. "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/.

29. 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/.

30. "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-deployedfacial-recognition-65bf5cc9ed03.

31. "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.

32. "Should Government Halt the Use of Facial-Recognition Technology?" *The Wall Street Journal*, February 23, 2020, https://www.wsj.com/articles/should-government-halt-the-use-of-facial-recognition-technology-11582513260.

33. Daniel Castro, "Connecticut's Facial Recognition Bill: A Model For States?," *Government Technology* , May 31, 2016, https://www.govtech.com/opinion/Connecticuts-Facial-Recognition-Bill-A-Model-for-States.html.

34. Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

35. "Should Government Halt the Use of Facial-Recognition Technology?" *The Wall Street Journal*, February 23, 2020, https://www.wsj.com/articles/should-government-halt-the-use-of-facial-recognition-technology-11582513260.

36. Robert D. Atkinson, "Facial-Recognition Technology: Closer to Utopia Than Dystopia," *Nation Review* , November 25, 2019, https://www.nationalreview.com/2019/11/facial-recognition-technology-closer-to-utopia-than-dystopia/.

37. Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

38. Facial Recognition Technology Warrant Act of 2019, S.2878, 116th Cong. (2019); https://www.congress.gov/bill/116th-congress/senate-bill/2878/text.

39. Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

40. Peter Callaghan, "Minnesota Legislature Begins Considering Facial-Recognition Technology Regulations," *MinnPost,* February 3, 2020, https://www.minnpost.com/state-government/2020/02/minnesota-legislature-begins-considering-facial-recognition-technology-regulations/; "Understanding Facial Recognition Systems," (San Francisco: Partnership on AI, February 19, 2020), https://www.partnershiponai.org/facial-recognition-systems/.

41. "Understanding Facial Recognition Systems," (San Francisco: Partnership on AI, February 19, 2020), https://www.partnershiponai.org/facial-recognition-systems/; Daniel Castro, "Statement to the House Committee Statement to the House Committee on Oversight and Reform Regarding Facial Recognition and Civil Liberties," (Information Technology and Innovation Foundation), May 21, 2019, http://www2.itif.org/2019-itif-facial-recognition-letter-final.pdf?_ga=2.225391448.313082901.1583169240-354924416.1550612241.

42. Clare Garvie, "Garbage in, Garbage Out," (Georgetown Law Center on Privacy and Technology, May 16, 2019), https://www.flawedfacedata.com.

43. "Understanding Facial Recognition Systems," (San Francisco: Partnership on AI, February 19, 2020), https://www.partnershiponai.org/facial-recognition-systems/.

44. Daniel Castro and Michael McLaughlin, "Banning Facial Recognition in Policy Body Cameras Will make Californian's Less Safe," Information Technology and Innovation Foundation, September 10, 2019, https://itif.org/publications/2019/09/10/banning-facial-recognition-police-body-cameras-will-make-californians-less.

45. Daniel Castro and Michael McLaughlin, "Banning Facial Recognition in Policy Body Cameras Will make Californian's Less Safe," Information Technology and Innovation Foundation, September 10, 2019, https://itif.org/publications/2019/09/10/banning-facial-recognition-police-body-cameras-will-make-californians-less; Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (Washington, DC: National Institute of Standards and Technology, December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

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

47. Daniel Castro, Hearing on "Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy," (Before the House Committee on Oversight and Reform), January 15, 2020, http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

48. Ryan Suppe, "Amazon's Facial Recognition Tool Misidentified 28 Members of Congress in ACLU Test," *USA Today*, July 30, 2018, https://www.usatoday.com/story/tech/2018/07/26/amazon-rekognition-misidentified-28-members-congress-aclu-test/843169002/; 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.

49. Madeleine Gregory, "Amazon's Facial Recognition Misidentified 1 in 5 California Lawmakers as Criminals," *Vice*, August 13, 2019, https://www.vice.com/en_us/article/ne8wa8/amazons-facial-recognition-misidentified-1-in-5-california-lawmakers-as-criminals.

50. Daniel Castro and Michael McLaughlin, "Banning Facial Recognition in Policy Body Cameras Will make Californian's Less Safe," Information Technology and Innovation Foundation, September 10, 2019, https://itif.org/publications/2019/09/10/banning-facial-recognition-police-body-cameras-will-make-californians-less.

51. 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/.

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

53. Natasha Singer, "Amazon is Pushing Facial Technology That a Study Says Could Be Biased," *The New York Ti*https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

54. 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.

55. Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, September 2019), https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf.

56. Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist," (Information Technology and Innovation Foundation, January 27, 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

57. Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist," (Information Technology and Innovation Foundation, January 27, 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

58. These algorithms include visionlabs-007 and everai-paravision-003; Patrick Grother, Mei Ngan, and Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 2: Identification (Washington, DC: National Institute of Standards and Technology, September 2019), 47, https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf.

59. Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist," (Information Technology and Innovation Foundation, January 27, 2020), https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms; "U.S. to Blacklist Chinese Artificial-Intelligence Companies," *Associated Press*, October 7, 2019, https://www.marketwatch.com/story/us-to-blacklist-chinese-artificial-intelligence-companies-2019-10-07.

60. National Institute of Standards and Technology, Ongoing Face Recognition Vendor Test (FRVT) (part 3: demographic effects, annex 15: genuine and imposter score distributions for United States mugshots, 19), https://pages.nist.gov/frvt/reports/demographics/annexes/annex_15.pdf#20.

61. Tom Simonite, "It's Hard to Ban Facial Recognition Tech in the iPhone Era," *Wired*, December 19, 2019, https://www.wired.com/story/hard-ban-facial-recognition-tech-iphone/.

62. Daniel Castro, "Facial Recognition Bans Handcuff Law Enforcement," *Real Clear Policy*, May 22, 2019, https://www.realclearpolicy.com/articles/2019/05/22/facial_recognition_bans_handcuff_law_enforcement_111200.html.

63. Alorie Gilbert, "California Bill Would Ban Tracking Chips in Ids," *ZDNet*, April 29, 2005, https://www.zdnet.com/article/california-bill-would-ban-tracking-chips-in-ids/; Daniel Castro and Michael McLaughlin, "Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence," (Information Technology and Innovation Foundation, February 4, 2019), https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence.

64. Donna Wentworth, "New Us Passports Will Serve as Terrorist Beacons," Electronic Frontier Foundation, March 31, 2005, https://www.eff.org/deeplinks/2005/03/new-us-passports-will-serve-terrorist-beacons; Daniel Castro and Michael McLaughlin, "Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence," (Information Technology and Innovation Foundation, February 4, 2019), https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence.

65. Daniel Castro, "In Attempt to Ban Facial Recognition Technology, Massachusetts Could Inadvertently Ban Facebook, iPhones, and More," Information Technology and Innovation Foundation, October 21, 2019, https://itif.org/publications/2019/10/21/attempt-ban-facial-recognition-technology-massachusetts-could-inadvertently.

66. Daniel Castro, "Are Governments Right to Ban Facial Recognition Technology?," *Government Technology*, May 2019, https://www.govtech.com/products/Are-Governments-Right-to-Ban-Facial-Recognition-Technology.html; Tom Simonite, "How Facial Recognition Is Fighting Child Sex Trafficking," Wired, June 19, 2019, https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/; Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *The New York Times*, January 12, 2020, https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.