LEGISLATIVE REFERENCE BUREAU

Facial Recognition Technology: Balancing Safety and Privacy

Jillian Slaight, PHD
legislative analyst

Ryan LeCloux
legislative analyst

WISCONSIN POLICY PROJECT • March 2020, Volume 3, Number 4

One East Main Street, Suite 200, Madison, Wisconsin 53703
http://legis.wisconsin.gov/lrb • 608-504-5801

Introduction

In the mid-2000s, legal researchers coined the term "*CSI* Effect," referring to the idea that television dramas had created unrealistic expectations of law enforcement technology and forensic science—expectations that real-life police and prosecutors struggled to meet.[1] But tech innovations have narrowed the gap between television and reality in the decade since. Of these, facial recognition technology increasingly enables police investigators to do what their fictional TV counterparts have done for years: identify a suspect based solely on a photograph or video still. For example, in 2019, an app developed by Clearview AI helped police apprehend "an adult who was visible in [a child exploitation video] just for a few seconds in the background." The app matched the man's image with a face "in the background of someone else's gym selfie" posted on social media, which led investigators to the suspect's gym, where employees identified the man.[2]

This example spells out the potential rewards of facial recognition. However, other examples spell out its risks—such as in China, where the technology facilitates the suppression of minorities and discourages "uncivilized behavior" in public.[3] How can Americans ensure that private and public entities will not use facial recognition to intrude in their private lives? "In circumstances involving dramatic technological change," U.S. Supreme Court Justice Samuel Alito remarked in *United States v. Jones*, "the best solution to privacy concerns may be legislative." As Alito explained, "a legislative body is well situated to gauge changing public attitudes . . . and to balance privacy and public safety in a comprehensive way."[4] For these reasons, state legislators across the country have begun to debate whether and how to regulate facial recognition technology. This publication introduces this technology, reviews its applications and current implementation, and surveys existing and proposed regulations at the federal, state, and local levels of government.

Overview of facial recognition technology

Facial recognition technology falls under the broader category of **biometrics**, a term that designates "identification of individuals based on their biological or behavioral characteristics."[5] Biological characteristics include a person's face, eyes, handprint, fingerprint,

[1] See, for example, N. J. Schweitzer and Michael J. Saks, "The CSI Effect: Popular Fiction about Forensic Science Affects the Public's Expectations about Real Forensic Science," *Jurimetrics* 47, (Spring 2007): 357–64, https://public.asu.edu; Susan Sarapin and Glenn Sparks, "Eyewitnesses to TV versions of reality: The relationship between exposure to TV crime dramas and perceptions of the criminal justice system," in *How Television Shapes our World View: Media Representations of Social Trends and Change* (New York: Springer, 2014), 145–70; and Kimberlianne Podlas, "The '*CSI* Effect'" *Criminology and Criminal Justice* (August 2017), https://oxfordre.com. For a rebuttal of these arguments, see, for example, Donald Shelton, "The 'CSI Effect': Does It Really Exist?" *NIJ Journal* 259 (March 2008).

[2] Michael Barbaro, "The End of Privacy as We Know It?" The Daily (podcast), February 10, 2020, https://nytimes.com.

[3] Darren Byler, "China's hi-tech war on its Muslim minority," *Guardian*, April 11, 2019, https://theguardian.com; Amy Qin, "Facial Recognition Marks Chinese Pajama Wearers," *New York Times*, January 22, 2020.

[4] United States v. Jones, No. 10-1259 at 13 (U.S. Jan. 23, 2012).

[5] Anil K. Jain, Ruud Bolle, and Sharath Pankanti, *Biometrics: Personal Identification in Networked Society* (New York:

or DNA, whereas behavioral characteristics include the way a person walks, speaks, or writes.[6] According to computer scientist Anil K. Jain of Michigan State University, a biometric measure must possess all of the following qualities to be useful as a form of identification:[7]

- **universal**—everyone has it.
- **unique**—it varies from person to person.
- **permanen**t—it does not change over time.
- **collectable**—it may be captured, measured, and compared.

Faces do not necessarily meet the standards outlined above. On one hand, faces are universal and unique; all people have them, and no two people's faces are identical. On the other hand, they change over time with age, injury, or cosmetics. Moreover, experts dispute whether computers can actually measure and compare faces with accuracy.[8] Nevertheless, researchers have pursued advances in **facial recognition technology**, i.e., "automated systems for identifying human faces and distinguishing them from one another."[9]

The success of this technology relies on teaching computers how to do something that humans do instinctively. Generally, humans recognize each other by simultaneously interpreting a face holistically (i.e., registering the face in its entirety) and interpreting it piecemeal (i.e., registering component parts like the nose, eyes, or mouth).[10] By comparison, computers tend to rely on the piecemeal method.[11] Accordingly, facial recognition systems engineers must design algorithms that analyze the component parts of the face, such as the length of the nose, distance between the nose and upper lip, color of the cheek, or curvature of the hairline. These algorithms allow computers to compare faces on the basis of quantifiable data. Generally, systems engineers create algorithms using a selective "training set" of images but may make changes as they draw conclusions about the facial features that tend to predict more accurate comparisons.[12]

Springer, 2002), 1–4. See also definitions provided in "Introduction" in Julian Ashbourn, *Practical Biometrics* (London: Springer, 2015), 1–10: 1.

[6] Eyes may be identified by either the iris or retina. Jain, Bolle, and Pankanti, *Biometrics*, 1–4.

[7] Jain, Bolle, and Pankanti, *Biometrics*, 4.

[8] These disputes will be addressed later in this publication.

[9] Kelly A. Gates, *Our Biometric Future: Facial Recognition and the Culture of Surveillance* (New York: New York University Press, 2011), 3. Please note that this publication employs the more broadly used term "facial recognition technology" in lieu of "face recognition technology," employed by many scientists and researchers.

[10] Scientists seem to disagree on how the brain precisely balances these two approaches. On human recognition of faces, see Vicki Bruce and Andy Young, "Understanding face recognition," *British Journal of Psychology* 77 (1986), 305–27; Morris Moscovitch, Gordon Winocur, and Marlene Behrmann, "What is special about face recognition? Nineteen experiments on a person with visual object…," *Journal of Cognitive Neuroscience* 9 (1997), 555–604; and Jason J. S. Barton and Sherryse L. Corrow, "Recognizing and identifying people: A neuropsychological review," *Cortex* 75 (2016), 132–50.

[11] That said, the tech industry has made recent advances in "deep learning," a way of making computers function more like the human brain, thus more capable of recognizing certain images without first undergoing training. See, for example, Robert D. Hof, "Deep Learning: With massive amounts of computational power, machines can now recognize objects and translate speech in real time. Artificial intelligence is finally getting smart," *MIT Technology Review*, April, 23, 2013, https://technologyreview.com.

[12] For a succinct description, see Clare Garvie, Alvaro M. Bedoya, and Jonathan Frankle, The Perpetual Line-Up:

In practice, facial recognition technology operates much like DNA identification by law enforcement. Facial images of known persons undergo **enrollment**, i.e., storage within a database alongside other identifying information, such as name, date of birth, or place of residence. Database operators may then perform **matching**, i.e., comparison to all other database enrollees to generate a numerical "match score" representing the likelihood that the two faces belong to the same person.[13]

Applications

For scientists, facial recognition represents an opportunity to explore the fundamental differences between the intelligences of humans and computers, to learn from their interactions with each other, and to consider whether and how they may someday become more alike.[14] For the broader public, this technology represents the potential to quickly and accurately identify individuals for the sake of public safety and personal convenience.

Identity verification. Reliable, well-functioning facial recognition programs could replace other forms of identity verification that are easily lost, stolen, or forgotten—like driver's licenses, passports, PINs, keys, or alphanumeric passwords.[15] In the near future, people may rely on facial recognition alone to enter their homes, access their bank accounts, or pass through security checkpoints at airports. Companies like Apple have already implemented this technology in personal devices like the iPhone in lieu of cumbersome, less secure modes of entry like alphanumeric codes.[16] In this context and others, facial recognition promises convenience as well as security.

Safety, security and surveillance. Facial recognition technology also promises to improve public and private security surveillance systems. Using mobile facial recognition programs, law enforcement officers may verify the identity of a suspect—or a John Doe victim—at the scene of a crime. Similar programs may enable TSA employees to apprehend terrorists at an airport terminal, or allow private security officers to stop known shoplifters upon entering a store. Where surveillance cameras are already in place, facial recognition programs promise to eliminate or reduce personnel hours spent watching surveillance camera footage. These programs may also reduce human error in identifying unknown persons from surveillance footage.[17]

Unregulated Police Face Recognition in America, (Washington, D.C.: Georgetown Law Center on Privacy & Technology, October 18, 2016): 9–10, https://perpetuallineup.org.

[13] "Face Recognition," Electronic Frontier Foundation, last accessed November 2, 2018, https://eff.org; U.S. Government Accountability Office, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy, (Washington, D.C.: Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate, May 2016): 5–6, https;//gao.gov.

[14] See, for example, the opening pages of Gates, 3.

[15] Jain, Bolle, and Pankanti, *Biometrics*, 1–4.

[16] "Facial recognition technology will change the way we live" YouTube video, posted by "The Economist," November 1, 2017, https://youtube.com.

[17] Gates, *Our Biometric Future*, 3.

Consumer data. Facial recognition systems can be used in myriad commercial settings. For instance, they could facilitate market research by enabling companies to identify and collect data about their customers. The same systems could also identify and greet loyal customers as they enter a business.[18]

Products that promise to instantaneously name unknown people—whether shoppers or shoplifters, travelers or terrorists—have broad commercial and noncommercial potential. On the basis of that potential, the market for facial recognition technology has expanded rapidly and may reach $9.6 billion over the next four years.[19] Most industry players orient themselves toward law enforcement agencies or private security firms.[20] However, many companies market themselves to retailers for the purposes of data analytics,[21] and several programs are designed specifically for schools with the goal of preventing shootings.[22]

Implementation in the United States

In the United States, facial recognition technology is already in use, generally among public and private entities that maintain existing databases of facial images. These include local, state, and federal law enforcement agencies, other state and federal agencies, and social media companies.

Among state and local law enforcement agencies, the extent of implementation is unclear.[23] The Center on Privacy & Technology at Georgetown Law, an interest group

[18] Nick Tabor, "Smile! The Secretive Business of Facial-Recognition Software in Retail Stores," *New York Magazine*, October 20, 2018, https://nymag.com; FaceVACS-Video Scan, "Face recognition technology for real-time watch list alerts and anonymous people analytics," promotional flyer, accessed March 3, 2020, https;//cognitec.com.

[19] Rachna Singh, *Facial Recognition Market Overview*, (Allied Market Research, June 2016), https://alliedmarketresearch.com. Within the United States, the facial recognition technology vendor Rekognition has attracted outsized attention due to its parent company (Amazon). Other vendors include FaceFirst; Cognitec FaceVACS—VideoScan; Idemia—EFF; NEC NeoFace Reveal; Gemalto Cogent—Live Face Identification System; DataWords Plus—FACE Plus.

[20] For example, Idemia's Face Expert 2.0 promises to help law enforcement identify missing persons with imperfect images. "Face Expert: Helping police and intelligent services to put a name to a face," Idemia, accessed March 3, 2020, https://idemia.com. FACE Plus from DataWorks Plus promises police officers the ability to remotely identify suspects using photographs taken from their mobile devices. "FACE Plus: Facial Recognition Technology & Case Management," DataWorks Plus, accessed March 3, 2020, https;//dataworksplus.com.

[21] A promotional flyer for Cognitec FaceVACS-VideoScan, for example, advertises the program's potential to "alert staff to provide special treatment to valued customers." The same materials also suggest that clients may use the system to "analyze traffic patterns and times" and "define, view and export statistics about people flow, visitor demographics and client behavior." FaceVACS-Video Scan, "Face recognition technology."

[22] For an overview of these products and their implementation in one school system in New York, see Rose Eveleth, "Facing Tomorrow's High-Tech School Surveillance," *Vice Motherboard*, October 29, 2018, https://vice.com. Aegis (SN Technologies Corp, Canada), for example, notifies school administrators of unauthorized entry into the school by prohibited persons like sex offenders or fired personnel. "Products," SNTech, accessed March 3, 2020, https://sntechnologies.ca. SAFR is a free, open-source program that works with existing surveillance hardware to help schools "analyze potential threats such as expelled students." "SAFR," RealNetworks, accessed November 19, 2018, https;//safr.com.

[23] Barring reliable statistics, journalists reporting on the issue tend to focus on individual police departments with confirmed contracts with companies that provide facial recognition services. *BuzzFeed*, for example, has investigated use of the technology by the Orlando (Florida) Police Department, whereas the Center for Investigative Journalism has looked specifically at San Diego County. Davey Alba, "With No Laws to Guide It, Here's How Orlando Is Using Amazon's Facial Recognition Technology," *BuzzFeed News*, last updated October 30, 2018, https://buzzfeednews.com; Ali Winston, "Facial recognition, once a battlefield tool, lands in San Diego County," *Reveal from the Center for Investigative Journalism*, November 7, 2013, https://revealnews.org. Unsurprisingly, the frequency and nature of police departments' collaboration with commercial facial

lobbying for regulations in this area, estimates that about a quarter of law enforcement agencies in the United States have some facial recognition technology capabilities.[24] These capabilities vary, but generally serve the following purposes: matching arrestees to aliases, confirming the identity of suspects, and identifying wanted persons in surveillance footage. Normally, officers search for matches within mugshot databases but may also access statewide driver's license databases in about half of all states.[25] Likewise, the Federal Bureau of Investigation may access at least 18 states' driver's license databases.[26]

Certain states not only authorize law enforcement searches of driver's license databases, but also use facial recognition technology to root out identity theft and fraud within those same systems. The New York Department of Motor Vehicles first implemented this technology in 2010 to identify and take action against persons with driver's licenses under multiple names. (Other states, like New Jersey, followed suit.)[27] As of 2017, the New York DMV had found at least 20,000 instances of fraud—for example, persons who collected government benefits using multiple identities, and persons who used false identities to drive despite multiple drunk driving convictions.[28]

At the federal level, the FBI operates its own image database, the Next Generation Identification—Interstate Photo System (NGI-IPS), which contains about 38 million mugshots.[29] The Facial Analysis, Comparison, and Evaluation (FACE) Services unit searches for face matches within this database, as well as various other federal and state photo databases. All told, the FBI draws from a total of more than 400 million faces.[30] In addition to the FBI, other federal entities, such as Immigration and Customs Enforcement (ICE), have performed facial recognition searches using state photo databases.[31]

In addition to government use, private tech companies have also incorporated facial recognition technology in their platforms. For example, in December 2017, Facebook announced tools designed to help users identify or "tag" themselves in photographs or

recognition vendors is also unclear. See, for example, Tom Simonite, "Few Rules Govern Police Use of Facial-Recognition Technology," *Wired*, May 22, 2018, https://wired.com; Matt Cagle and Nicole A. Ozer, "Amazon Teams Up With Law Enforcement to Deploy Dangerous New Face Recognition Technology," *ACLU NorCal*, May 22, 2018, http://aclunc.org.

[24] This estimate is based on survey results and public records requests. Garvie et al., "The Perpetual Line-Up," 25.

[25] Garvie et al., "The Perpetual Line-Up," 11–12, 2.

[26] "Hearing Materials for Committee to Review Law Enforcement's Policies on Facial Recognition Technology," Before the Full Committee on Oversight and Reform, 115th Cong., March 22, 2017, https://republicans-oversight.house.gov/.

[27] Jenni Bergal, "States Use Facial Recognition Technology to Address License Fraud," *Governing*, July 15, 2015, https://governing.com.

[28] Office of New York Governor Andrew Cuomo, "Governor Cuomo Announces Major Facial Recognition Technology Milestone with 21,000 Fraud Cases Investigated," press release, August 21, 2017, https://governor.ny.gov.

[29] Erin M. Prest, Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System, (Federal Bureau of Investigation, approved October 29, 2019), https://fbi.gov.

[30] Garvie et al., "The Petpetual Line Up," 13. See also, Ernest J. Babcock, "Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit," Federal Bureau of Investigation, May 1, 2015, https://fbi.gov.

[31] Drew Harwell, "FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches," *Washington Post*, July 7, 2019, https://washingtonpost.com. The Department of Homeland Security has also explored the potential of scanning faces of international travelers leaving the country. Harrison Rudolph, Laura M. Moy, and Alvaro M. Bedoya, Not Ready for Takeoff: Face Scans at Airport Departure Gates, (Washington, D.C.: Georgetown Law Center on Privacy & Technology, December 21, 2017), https://airportfacescans.com.

to detect unauthorized uses of their likenesses.[32] Within just two years, Facebook scaled back these tools in response to backlash—and a lawsuit claiming that the company applied its facial recognition technology without user consent.[33] Whether or not they have implemented or released similar tools, other companies have harnessed user information to create and test facial recognition algorithms. Yahoo, for example, created a massive database of faces from millions of photos uploaded to Flickr. Researchers from other tech companies, such as Google and Amazon, have accessed photos from that database.[34] Granted, some of those companies, such as Google, have explored but withheld facial recognition programs due to concerns about their potential misuse.[35]

Finally, one recent application of facial recognition technology bridges the public and private sectors. In January 2020, the *New York Times* revealed that the small tech company Clearview AI had licensed a facial recognition app to an unspecified number of law enforcement agencies in 2019. Clearview AI boasts a database of at least three billion photographs culled or "scraped" from social media companies like Facebook, Twitter, and Venmo—often in direct contravention of those companies' terms of service. According to this reporting, law enforcement agencies have embraced the app not only for its breadth of images, but also for its "superior" ability to identify faces from photographs taken at indirect angles.[36]

Concerns

The characteristic that renders faces useful as biometric identifiers—universality, or the fact that everyone has a face—heightens the consequences of facial recognition technology. While this technology may help to keep people and personal data more secure, it may also enable widespread public and private surveillance. Nothing exemplifies this dystopian potential more than its implementation in China, where facial recognition has been used in tandem with as many as 300 million surveillance cameras for purposes as wide ranging as monitoring the movement of ethnic minorities and shaming people who wear pajamas in public.[37] However extreme these deployments are to international

[32] Joaquin Quiñonero Candela, "Managing Your Identity on Facebook With Face Recognition Technology," Facebook, December 19, 2017, https://about.fb.com.

[33] Srinivas Narayanan, "An Update About Face Recognition on Facebook," Facebook, September 3, 2019, https://about.fb.com; Emily Birnbaum, "Supreme Court Declines to Hear Facebook Facial Recognition Case," *The Hill*, January 21, 2020, https://thehill.com; Sigal Samuel, "Facebook Will Finally Ask Permission Before Using Facial Recognition on You," *Vox*, September 4, 2019, https;//vox.com.

[34] Kashmir Hill and Aaron Krolik, "How Photos of Your Kids Are Powering Surveillance Technology," *New York Times*, October 11, 2019, https://nytimes.com.

[35] Bianca Bosker, "Facial Recognition: The One Technology Google Is Holding Back," *HuffPost*, updated December 6, 2017, https://googleusercontent.com; Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020, https://nytimes.com.

[36] Kashmir Hill, "The Secretive Company." See also Allison Ross, Malena Carollo, and Kathryn Varn, "Florida cops use this facial recognition tech that could be pulling your pics," *Tampa Bay Times*, February 11, 2020.

[37] Darren Byler, "China's hi-tech war."; Amy Qin, "Facial Recognition."; Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *New York Times*, July 8, 2018, https://nytimes.com. Granted, there are limitations associated with this kind of widespread use. Harrison Jacobs, "China's 'Big Brother' surveillance technology isn't nearly as all-seeing as

observers, governments of other countries have also explored expanded use of facial recognition.[38]

Even when used justly, facial recognition technology may affect people unequally due to design flaws and overbroad applications. Generally, objections relating to design and applications center on inaccuracy, bias, disproportionate data, constitutional rights, and criminal procedure.

Inaccuracy. Critics raise concerns about inaccuracies associated with facial recognition technology, which, as currently deployed in law enforcement contexts, could result in false arrests. Experts generally divide inaccuracies into two categories: false negatives and false positives. A **false negative** describes a search that yields no matches even though a true match *does* exist within the database. A **false positive** describes a search that yields an incorrect match despite whether or not a true match exists within the database.[39] Both outcomes can become more prevalent as the underlying database expands to include more people.[40] This dilemma has already posed problems for the Chinese government, whose watch list of some 20 million people is simply "too many people for today's facial recognition technology to parse," according to experts.[41]

Even in smaller populations, facial recognition technologies do not meet clear standards of accuracy. As recent as 2016, the FBI reported an accuracy rate of 85 percent for its systems. This figure does not mean that the FBI's systems positively identified the correct person in 85 percent of real-life searches. Instead, it means that in 85 percent of searches conducted within a controlled database, the correct person was included among "a candidate list of 50 potential matches," ranked according to the strength of the match score. However, the correct person could be listed as the forty-ninth match in such a list for the search to be categorized as accurate. This classification is problematic, given that law enforcement agencies sometimes run searches with much shorter candidate lists.[42] Moreover, a survey of local law enforcement agencies conducted in 2015–16 revealed that few contractually obligate private facial recognition vendors to meet high standards of accuracy.[43]

Bias. Under the umbrella of broader concerns about inaccuracy, there is overwhelming evidence that facial recognition systems recognize certain faces better than others. In

the government wants you to think," *Business Insider*, July 15, 2018, https://businessinsider.com.

[38] The government of New South Wales (in southeastern Australia) recently rolled out a system designed to match official identification photos to footage from CCTV. The same system may eventually be used to match face images of unknown suspects to photos within existing government databases. Nigel Gladstone, "Surveillance state: NSW intensifies civilian tracking," *Sydney Morning Herald*, November 4, 2018, https://smh.com.au.

[39] "Face Recognition," Electronic Frontier Foundation, last accessed November 2, 2018, https://eff.org.

[40] "Face Recognition," Electronic Frontier Foundation.

[41] Paul Mozur, "Inside China's Dystopian Dreams."

[42] U.S. Government Accountability Office, "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy," 26–7.

[43] Of the police departments it surveyed, the Center on Privacy & Technology found only one "that conditioned purchase of technology on accuracy tests or thresholds." Garvie et al., "The Perpetual Line-Up," 3.

brief, human beings more accurately identify faces that resemble their own—especially with respect to skin color—and this tendency has carried over to computers through human-made algorithms. Scientists have found, for example, that facial recognition algorithms created in East Asia are more capable of correctly identifying Japanese, Chinese, or Korean faces than French, German, or American ones.[44] In the United States, where a plurality of tech industry workers are white and male, facial recognition systems are more likely to correctly identify white, male faces.[45] Additionally, systems learn from training sets of face images, but these training sets may not accurately reflect the demographic makeup of the population at large.[46] Whatever the cause, researchers have concluded that systems in use today produce less accurate results for women, black people, and people in their 20s.[47] The ACLU drew attention to these inaccuracies by processing the faces of members of Congress within a mugshot database using Amazon's Rekognition tool—the query produced disproportionate false positives among black members.[48]

Disproportionate data. Errors result not only from algorithmic flaws, but also from disproportionate representation of certain groups within mugshot databases. Recall that the potential for false positives and false negatives increases as a photo database grows. Accordingly, a larger number of black faces within a database heightens the possibility that searches for black faces will produce erroneous matches. Black men are overrepresented within existing mugshot databases, rendering them "more 'findable,'" but simultaneously more likely to be incorrectly identified.[49] Critics like the ACLU warn that together, bias and database overrepresentation would render black men the prime targets of facial recognition technology.[50]

Constitutional rights. Another area of objection centers around First and Fourth Amendment rights. Detractors of facial recognition technology say that widespread implementation of this technology by government entities could have a chilling effect on free speech and free association by prompting Americans to reconsider their participation

[44] Scientists often refer to this phenomenon as the "other-race effect." P. Jonathon Phillips, "An Other-Race Effect for Face Recognition Algorithms," *ACM Transactions on Applied Perception* 14 (2011), 1–13: 1.

[45] For statistics on tech industry demographics, see Garvie et al., "The Perpetual Line-Up," 87.

[46] For this reason, some researchers suggest that companies creating new face recognition systems "train face recognition algorithms on datasets that are evenly distributed across demographics, as this approach offers consistently high accuracy across all cohorts." Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge, and Anil K. Jain, "Face Recognition Performance: Role of Demographic Information," *IEEE Transactions on Information Forensics and Security* 7 (December 2012), 1789–1801.

[47] Klare et al., "Face Recognition Performance," 1789–1801. See also Mei Ngan and Patrick Grother, "Face Recognition Vendor Test (FRVT) Performance of Automated Gender Classification Algorithms," (National Institute of Standards and Technology, April 2015), http://dx.doi.org/10.6028/NIST.IR.8052. See also Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018), 1–15.

[48] Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," *ACLU*, July 26, 2018, https://aclu.org.

[49] Garvie et al, "The Perpetual Line-Up," 56.

[50] Snow, "Amazon's Face Recognition."

in myriad forms of public dissent.[51] They point to the fact that law enforcement agencies have already relied on this technology to identify rioters.[52] Legal scholars have raised questions about the lawfulness of searches and seizures that rely on facial recognition technology. Professor Elizabeth Joh of the University of California, Davis School of Law notes that certain U.S. Supreme Court decisions "[suggest] that any 'scientific enhancement' of the senses used by the police to watch activity falls outside of the Fourth Amendment's protections if the activity takes place in public."[53] That said, some justices have expressed apprehension about law enforcement's use of "novel modes of surveillance" that may "[chill] associational and expressive freedoms," as Justice Sonia Sotomayor put it in her concurring opinion in *United States v. Jones*.[54]

Criminal procedure. Ideological objections aside, critics have raised questions about how courts should address facial recognition technology, especially in the context of criminal investigations and trials. Should prosecutors be required to disclose to judges and jurors when or how law enforcement officers relied on these kinds of searches to identify a suspect? Likewise, should prosecutors be required to provide information about failed or inconclusive searches to defense attorneys, as they are required to do with exculpatory evidence?[55] Few if any standards currently guide the disclosure of information about law enforcement agencies' use of facial recognition technology. And as some recent cases illustrate, crime lab analysts are not necessarily well prepared to explain to juries how facial recognition technology works and how accurate results may be.[56]

Existing regulations

Federal laws are mostly silent on facial recognition technology, and most states have not enacted comprehensive regulations. For example, Wisconsin laws do not define this technology or establish general parameters for its public or private use. That said, some states have enacted piecemeal legislation to authorize or restrict the use of facial recognition technology by certain entities or for certain purposes. Of these, most regulation has occurred in the area of law enforcement. A second subset of regulations relates to

[51] Garvie et al., "The Perpetual Line-Up," 42–43.

[52] According to vendor Geofeedia, the Baltimore County Police Department employed its services to "run social media photos through facial recognition technology to discover rioters with outstanding warrants and arrest them directly from the crowd." Geofeedia, "Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots," promotional materials, accessed November 28, 2018, https://aclunc.org.

[53] Elizabeth E. Joh, "Policing By Numbers: Big data and the Fourth Amendment," *Washington Law Review* 35 (2014), 35–68: 60.

[54] United States v. Jones, No. 10-1259 at 2 (U.S. Jan. 23, 2012).

[55] Garvie et al., "The Perpetual Line-Up," 59. In *Brady v. Maryland* (1963), the U.S. Supreme Court ruled that suppression of exculpatory evidence constituted denial of due process under the Fourteenth Amendment. "Brady v. Maryland," Oyez, accessed January 31, 2020, http://oyez.org.

[56] See, for example, the case of Willie Lynch. Benjamin Conarck, "How a Jacksonville man caught in the drug war exposed details of police facial recognition," *Florida Times Union*, May 26, 2017.

identity verification in other government-related contexts, and a final subset addresses face images as a subset of consumer data writ large.

Law enforcement. At the federal level, existing laws require the FBI to provide public notices and privacy impact assessments relating to its data collection practices, including facial recognition searches under NGI-IPS and the FACE Services unit.[57] However, the Government Accountability Office found in 2016 that the FBI failed to meet these requirements in a "timely manner" and had not determined with "reasonable assurance" whether deployments of this technology "help enhance, rather than hinder, criminal investigations."[58] Nonetheless, no other federal laws place substantial restrictions on these deployments.

At the state level, recently enacted laws generally define and establish parameters for law enforcement use of facial recognition technology. Many of these laws concern facial recognition used with other technologies. For example, at least three states limit or prohibit law enforcement use of facial recognition technology on footage obtained from body cameras.[59] Of these, California law begins with the assertion that "biometric surveillance would corrupt the core purpose of officer-worn body-worn cameras by transforming those devices from transparency and accountability tools into roving surveillance systems."[60] Other state laws address surveillance with respect to unmanned aerial aircraft, or drones. Vermont law prohibits facial recognition technology from being used on any person on the basis of information collected by a drone, except for an authorized target of surveillance,[61] and Maine law directs a state board to develop restrictions on facial recognition technology in tandem with drones.[62]

Other state laws codify or restrict law enforcement's use of DMV databases. Texas law authorizes the DMV's use of "image verification" to eliminate driver's license fraud, as well as to "aid other law enforcement agencies in . . . establishing the identity of a victim of a disaster or crime . . . or conducting an investigation of criminal conduct."[63] By contrast, Washington law imposes limits on disclosure of DMV facial recognition search results to law enforcement, such as requests authorized by a court order and investigations of driver's license fraud.[64] Although no state legislature has enacted laws relating to law enforcement use of commercial databases, the New Jersey attorney general issued

[57] These requirements exist under the Privacy Act of 1974 and the E-Government Act of 2002. Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation (May 2019), 17–18, http://eff.org. The most recently issued privacy impact reports are available here: Federal Bureau of Investigation, "Department of Justice/FBI Privacy Impact Assessments (PIAs)," accessed February 13, 2020, http://fbi.gov.

[58] U.S. Government Accountability Office, "Face Recognition Technology."

[59] Cal. Penal Code § 832.19 (b); N.H. Rev. Stat. Ann. § 105-D:2.; and Or. Rev. Stat. § 133.741 (1) (b) (D).

[60] 2019 Cal. AB 1215.

[61] Vt. Stat. Ann. tit. 20, § 4622 (d) (2).

[62] Me. Rev. Stat. tit. 25 § 4501.5.D.

[63] Tex. Transp. Code § 521.059.

[64] Wash. Rev. Code § 46.20.037.

an order in January 2020 to halt law enforcement agencies' use of Clearview AI in that state.[65]

As an outlier, one Illinois law appears to indirectly facilitate law enforcement use of facial recognition technology. The same legislation that legalized recreational marijuana, effective January 2020, requires security precautions to be implemented at dispensaries, including cameras "angled to allow for facial recognition . . . of any person entering or exiting the dispensary area."[66] These provisions appear to address—and attempt to preempt—dispensaries' vulnerability to theft and other crimes.

For their part, various law enforcement agencies have self-regulated and devised policies to codify their deployment of facial recognition technology.[67] However, where these policies exist, few restrict use of the technology to monitor protected forms of assembly or free speech, or instruct officers to remove from their databases the face images of people who were never charged or not convicted.[68] None require officers to obtain a warrant prior to running a search of a person's face.[69] Finally, only a small minority of departments share these policies with the general public.[70]

Other public uses. The second most significant area of state regulation concerns identity verification in other public or government-related contexts. For example, Connecticut and Maine laws authorize DMV use of facial recognition technology to verify identities and prevent fraud. A handful of states have enacted laws that authorize the technology's use as a form of legal identity verification for notaries.[71] Illinois law requires school districts that collect biometric information to adopt policies that require, at minimum, use of biometric data "solely for identification or fraud prevention," as well as written permission from legal guardians and eventual destruction of data.[72] Conversely, some states expressly prohibit use of the technology for identity verification purposes in certain contexts, such as the DMV[73] or in relation to autopsies.[74]

Notably, some municipalities have opted to establish broad prohibitions on the use of facial recognition technology by local government entities. San Francisco was the first

[65] Kashmir Hill, "New Jersey Bars Police From Using Clearview Facial Recognition App," *New York Times*, Jan. 24, 2020.

[66] 410 Ill. Comp. Stat. § 705/15-100.

[67] Garvie et al, "The Perpetual Line-Up," 37.

[68] According to the report, all but one of the agencies that were surveyed (the Ohio Bureau of Criminal Investigation) failed to spell out restrictions on use of the technology "to track individuals engaging in political, religious, or other protected free speech." Garvie et al, "The Perpetual Line-Up," 3. Additionally, only one agency (the Michigan State Police) instructed officers to remove the faces of people who were not charged or convicted. Garvie et al, "The Perpetual Line-Up," 26. See also Mich. Comp. Laws Ann § 28.243.

[69] Garvie et al, "The Perpetual Line-Up," 37.

[70] Those included agencies in Honolulu, San Diego, Seattle, and the state of Michigan. Garvie et al, "The Perpetual Line-Up," 59–60.

[71] Mont. Code Ann. § 1-5-602; Nev. Rev. Stat. Ann. § 133.085; and Utah Code Ann. § 46-1-2.

[72] 105 Ill. Comp. Stat. § 5/10-20.40 and 105 Ill. Comp. Stat. § 5/34-18.34.

[73] Conn. Gen. Stat. § 17b-30; Me. Rev. Stat. tit. 29-A, § 1401; and N.H. Rev. Stat. Ann. § 263:40-b.

[74] N.D. Cent. Code § 44-04-18.18 and S.C. Code Ann. § 17-5-535.

municipality to ban use of the technology by the government, doing so in May 2019.[75] Oakland, California, and Somerville, Massachusetts, followed soon after.[76]

Consumer data. Finally, a small minority of states have enacted data privacy laws that affect face image data as a subset of personal consumer data. These laws generally restrict private companies' use of consumer data and establish customers' rights over their data.[77] The California Consumer Privacy Act, effective January 2020, requires businesses to disclose information about the personal data they collect about consumers and the purposes for which they collect that data.[78] The act also establishes the consumer's right to request deletion of personal data and to opt out of third-party commercial use of personal data.[79] Under Illinois' Biometric Information Privacy Act, which was enacted in 2008, companies may not disclose or disseminate biometric information about a customer without the customer's consent. The act creates a private right of action against companies violating this requirement.[80] Consequently, various class-action lawsuits have been filed, including one against Facebook for its use of facial recognition technology to tag individuals in photos without their consent. (This case applied only to Facebook users in Illinois.)[81] In January 2020, Facebook announced a $550 million settlement that its critics consider "a major victory."[82] Although the Illinois law has posed a considerable obstacle to social media companies' use of facial recognition tools, other state-level data privacy laws are considerably limited by comparison.[83]

Proposed regulations

Like existing state and federal laws, other proposed legislation often relates to law enforcement, other public uses, and consumer data privacy.

[75] Kate Conger, Richard Fausset and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *New York Times*, May 14, 2019, https://www.nytimes.com/.

[76] Graham Vyse, "Cities Ban Government Use of Facial Recognition," *Governing*, July 24, 2019, https://www.governing.com/; Jason Tashea, "As facial recognition software becomes more ubiquitous, some governments slam on the brakes," *American Bar Association Journal*, Sep. 24, 2019, http://www.abajournal.com/.

[77] These laws generally resemble European data protection regulations that went into effect in May 2018. For a useful summary, see Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *New York Times*, May 24, 2018, https://www.nytimes.com/.

[78] California's law applies only to a business that meets at least one of the following three criteria: (1) has annual gross revenues over $25 million, (2) receives personal information of 50,000 consumers or more annually, or (3) derives 50 percent or more of annual revenues from selling consumers' personal information.

[79] Cal. Civ. Code § 1798.100 to 1798.199. The act defines "unique biometric" data to exclude photographs, except for those "used or stored for facial recognition purposes," per section 1798.29.

[80] Damages specified are $1,000 or $5,000 for negligently or intentionally disclosing data without consent 740 Ill. Comp. Stat. § 14/.

[81] Sasha Ingber, "Users Can Sue Facebook Over Facial Recognition Software, Court Rules," *NPR*, August 8, 2019, https://www.npr.org/.

[82] Natasha Singer and Mike Isaac, "Facebook to Pay $550 Million to Settle Facial Recognition Suit," *New York Times*, January 29, 2020, https://nytimes.com.

[83] The National Conference of State Legislatures provides a useful synopsis of private sector data security laws that includes a table of proposed and enacted laws. NCSL, "Data Security Laws—Private Sector," last updated May 29, 2019, https://ncsl.org; NCSL, "2019 Consumer Data Privacy Legislation," last updated January 3, 2020, https://ncsl.org.

Law enforcement. Similar to the enacted legislation discussed above, several introduced proposals would limit use of facial recognition technology in tandem with police body cameras[84] or drones.[85] On the other end of the spectrum, one bill introduced in New Jersey would integrate the technology with vehicle dash cameras.[86] Another notable subset of introduced bills concerns transparency and oversight, requiring law enforcement agencies to develop detailed policies around facial recognition or obtain approval prior to its use.[87] Other proposals authorize or prohibit facial recognition searches under certain circumstances. For example, various bills would restrict use of the technology to conduct real-time surveillance,[88] and others would limit access to DMV databases.[89] Under Maryland 2017 HB 1148, authorized purposes would include identification of missing, incapacitated, or deceased persons, as well as victims of crime.

Other public uses. A Minnesota bill authorizes the use of facial recognition technology at the DMV.[90] Legislation in New York would prohibit the use of the technology in elementary and secondary schools.[91] Additionally, lawmakers in New York and Washington have introduced bills to prohibit the use of facial recognition in housing.[92]

Consumer data privacy. Legislators in several states have introduced data privacy legislation in the same vein as California's and Illinois's laws.[93] For example, a Vermont bill provides specific requirements for how a business must inform consumers about data collection, including a "clear and conspicuous physical sign at the entrance of a business location."[94] Another bill introduced in Rhode Island requires any private entity that collects biometric data, including face images, to obtain written consent and provide information about data storage and use policies.[95]

Beyond the categories listed above, state legislators have also introduced bills that

[84] S06776, 2019–2020 Reg. Sess. (N.Y. 2019); H. 4709, 123rd Sess. (S.C. 2019); and H. 2120, 191st Gen. Court (Mass. 2019). Similar bills have been proposed at the federal level: H.R. 120, 116th Cong. (2019) and H.R. 3364, 116th Cong. (2019).

[85] H.F. 1236, 91st Leg., 2019–2020 Sess. (Minn. 2019); A04030, 2019–2020 Reg. Sess. (N.Y. 2019); A06435, 2019–2020 Reg. Sess. (N.Y. 2019); S. 1447, 191st Gen. Court (Mass. 2019); and S. 1446, 191st Gen. Court (Mass. 2019).

[86] A2489, 218th Leg. (N.J. 2018).

[87] H.B. 1238, 2020 Sess. (Ind. 2020); H.B. 2761, 66th Leg., 2020 Reg. Sess. (Wash. 2020). Another bill, A1210, 219th Leg. (N.J. 2020), would require a public hearing as part of this approval process.

[88] Certain bills carve out exceptions for emergency situations: S.B. 0342 (Mich. 2019); S.B. 6280, 66th Leg., 2020 Reg. Sess. (Wash. 2020); and H.B. 1148 (Md. 2017). Similarly, at the federal level, H.R. 4021, 116th Cong. (2019) and S. 2878, 116th Cong. (2019) would require a court order to be obtained in order to use the technology.

[89] H.B. 2446, 66th Leg., 2020 Reg. Sess. (Wash. 2020); S.B. 2269, 101st Gen. Assemb., 2019–2020 Sess. (Ill. 2019); and H.B. 1700, 2020 Sess. (Va. 2020).

[90] H.F. 487, 91st Leg., 2019–2020 Sess. (Minn. 2019).

[91] A01692, 2019–2020 Reg. Sess. (N.Y. 2019); A06787, 2019–2020 Reg. Sess. (N.Y. 2019); S05140, 2019–2020 Reg. Sess. (N.Y. 2019); and A08373, 2019–2020 Reg. Sess. (N.Y. 2019).

[92] The Washington bill applies only to rental units receiving government assistance, while the New York bill applies to all landlords. S05687, 2019–2020 Reg. Sess. (N.Y. 2019); A07790, 2019–2020 Reg. Sess. (N.Y. 2019); and H.B. 2760, 66th Leg., 2020 Reg. Sess. (Wash. 2020). At the federal level, H.R. 4008, 116th Cong. (2019) would prohibit the use of the technology in federally funded public housing projects.

[93] NCSL, "2019 Consumer Data Privacy Legislation."

[94] H. 899 (Vt. 2020). See also, at the federal level, S. 847, 116th Cong. (2019).

[95] H. 5945 (R.I. 2019).

address other concerns, such as the admissibility of facial recognition search data in criminal court cases, or that impose broad prohibitions, such as public and private bans on facial recognition technology.

Criminal procedure. State legislators are beginning to address the role of facial recognition searches in criminal investigations and related court proceedings. For example, legislation introduced in Washington would prohibit using information gathered from facial recognition technology as the "sole basis to establish probable cause in a criminal investigation."[96] A Maryland bill requires the state to disclose information about the use of facial recognition technology to defendants in criminal cases.[97] Finally, South Carolina legislation would prohibit the use of data collected illegally through facial recognition technology in police body cameras from being used in court proceedings.[98]

Accuracy, bias, and oversight. Some proposals would condition government use of facial recognition systems on the creation of related accuracy standards, oversight mechanisms, and data policies. A New Jersey bill would condition use of these systems on minimum accuracy rates for certain categories of faces—i.e., age, gender, and race—in addition to defined data retention, disclosure, and access policies.[99] Similarly, proposals introduced in Washington and Massachusetts include requirements relating to bias testing, due process and privacy protections, and defined testing procedures.[100]

Broad prohibitions. Legislation introduced in Hawaii proposes a complete public and private ban on facial recognition technology, with certain exceptions for specific uses by law enforcement.[101] Portland, Oregon, is currently considering a ban on commercial and government uses of facial recognition technology.[102]

Conclusion

In July 2018, the president of Microsoft, Bradford Smith, urged Congress to regulate facial recognition—making him the first leader of a major technology company to advocate to do so.[103] As Smith reflected, "All tools can be used for good or ill," and "the more powerful the tool, the greater the benefit or damage it can cause."[104] Facial recognition

[96] H.B. 1654, 66th Leg., 2019 Reg. Sess. (Wash. 2019).

[97] S.B. 46 (Md. 2020).

[98] H. 4709, 123rd Sess. (S.C. 2020).

[99] S.B. 116, 219th Leg. (N.J. 2020).

[100] S.B. 5528, 66th Leg., 2019 Reg. Sess. (Wash. 2019); S. 1385, 191st Gen. Court (Mass. 2019); and S.B. 6280, 66th Leg., 2020 Reg. Sess. (Wash. 2020).

[101] S.B. 3148, 30th Leg. (Haw. 2020) and H.B. 2745, 30th Leg. (Haw. 2020). Similarly, at the federal level, H.R. 3875, 116th Cong. (2019) seeks to completely prohibit federal funding from being used to purchase or use the technology.

[102] Susan Crawford, "Facial Recognition Laws Are (Literally) All Over the Map," *Wired*, December 16, 2019, https://wired.com.

[103] Natasha Singer, "Microsoft Urges Congress to Regulate Use of Facial Recognition," *New York Times*, July 13, 2018, https://www.nytimes.com/.

[104] Brad Smith, "Facial recognition technology: The need for public regulation and corporate responsibility," *Microsoft on*

technology represents a potential boon to governments, making airports, schools, and city streets safer by identifying would-be terrorists, shooters, and petty thieves. Without oversight, however, the same capabilities could be used to instill fear and suppress dissent. Policymakers at all levels—local, state, and federal—stand to determine the future of facial recognition with the policies they craft in this decade. ■

the Issues, July 13, 2018, http://www.blogs.microsoft.com.