# What Is Facial Recognition?

## ITIF Technology Explainer Series • www.itif.org

Facial recognition technology has a growing number of uses: Airports use it to expedite security screening, social networks use it to organize photos, smartphones use it for logins, and law enforcement uses it to solve crimes.[1] Public policy can establish important guardrails to ensure organizations use facial recognition responsibly, while still allowing—and ideally promoting—innovative uses of the technology.

## Summary

Facial recognition technology compares images of faces in order to estimate their similarities. It is not the same as other types of technology that also analyze the face, including systems that predict a person's age, race, gender, or outward emotions.

Facial recognition systems typically perform two types of searches:

**Verification (One-to-One):** In verification comparisons, the technology compares two images to determine whether two faces are the same.

**Identification (One-to-Many):** In identification comparisons, the technology searches a database of images to find potential matches with an initial image of a face.

Facial recognition technology uses algorithms that detect faces' unique features, such as the distance between the eyes, to create a mathematical representation that determines their similarity. For example, faces shown on a given image are considered a possible match if their similarity scores meet or exceed the match threshold, which is a number the operator assigns that represents a minimum acceptable similarity score. A facial recognition system's false-positive and false-negative rates are common ways to measure its accuracy, while other metrics, such as how fast the system can perform a search, also affect its performance.[2]

Facial recognition technology can increase public safety by helping law enforcement more quickly and accurately find and identify victims, witnesses, and suspects. It can also increase security online and in person by authenticating individuals. In addition, the technology can increase convenience for consumers by helping them perform tasks ranging from quickly organizing their photos on their smartphone to boarding a plane to paying for products using their face.

## Why Now?

Computer scientists began developing technology to recognize faces in the 1960s. However, the increased use of deep convolutional neural networks, which process multiple layers of abstraction of data to identify patterns, has led to significant improvements in the accuracy of algorithms. For example, the National Institute of Standards and Technology found that identification algorithms were 100 times more accurate in 2019 than in 2010.[3] Moreover, the most accurate algorithms in 2020 fail to rank the correct candidate as the top potential match only 0.1 percent of the time when searching a database containing images of 1.6 million individuals (1 out of 1,000 times).[4] Higher-quality images from better cameras and better hardware have also improved the performance of facial recognition systems.

## Prospects for Advancement

On top of rapid progress to date, facial recognition algorithms continue to improve at a brisk pace. Indeed, algorithms that are only a year old may significantly underperform relative to newer ones. Moreover, the most accurate algorithms are increasingly tolerant of image-quality problems, such as poor illumination.[5] Similarly, the best-performing algorithms now display little to no bias across demographic groups.[6]

Facial recognition systems will likely continue to improve. However, some advocates have opposed the technology out of concerns about biased outcomes and mass surveillance, leading a number of cities to restrict the use of the technology by government. As the technology becomes more prevalent with more applications—and governments implement targeted regulation—fears about mass surveillance and biased outcomes will likely fade.

## Applications and Impact

Facial recognition systems have multiple applications:

- Public Safety: Facial recognition helps police identify victims, suspects, and witnesses to crimes. For example, it has helped authorities find and rescue human trafficking victims, and identified individuals committing crimes ranging from shoplifting and check forgery to armed robbery and murder.[7]

- Security: Businesses are using the technology to improve security in several ways. For example, credit card companies such as Visa and Mastercard have launched services that allow customers to use selfies to verify the authenticity of online purchases.[8]

- Convenience: Businesses are using facial recognition to increase convenience for consumers, including by helping travelers get through airports faster. For example, in a test at the Los Angeles International Airport, facial recognition reduced by half the time it typically takes to board a plane.[9] Facial recognition can also be used to allow individuals entry into gyms, schools, apartments, and office buildings.

- Accessibility: Facial recognition improves the accessibility of online services, and can help visually impaired individuals better understand their surroundings. For example, Facebook uses the technology to make its platform more accessible by automatically adding descriptive text to photos, which screen readers can read aloud.[10]

## Policy Implications

There are four essential policy implications to implementing facial recognition. First, governments should minimize potential abuse of the technology, including by law enforcement. The standard of probable cause for law enforcement to make arrests already protects individuals from adverse outcomes resulting from false-positive matches. But other policies could provide additional protections. For example, policymakers should require that law enforcement obtain a search warrant to use any technology to surveil an individual for an extended period.

And policymakers should set standards for when the government may use facial recognition in sensitive environments, such as at protests, and require law enforcement to develop data-retention policies for images used in facial recognition systems. Finally, policymakers should encourage law enforcement to pilot the technology, which can help it evaluate how the technology performs in its communities, and fund training to teach law enforcement how to use the technology properly.

Second, governments should only use highly accurate facial recognition systems and set performance standards for facial recognition systems their agencies procure. Several organizations provide facial recognition systems that are accurate across demographic groups.[11]

Third, governments should not ban facial recognition because doing so would inhibit positive uses of the technology. For example, a ban would prohibit using facial recognition to create a biometric entry/exit system, which the 9/11 Commission concluded was crucial to U.S. national security.[12]

Fourth, governments should support the development and use of facial recognition in the private sector. For example, by passing legislation to create a national privacy framework that streamlines regulation, preempts state laws, and establishes basic consumer data rights, lawmakers can protect consumer privacy while minimizing the impact on innovation. Governments should also continue to fund independent testing of commercial facial recognition systems, and fund the development of diverse datasets of faces to foster further algorithmic improvements.[13]

[1] 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/; “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/.

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

[3] Ibid.

[4] Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 2: Identification” (Washington, D.C.: National Institute of Standards and Technology, March 2020), 48, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

[5] Ibid.

[6] 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.

[7] 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; “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/.

[8] Banco Neon, “Fighting fraud with a smile,” Visa, n.d., accessed January 12, 2020, https://usa.visa.com/visa-everywhere/security/fighting-fraud-with-a-smile.html; “Mastercard and BMO make Fingerprint and ‘Selfie’ Payment Technology a Reality in North America,” Mastercard, October 24, 2016, https://newsroom.mastercard.com/press-releases/mastercard-and-bmo-make-fingerprint-and-selfie-payment-technology-a-reality-in-north-america/; Daniel Castro, Hearing before the House Committee on Oversight and Reform, January 15, 2020, on “Facial Recognition Technology (Part III): Ensure Commercial Transparency & Accuracy,” http://www2.itif.org/2020-commercial-use-facial-recognition.pdf?_ga=2.162517758.313082901.1583169240-354924416.1550612241.

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

[10] “What is the face recognition setting on Facebook and how does it work?” Facebook, n.d., accessed January 12, 2020, https://www.facebook.com/help/122175507864081; Kyle Wiggers, “Microsoft’s Project Tokyo Helps Visually Impaired Users ‘See’ With AI and AR,” *VentureBeat*, January 28, 2020, https://venturebeat.com/2020/01/28/microsofts-project-tokyo-helps-visually-impaired-users-see-with-ai-and-ar.

[11] Ibid.

[12] “What to Do? A Global Strategy in Final Report of the National Commission on Terrorist Attacks Upon the United States,” in *National Commission on Terrorist Attacks Upon the United States*, 2004, 389 https://govinfo.library.unt.edu/911/report/911Report_Ch12.pdf.

[13] Daniel Castro and Joshua New, “Comments to OMB on Federal Data and Models for AI R&D” (Center for Data Innovation), August 9, 2019, https://s3.amazonaws.com/www2.datainnovation.org/2019-omb-federal-data-models-rfi.pdf.

## Recommended Reading

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).

Daniel Castro, “Note to Press: Facial Analysis Is Not Facial Recognition” (Information Technology and Innovation Foundation, January 27, 2019).

“NIST Report on Facial Recognition: A Game Changer” (International Biometrics + Identity Association, February 14, 2020).

Yevgeniy Sirotin, “‘Bias’ in Face Recognition: Some Facts.” *LinkedIn*, October 16, 2019.

Michael McLaughlin, Hearing before the California State Assembly Privacy and Consumer Protection Committee and the Assembly Select Committee on Emerging Technologies and Innovation on “Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges” (Information Technology and Innovation Foundation, March 10, 2020).

“Face Facts: Dispelling Common Myths Associated with Facial Recognition Technology” (Security Industry Association), accessed March 5, 2020.