Facial Recognition in Law Enforcement

Joseph DiMartino

University of Tampa, Department of Computer Science

The rapid advancement of Artificial Intelligence (AI) has brought many new opportunities were unimaginable only a few years ago. Innovations in facial recognition technology now sparks debate over whether it should be used in public spaces and if law enforcement should have access to this data. To fully understand the implications of law enforcement agencies using facial recognition technology, it's essential to learn about how it works and its capabilities.

Facial recognition technology in simple terms is [1] a way for a computer to confirm who an individual is in real time. Facial recognition can be used to identify individuals either in photos, videos, and even real time surveillance. The technology will first [2] "read" the image/video and will "look" at the geometry of someone's face. Then, to put a name to the face, the technology will search through a database of known faces. If the AI determines that the face is similar enough to the face in the database, a match is found, and the person is recognized. In many cases, the AI will show a box around a person's face as it tries to identify the person and a name on the top of the box will be added if the person is identified.

Facial recognition technology is only possible with computer vision. [3] Computer vision is a field of AI that utilizes neural networks and machine learning. The computer vision model is trained to create meaningful information from any digital input such as image or video. Computer vision requires huge amounts of data to accurately make predictions whether something that the computer "sees" is actually that item or person. Facial recognition technology is a specific subset of computer vision where the computer attempts to match a specific person with a face in the database, as mentioned earlier. Without proper data, the technology would not be accurate. For example, if an ATM camera only sees a person's face from an upwards angle, the database would

---

[1] Amazon Web Services, "What is facial recognition?" AWS, 2025. [Online]. Available: https://aws.amazon.com/what-is/facial-recognition/. [Accessed: Mar. 24, 2025].
[2] Microsoft Azure, "What is face recognition?" Microsoft, 2025. [Online]. Available: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-face-recognition/. [Accessed: Mar. 24, 2025].
[3] IBM, "Computer vision," IBM, 2025. [Online]. Available: https://www.ibm.com/think/topics/computer-vision. [Accessed: Mar. 24, 2025].

most likely need an image of the persons face that's similar in order to determine a match. In the example from the IBM article, to identify a tire from a photo, the computer vision model must be trained on a large number of tire images without any defects to learn how to determine if something is or is not a tire. All computer vision models are very specific and can only identify whether or not something is that item, facial recognition takes it a step further by processing whether or not someone's identity can be verified.

Facial recognition technology can take many forms. It can be applied to saved surveillance videos such as recordings from ATM machines or used in real time in the body camera of a police officer patrolling the streets. The diversity of facial recognition technology raises many questions over the benefits of its use and possible risks as the technology grows.

Many law enforcement agencies are using facial recognition technology in their investigations. Many [4] U.S. law enforcement agencies have used AI in their investigations, such as the FBI, DEA, U.S. Secret Service, and Homeland Security Investigations. The earliest dates back to 2018 and not all of these agencies are using the technology currently. According to the Government Accountability Office, these agencies were under investigations on how the AI was being used, how officials were being trained to use this technology, and if they in anyway violated an individual's First Amendment rights. As the technology was being used it was not limited to the identification of those involved in doing a crime but also tracking missing persons.

As this AI technology gets more and more advanced, we can expect it to become capable of much more than just reading a face and returning a name. With enough surveillance cameras, an individual can be tracked in real-time as they move throughout a space where camera have the capability of recognizing them. Facial recognition technology can move further and analyze an individual's data to predict when and where they will be at a place, read their license plates to enhance tracking capabilities, and even track those you're associated with. As we make the argument for and against law enforcement using this technology, we must also consider what types of advancements will be made and what restrictions would need to be put in place if law enforcement is granted facial recognition capabilities.

Whether or not law enforcement agencies have the right to both use facial recognition technology in public as well as store our facial data is up for debate. Those who are against law enforcement using this technology prioritize [5] privacy concerns,

---

[4] U.S. Government Accountability Office, "Facial recognition technology: Privacy and accuracy issues," GAO-24-107372, 2024. [Online]. Available: https://www.gao.gov/products/gao-24-107372. [Accessed: Mar. 24, 2025].

[5] E. M. Chapman, "Police surveillance and facial recognition: Why data privacy is an imperative for communities of color," *Brookings Institution*, 2025. [Online]. Available: https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/. [Accessed: Mar. 24, 2025].

make arguments about the infringement of their rights, and fear potential biases against certain groups. Those who stand for this technology are more concerned [6] about public safety and reduction of human error within the court process.

For Position:

Facial recognition technology can be a very powerful tool for law enforcement to utilize. The use of this technology can help enhance public safety, expedite criminal investigations, and improve the accuracy of criminal trials. Even today, many local, state, and federal law enforcement agencies are using facial recognition technology. There are many different ways these agencies utilize this technology [7] including inserting an image from surveillance cameras into a database of faces, confirm the identity of suspects from using their face in comparison to one in a database, flag wanted individuals in public spaces, and even unlock a suspect's device if it requires face ID.

Confirming the identity of a suspect of a crime is a huge step in ensuring accurate and fair trials for alleged criminals. One way we all experience facial verification is at TSA [8], where we give our ID and stand in front of a camera for confirmation on whether we're the person on the ID or not. In this case, the facial verification technology improves travel safety, increases convenience for travelers by being faster to confirm identities than traditional methods, and provides more accurate results with the highest performing matching algorithms. This verification technology is also useful for one-to-one matching for suspects, meaning that if a suspect is caught on a camera at a crime scene and eventually gets taken into custody, police can compare the two and verify if they're the same person [9] This can strengthen a case to see if a person is the actual criminal or not, as well as allow for innocent people stay away from false allegations.

Safety is a huge concern for many of us, especially when we're in public spaces. The use of facial recognition technology being used at large gatherings can be utilized to scan the crowd and possibly identify suspects. The human eye may find it difficult to find a wanted individual if they're trying to evade detection in a crowd, but an elevated camera utilizing facial recognition technology would have less of an issue locating

---

[6] C3.ai, "C3 AI for law enforcement," C3.ai, 2025. [Online]. Available: https://c3.ai/products/c3-law-enforcement/. [Accessed: Mar. 24, 2025].
[7] ACE, "Understanding the Debate on Facial Recognition Technology in Policing: Pros, Cons, and Privacy Concerns," *ACE USA*, Mar. 6, 2024. [Online]. Available: https://ace-usa.org/blog/research/understanding-the-debate-on-facial-recognition-technology-in-policing-pros-cons-and-privacy-concerns/
[8] Transportation Security Administration, "Facial Recognition Technology," *TSA*, [Online]. Available: https://www.tsa.gov/news/press/factsheets/facial-recognition-technology. [Accessed: Apr. 7, 2025].
[9] E. Sullivan, "Facial Recognition Technology: Verification vs. Identification," *Montana State Legislature*, Nov. 2021. [Online]. Available: https://archive.legmt.gov/content/Committees/Interim/2021-2022/Economic%20Affairs/Meetings/November%202021/Facial-verification-vs-facial-identification.pdf

where this person is [10]. These individuals being identified can have a range of backgrounds, from those with an outstanding warrant to any unknown suspect seen at a different crime scene. Additionally, this can be used as a disaster prevention mechanism. Terrorism is becoming more and more common in large gatherings, and it's in the publics best interests to let law enforcement utilize facial recognition technology to decrease reaction time and identify attackers before they can strike.

Against position:

Those who argue for the use of facial recognition technology used in law enforcement share common themes of security and consistency. However, allowing law enforcement to use this technology can actually increase the error rate in identifying suspects. Specifically, facial recognition can be trained to be racially biased [11] and have been known to have higher error rates with minorities. Unfortunately, the technology seems to have the highest error rate with black women at about 35 percent. For a technology to be so uncertain, we cannot possibly think to allow law enforcement to use it on a daily basis, especially when it can be used as evidence against suspects. Christopher Galtin and Jason Vernau are two victims of the misuse of facial recognition technology [12]. Both men were wrongfully identified by facial recognition technology in St. Louis and Miami, causing them both to be falsely put in jail despite having readily available evidence to prove their innocence. Despite this, they were still held in jail because of the match by the facial recognition technology. These two men are only a small fraction of the growing list of individuals taken into custody by police because of false identification, a vast majority in this list being black. Despite federal testing and acknowledgement of bias [13], law enforcement continues to use this technology. In an article by the National Institute of Standards and Technology, the rise in error rate for certain demographics were noted as something to be evaluated for bias. Although facial recognition technology has potential to allow for more fair trials and allow law enforcement to better identify suspects, we still have a lot of improvements to make until we get to the point of using it in real-world cases and have it for everyday use.

---

[10] Aware, Inc., "Facial Recognition & Law Enforcement – The Value Proposition," *Aware Blog*, Feb. 16, 2023. [Online]. Available: https://www.aware.com/blog-facial-recognition-used-in-law-enforcement/. [Accessed: Apr. 7, 2025].
[11] N. Hassanin, "Law professor explores racial bias implications in facial recognition technology," *University of Calgary News*, Aug. 23, 2023. [Online]. Available: https://ucalgary.ca/news/law-professor-explores-racial-bias-implications-facial-recognition-technology
[12]M. Guariglia, "Police Use of Face Recognition Continues to Wrack Up Real-World Harms," *Electronic Frontier Foundation*, Jan. 15, 2025. [Online]. Available: https://www.eff.org/deeplinks/2025/01/police-use-face-recognition-continues-wrack-real-world-harms
[13] P. Grother, M. Ngan, and K. Hanaoka, "Face Recognition Technology Evaluation (FRTE) Part 1: Verification," National Institute of Standards and Technology, Mar. 2025. [Online]. Available: https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf

The invasiveness of facial recognition technology can also reduce public safety, by making people less secure than they would be without law enforcement using it. Data security is one of the biggest concerns when it comes to the government collecting our faces and storing them in remote places. Sure, the government grabbing data and storing our information might not be something out of the ordinary, except for the fact that unlike passwords and credit card information, we cannot encrypt our faces [14]. From this, hackers have the ability to get ahold of our facial data and increase the potential for identity theft, stalking, and harassment. In a world that becomes more and more reliant on face ID, such as for unlocking our phones, this possesses a serious risk of privacy violations and large-scale data breaches.

While facial recognition technology also continues to grow, not all individuals are willing to surrender something so personal as their face to these surveillance systems. Privacy is a huge concern for many Americans, some going as far as saying the use of facial recognition technology in public spaces goes against our first amendment right [15]. To lose all sense of anonymity every time you go outside is a troubling reality, which may become a reality soon as we allow an increasing number of law enforcement agencies to use facial recognition technology.

We would need an extraordinary amount of public trust in law enforcement agencies to comfortably give them our faces without any question. In 2021, [16] a bill was introduced to the New York State legislative session to safeguard individual privacy and restrict agencies who collect facial recognition data from releasing and distributing it to third parties. This bill also prohibits the collection of facial images and sharing these images without any court-issues authority, restricts the use of surveillance systems in public spaces, and excepts the distribution if specific lawfully obtained pieces of evidence to other law enforcement agencies if it is a part of a criminal investigation. This unique bill is the only one ensuring our collected facial data is safe from being spread to unwanted individuals or agencies. Not only has this bill not been passed yet, but it would only apply to New York state agencies and departments, keeping us vulnerable to the various other law enforcement agencies using this technology as we speak.

---

[14]A. M. Bedoya, "You Cannot Encrypt Your Face," *The Atlantic*, May 5, 2017. [Online]. Available: https://www.theatlantic.com/technology/archive/2017/05/you-cannot-encrypt-your-face/524073/

[15] H. Lacey, "Face Value," *Law Week Colorado*, May 8, 2017. [Online]. Available: https://www.lawweekcolorado.com/article/face-value-2/

[16] T. Abinanti, “Assembly Bill A4916: Prohibits the state, state agencies and departments and contractors doing business with the state, its agencies or departments from retaining facial recognition images or sharing such images with third parties without legal authorization by a court,” New York State Assembly, Feb. 8, 2021. [Online]. Available: https://www.nysenate.gov/legislation/bills/2021/A4916