International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 4, Jul-Aug 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Facial Recognition in Law Enforcement

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Facial recognition in law enforcement allows agencies to identify individuals by analyzing facial features in images and comparing them to databases of known faces. It can help identify suspects in crimes by matching images from surveillance footage to databases. The technology is used by law enforcement for various purposes, including identifying suspects, enhancing investigations, and improving public safety. It allows for the automated identification of individuals that may in some way be related to criminal events, such as suspects, wanted persons, victims or witnesses. This paper explores the use of facial recognition technology (FRT) in law enforcement.

KEYWORDS: *facial recognition, facial recognition technology (FRT), facial recognition software, biometrics, policing, law enforcement.*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Facial Recognition in Law Enforcement" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-4, August 2025, pp.809-816, URL: www.ijtsrd.com/papers/ijtsrd97338.pdf

IJTSRD97338

INTRODUCTION

Facial recognition technology (FRT) use constitutes biometric data processing and comes with a particularly sensitive analysis of data. It might be one of the most powerful applications of artificial intelligence (AI) for law enforcement and surveillance practices. The technology is a classic biometric one, based on the identification of an individual's biological or behavioral features, like fingerprint, iris, voice or signature. The facial recognition approach has been significantly transformed by the development of AI and deep learning, which makes FRT an application of "smart criminal justice." Traditional facial recognition methods relied on comparing specific features of the face and were later on combined with machine learning techniques to process facial features. Modern facial recognition systems thus involve AI techniques that are applied to solve the recognition problem.

FRT in law enforcement can be used for both preventive and repressive purposes; each accompanied by different legal implications. For prevention, FRT is used for general surveillance of publicly accessible spaces. Repressive purposes refer to actions taken to prosecute criminal offences (i.e., in the aftermath of a crime) [1].

Biometrics make use of our most unique physical features and behaviors to serve as digital identifiers that computers and software can interpret and utilize for identity-related applications. They can be used to identify someone in a biometric database or to verify the authenticity of a claimed identity. Facial recognition apps apply the science of biometrics to a user's facial features. Facial recognition algorithms create a biometric template by detecting and measuring various characteristics, or feature points, of human faces, including location of the eyes, eyebrows, nose, mouth, chin, and ears. Figure 1 shows a facial recognition algorithm that creates a biometric template [2].

The use of biometrics in law enforcement has a long history. In the early 1900s, police officers began using fingerprint evidence to help investigations. Facial recognition technology dates back to the 1960s, with techniques that relied on hand coding facial features of each face in the database. Since then, increasingly sophisticated technologies have

expanded how biometric data enables law enforcement to help build an evidentiary case against suspects [3].

WHAT IS FACIAL RECOGNITION?

Facial recognition refers to the process of identifying or confirming an individual's identity based on their facial features. Naturally done by humans, this task can also be performed by machines, namely through facial recognition technology (FRT). FRT has emerged as a powerful tool for law enforcement, enabling the automated identification of individuals based on their unique facial features. The technology can be used to identify missing individuals by matching their images to those in databases. Facial recognition systems start by capturing an image or video of a person's face. This can be from surveillance cameras, body-worn cameras, or even photos taken by officers. Figure 2 shows a surveillance camera above a Boston street in 2014 [4].

For example, New York City Police Department (NYPD) uses facial recognition to identify suspects in various crimes, including robberies, burglaries, and assaults. NYPD uses FRT to compare images obtained during criminal investigations with lawfully possessed arrest photos. Security Industry Association (SIA) reports that the NYPD used facial recognition to identify a suspect who left a suspicious package in a subway station, showcasing how it can be used in counter-terrorism efforts. The New York DMV uses facial recognition to verify identities and prevent fraud by comparing photos taken at the DMV with existing databases [5].

FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology automates the process of comparing one photograph to other photographs to find potential matches. Law enforcement agencies capture an image of a suspect (from surveillance footage, body-worn cameras, etc.). This image is then inputted into a facial recognition system, which compares it against a database of known faces (e.g., booking photos, driver's license photos, social media profiles). The system generates a list of potential matches, ranked by the software's algorithm, along with other identifying information about the potential match. Law enforcement officers must verify any potential matches through further investigation and traditional police work. In order for law enforcement officers to use such technology, they need a large database of photographs of known individuals against which they can compare a photo of an unidentified suspect. Thus facial recognition systems follow several steps shown in Figure 3 [1].

FRT can be used to generate leads in investigations, identify suspects and victims, and find missing persons, but it also raises concerns about privacy and potential for errors. For example, the INTERPOL Facial Recognition System (IFRS) uses facial recognition technology to identify individuals across borders. Since its creation, the IFRS System has helped to identify several thousand individuals including terrorists, criminals, fugitives, etc. Figure 4 shows a facial recognition system designed for law enforcement use [4].

FACIAL RECOGNITION SOFTWARE

Law enforcement officers in the United States are increasingly turning to a new technology to make their jobs easier: facial recognition software. Facial recognition software is capable of potentially identifying or verifying the identity of a person by analyzing patterns based on a person's facial feature locations and contours and comparing them to those features in other photographs. Facial recognition software used by law enforcement typically involves using algorithms to analyze facial features in images or videos and compare them against databases of known individuals, This software is used to identify suspects in investigations, verify identities, and potentially prevent crimes by flagging individuals on watchlists. The software analyzes the image, identifying key facial features like the distance between the eyes, the shape of the nose, and the position of the mouth. These features are converted into a numerical representation, called a faceprint. The faceprint is compared against a database of known individuals, such as mugshots, watchlists, or even public social media profiles. If a match is found, the system provides a score indicating the likelihood of the match. Law enforcement officers then typically review the results and verify the match using other methods before taking any action.

Facial recognition software is used by local, state, and federal law enforcement, but its adoption is uneven. For example, Colorado Information Sharing Consortium (CISC) facilitates the use of facial recognition software, allowing law enforcement agencies to share data securely and identify suspects. Some cities, like San Francisco and Boston, have banned its use for law enforcement, while others have embraced it. In spite of this, the software has been instrumental in solving cold cases, tracking suspects, and finding missing persons, and is considered a game changer by some in law enforcement.

APPLICATION OF FACIAL RECOGNITION FOR LAW ENFORCEMENT

Facial recognition software can be integrated with existing police databases, including mugshots and

driver's license records. Facial recognition technology can be used in a number of ways, including to prevent and detect crime, find wanted criminals, safeguard vulnerable people, and to protect people from harm – all to keep the people safe. Common applications of facial recognition include the following [6-8]:

- *Investigative Tool*: Perhaps one of the most well-known applications of facial recognition technology is law enforcement, where agencies can use it to find missing people, aid in solving crimes, and help monitor large crowds of people. Facial recognition technology is used to assist in ID of subjects while ensuring that improper or incorrect ID does not lead to the arrest of an innocent person. Police claim to use FRT just as an investigatory lead, but in practice officers routinely ignore protocol and immediately arrest the most likely match spit out by the computer without first doing their own investigation. Law enforcement agencies such as the Federal Bureau of Investigation (FBI) use facial recognition technology to search criminal watch lists and help conclusively identify a person of interest. They can match a recently taken photo or video against a database of single images to help identify that person. Governments around the world use facial for biometric identification for a variety of applications including customs and border security, fraud prevention, and citizen ID. There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads. As a consequence, agencies across the country can—and do—submit all manner of "probe photos," photos of unknown individuals submitted for search against a police or driver license database.
- *Retrospective Facial Recognition*: RFR is used after an event or incident as part of a criminal investigation. Images are typically supplied from CCTV, mobile phone footage, dashcam or doorbell footage or social media. These images are then compared against images of people taken on arrest to identify a suspect. The investigating officer will consider all of the evidence available and follow up all reasonable enquiries as in any normal investigation. This is a key tool for the police to identify suspects more quickly and accurately. It can also help identify missing or deceased people.
- *Live Facial Recognition:* Live facial recognition (LFR) enables police to identify wanted people, a core part of policing. Every day, police officers are briefed with images of suspects to look out for. LFR cameras are focused on a specific area; when people pass through that area their images are streamed directly to the LFR system and compared to a watchlist. A facial image is like a fingerprint: a unique piece of human data that can identify an individual or connect them to a crime. Figure 5 shows a typical fingerprint [9]. Law enforcement uses facial recognition to identify suspects, monitor large crowds, and ensure public safety. During a face recognition search on an edited photo, the algorithm does not distinguish between the parts of the face that were in the original evidence—the probe photo—and the parts that were either computer generated or added in by a detective, often from photos of different people unrelated to the crime. For example, a two-year operation was undertaken to disrupt, deter, and build intelligence of drug operations within communities in Cardiff. RFR identified those involved and generated an intelligence picture of drug dealing in the city.

BENEFITS

Facial recognition technology offers several benefits to law enforcement, including improved suspect identification, location of missing persons, and faster resolution of criminal investigations. It can be a valuable tool for monitoring public spaces, enhancing overall public safety. It can be used to analyze old images and potentially identify individuals involved in unsolved crimes. Other benefits of facial recognition include the following:

- *Faster Investigation Times*: Facial recognition can help law enforcement identify individuals more quickly than traditional methods. In a connected world, facial recognition technology enables law enforcement agencies to complete investigations faster. Whether using a criminal database or comparing across images taken in public places, the technology automates many manual tasks to help identify potential suspects or missing persons more efficiently. By rapidly identifying potential suspects or victims, facial recognition can significantly speed up the investigative process, potentially leading to quicker arrests and case closures.
- *Identification and Investigation*: Facial recognition can quickly compare images from crime scenes or surveillance footage with databases of known individuals, potentially identifying suspects involved in various crimes, from burglaries to terrorist attacks. The technology can be used to identify individuals who have been reported missing, potentially leading to their safe recovery. Facial recognition

can also be used to exonerate individuals who have been wrongly accused by comparing their images to available evidence and databases.

- *Enhanced Public Safety*: Facial recognition can be used to monitor public spaces, such as airports and crowded events, to identify individuals of interest or potential threats. The potential for identifying and apprehending criminals in real-time can act as a deterrent, potentially preventing future offenses, according to some analyses. In large gatherings, facial recognition can help identify individuals who are causing disturbances or engaging in illegal activities, improving crowd control and safety.

CHALLENGES

The increasing use of facial recognition by in law enforcement has not been without controversy due to its relation to fundamental rights and risks regarding (illegitimate) surveillance. Data collection (and analysis) is usually carried out without the knowledge of the data subject, increasing the intensity of the interference. Police have shown, time and time again, that they cannot be trusted with face recognition technology (FRT). It is too dangerous, invasive, and in the hands of law enforcement, a perpetual liability. Mistaken identity can lead to wrongful arrests and accusations, impacting individuals and communities. The following other challenges must be addressed for facial recognition apps to be useful:

- *Accuracy:* Facial recognition technology is not always accurate and can produce false positive matches, potentially leading to misidentification and wrongful arrest. This is especially true with images of low quality or when identifying individuals from diverse populations. Due to its probabilistic nature, FRT does not deliver definite results, but rather probability measures about the similarity of faces. Statistical procedures can be error-prone and are not free of discriminatory bias. Working with good quality images is crucial. Poor quality images may not be searchable in the IFRS system. The stakes are too high in criminal investigations to rely on unreliable—or wrong—inputs. "Garbage in, garbage out" is a phrase used to express the idea that inputting low-quality or nonsensical data into a system will produce low-quality or nonsensical results.
- *Bias:* Facial recognition technology is not foolproof. There are concerns that facial recognition technology can perpetuate existing biases in law enforcement, leading to discriminatory outcomes. There have been cases of misidentification, particularly with individuals from certain demographics, highlighting the potential for bias in the algorithms. Some studies have found variations in accuracy for some software products in analyzing the faces of African Americans, Asians Americans, women, and groups other than non-white males. Law enforcement agencies have an obligation to avoid bias against protected groups defined by gender, age, race and ethnicity, and this duty includes their use of facial recognition software.
- *Privacy Concerns:* The use of facial recognition raises significant privacy concerns, as it involves collecting and processing personal data, including images of individuals who may not be suspects. It raises concerns about the potential for mass surveillance and the collection of personal data without consent. Some cities, like San Francisco and Boston, have banned or restricted the use of facial recognition technology by law enforcement due to privacy concerns. In Europe, real-time FRT use for law enforcement purposes is prohibited, but member states have the possibility of authorizing real-time use in their national law.
- *Legal and Ethical Implications*: The use of facial recognition technology in law enforcement is subject to legal and ethical scrutiny, with ongoing debates about the need for regulations and oversight. Several agencies implemented the use of such software before requiring even basic training on facial recognition technology. Data collection for the FRT process not only requires a legal basis, but specific legal bases that precisely regulate the circumstances of the data collection and the specific purpose for which it is collected.
- *Lack of Regulation:* Due to its impact on fundamental rights, facial reconition must be appropriately regulated. Such regulation should consider the multiple data processing steps and reflect each step's impact on fundamental rights. In spite of the fact that a significant number of federal agencies use facial recognition software, there are no federal laws in place to limit how law enforcement uses the technology. There is a lack of clear legal framework and regulations governing the use of facial recognition technology by law enforcement. In spite of the lack of federal controls, local governments have begun to push back against law enforcement's use of facial recognition technology. Many jurisdictions are developing laws and regulations to govern the use of facial recognition technology by law enforcement to address privacy concerns and ensure accountability.

- *Over-reliance:* There is a risk of over-reliance on facial recognition technology, potentially leading to a decline in traditional investigative methods. Some policymakers believe that the safety and civil rights problems of facial recognition can be solved by mandating a certain performance score or grade. Relying solely on test scores risks obscuring deeper problems with face recognition while overstating its effectiveness and real-life safety. It is easy to be misled by performance scores.
- *Banning:* Cities across the United States have decided to join the growing movement to ban police use of face recognition because this technology is simply too dangerous in the hands of police. People who have heard or read a lot about the use of facial recognition technology by police are more likely to say it is a bad idea for society, compared with those who have heard a little or nothing at all on the topic. While a plurality of Americans think widespread use of facial recognition by police is a good idea, a majority are not convinced such usage would cut crime. Figure 6 shows that older US adults trust facial recognition use by law enforcement [4].

CONCLUSION

Facial recognition technology (FRT) is no longer science fiction. From unlocking our phones to streamlining airport security, FRT has been quietly integrated into daily life. FRT supports the identification of individuals and can therefore be of great use to law enforcement authorities (i.e., the police, public prosecution, and ultimately, the courts). As explained earlier, the facial recognition process consists of several steps. Data is collected, analyzed, and the information generated further exploited. Unlike fingerprints and DNA, which do not change during a person's life, facial recognition must take into account different factors, such as ageing, plastic surgery, cosmetics, effects of drug abuse or smoking, pose of the subject, etc. When used in combination with human analysis and additional investigation, facial recognition technology is a valuable tool in solving crimes and increasing public safety. The implementation of facial recognition systems is in its infancy in many countries and standards and best practices are still in the process of being created. While facial recognition systems have huge potential for national safety and security, they require a robust governing structure to protect human rights and personal data. Many facial recognition systems are tested by the federal National Institute of Standards and Technology (NIST). As facial recognition technology becomes more advanced, law enforcement agencies increasingly adopt it [10]. More information about facial recognition in law enforcement can be found in the books in [11,12].

REFERENCES

[1] M. Simmler and G. Canova, "Facial recognition technology in law enforcement: Regulating data analysis of another kind," *Computer Law & Security Review,* vol.56, April 2025.

[2] W. McKee, "Police and facial recognition technology: How innovation can threaten privacy," December 2024, https://journals.library.columbia.edu/index.php/stlr/blog/view/655

[3] "Facial recognition & law enforcement – The value proposition," February 2023, https://www.aware.com/blog-facial-recognition-used-in-law-enforcement/

[4] L. Rainie et al., "Public more likely to see facial recognition use by police as good, rather than bad for society," March 2022, https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/

[5] "NYPD questions and answers facial recognition," https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

[6] "Facial recognition technology," https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/

[7] C. Garvie, "Garbage in, garbage out," May 2019, https://www.flawedfacedata.com/

[8] "Live facial recognition," https://www.college.police.uk/app/live-facial-recognition

[9] "Arrested by AI: Police ignore standards after facial recognition matches," https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/

[10] "Facial recognition," https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition

[11] D. Yeung et al., *Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias.* RAND Corporation, 2020.

[12] J. D. Woodward, *Biometrics: A Look at Facial Recognition.* RAND Corporation, 2003.

Figure 1 A facial recognition algorithm that creates a biometric template [2].

Figure 2 A surveillance camera above a Boston street in 2014 [4].

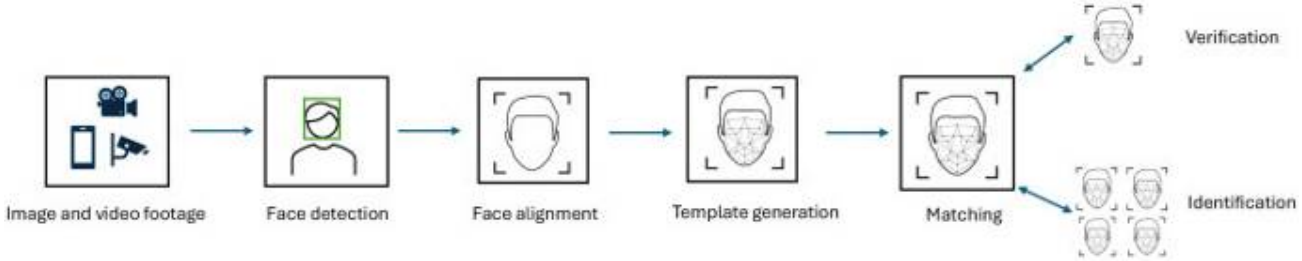

Figure 3 Facial recognition systems follow several steps [1].

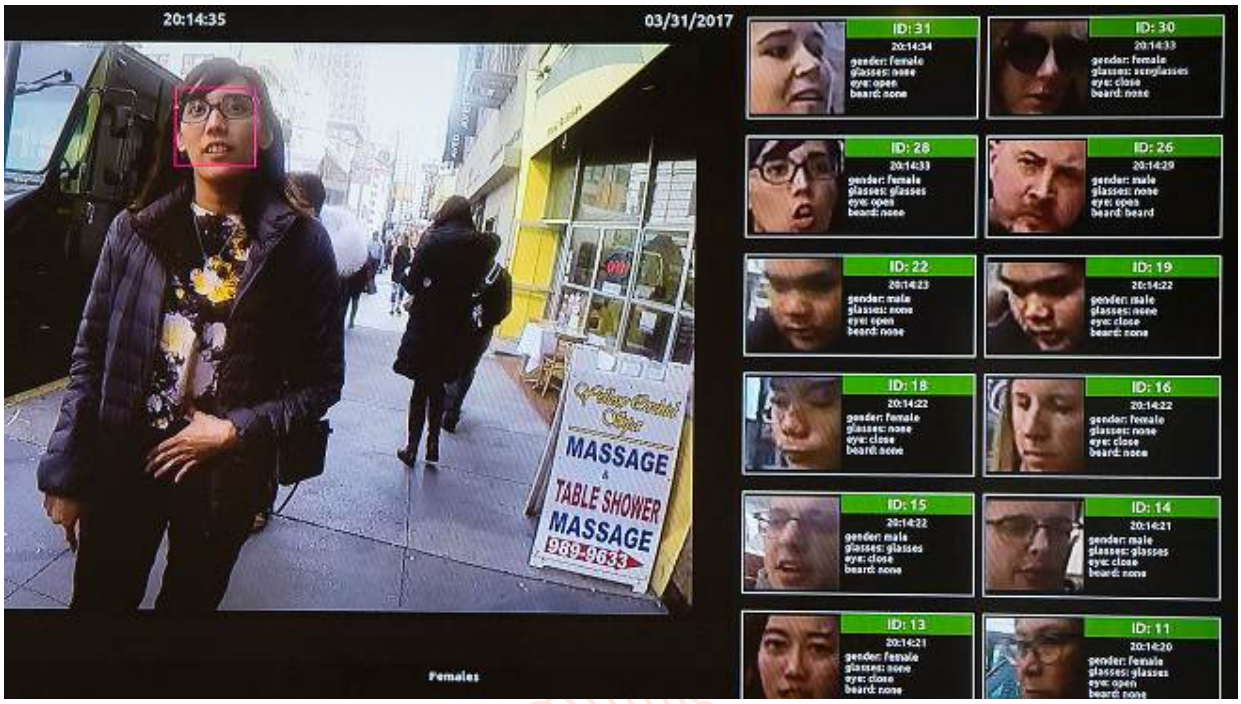

Figure 4 A facial recognition system designed for law enforcement use [4].

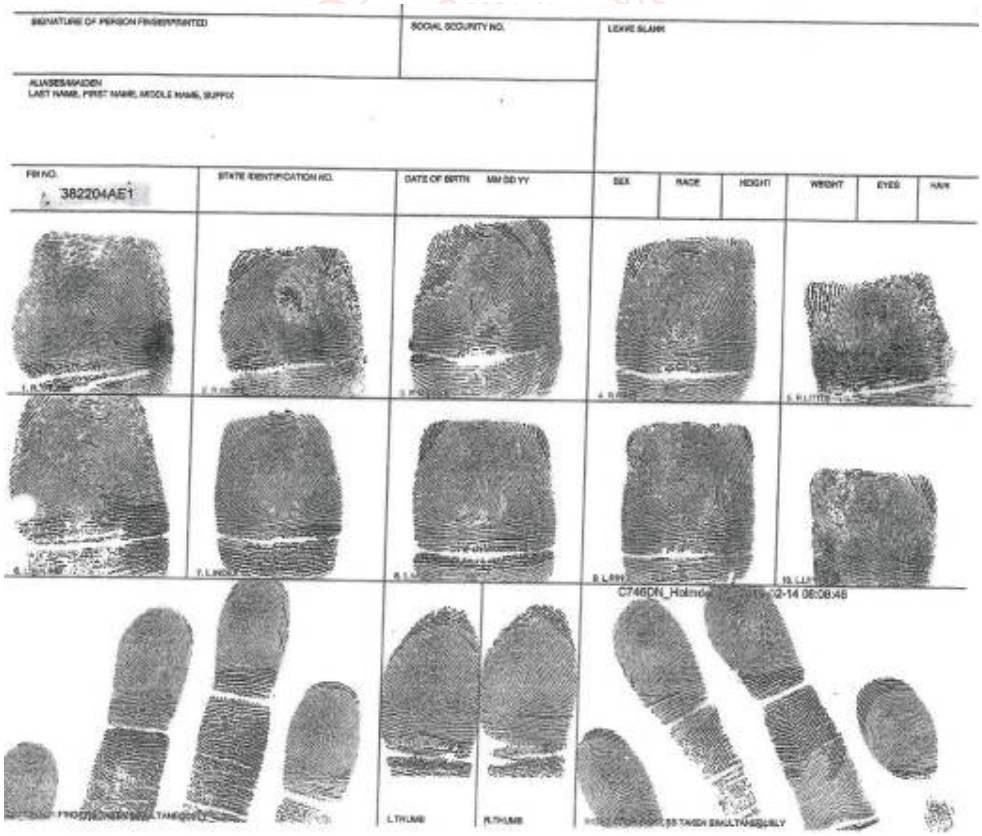

Figure 5 A typical fingerprint [9].

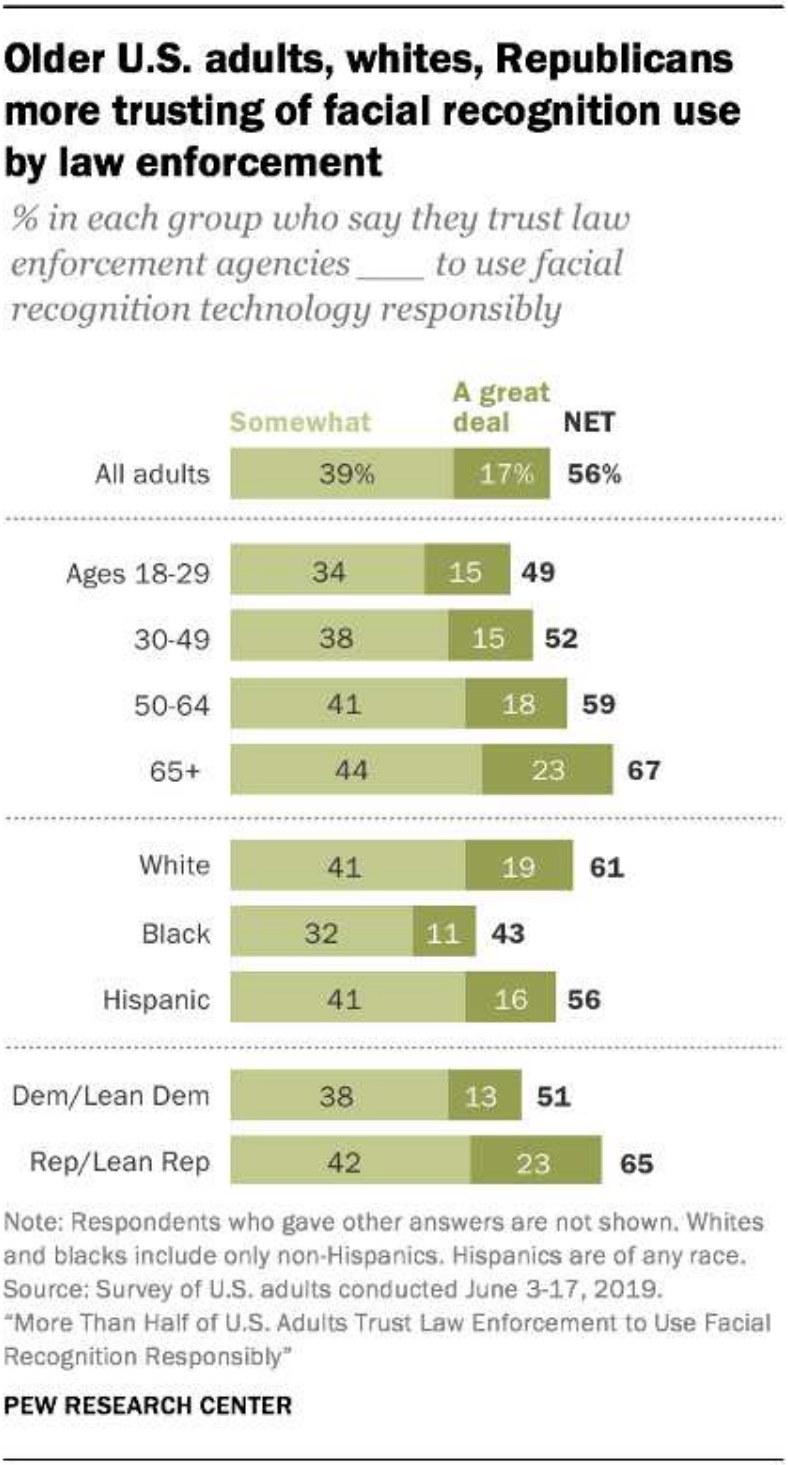

Figure 6 Older US adults trust facial recognition use by law enforcement [4].