State of Police Facial Recognition in Seattle

Maitreyee Joshi (Chair, Seattle Smart Cities Committee) and Rene Peters (Vice Chair, Seattle Smart Cities Committee)

Executive Summary

Facial recognition is a nascent technology that is being rapidly adopted by law enforcement agencies. In this report, we explain the basics of facial recognition technology and its usage by the police, review the current laws and regulations surrounding facial recognition technology, and discuss the legal issues and technological flaws of the current facial recognition systems.

Background

What is facial recognition technology?

Facial recognition systems use technology to automatically compare two images of a face and determine whether they belong to the same individual[1]. There are two primary use cases of facial recognition technology:

- **Facial verification:** Facial recognition technology can be used to confirm the identity of an individual. For example, Apple's Face ID uses facial recognition to confirm that the individual unlocking the phone is indeed allowed to unlock the phone. Face verification is typically used in consumer technology.
- **Facial identification:** Facial recognition technology can also be used to match a photographed individual to a large database of faces. For example, the police can run footage from a security camera through a facial recognition system to figure out the identities of the individuals in the video.

Generally, most facial recognition technologies use the following four key, high-level steps to verify or recognize the identity of an individual:

- **Face Detection:** The facial recognition system first detects the face in the image and highlights it.

[1] https://www.perpetuallineup.org/background

- **Face Alignment:** The system then rotates and aligns the detected face to the optimal angle for comparison.
- **Feature Extraction:** The system extracts data about features from the image that it has previously found most helpful in determining the identity of individuals. Some important features that facial recognition systems generally look for are the distance between the eyes, the width of the nostrils, the width of the chin, and the height of the forehead.
- **Feature Matching:** Then, the system compares the feature data previously extracted to similar available for millions of images in a database. For the verification use case, if there is a match between the extracted feature data and the correct individual in the database, the system returns yes. For the recognition use case, the system returns the closest matches from the database based on feature data[2].

How is facial recognition currently being used by the police?

There are four main ways that the police are currently using facial recognition technologies:

- **General Surveillance:** Facial recognition technology can be used to generally monitor crowds. For example, facial recognition technology was used at the 2001 Super Bowl in Tampa, Florida to stop any potential criminals and terrorists from entering the event. In 2015, Baltimore police used facial recognition technology to monitor protesters during the rioting after Freddie Gray's death. The use of the tech led to the arrests of protesters that had outstanding warrants.
- **Targeted Photo Comparisons:** Facial recognition technology has also been used to identify specific individuals. For example, New York has used facial recognition technology to find over 10,000 individuals committing identification fraud by having multiple driver's licenses.
- **Active Criminal Case Investigations:** Facial recognition technology has also been useful in criminal investigations. For example, the NYPD arrested an individual that had been connected to a shooting by taking a surveillance image from a nightclub and running it through a facial recognition to generate a list of 200 possible suspects.
- **Trial Evidence:** Prosecutors may start soon to use facial recognition technology as evidence in court, in order to establish probable cause or provide evidence.[3]

[2] https://towardsdatascience.com/an-intro-to-deep-learning-for-face-recognition-aa8dfbbc51fb

[3] https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/

Current Laws and Regulations

Facial recognition technology is largely unregulated at the moment. Three US cities — San Francisco, Oakland, and Somerville, Massachusetts — have implemented blanket bans on government usage of facial recognition. Several other cities have some legislation regulating facial recognition. This interactive map shows where facial recognition is being used and what legislation has passed to regulate it in different parts of the country.

Legal Issues

Facial recognition poses several legal challenges. Three prominent legal issues that may arise are:

- **Fourth Amendment Issues:** If facial recognition tracks an individual's movements over an extended period of time, it can reveal intimate details about the individual's life. This may violate the Fourth Amendment.
- **First Amendment Issues:** Facial recognition technology could also violate an individual's First Amendment right to freedom of association and right to privacy by causing individuals to self-censor themselves in fear of repercussions.[4] For instance, individuals could stop attending peaceful protests if they feared that police could identify their faces in video recordings and then retaliate against them, similar to when the Baltimore police used facial recognition monitor protesters during the rioting after Freddie Gray's death.
- **Lack of Legislative Oversight:** Many federal agencies are using facial recognition technologies without any legislative oversight. A study by the Center of Privacy and Technology at Georgetown Law found that, out of 52 agencies only four have a publicly available facial recognition use policy and only one agency received legislative approval for its policy.

Technological Flaws

In addition to the legal challenges that facial recognition technology poses, there are also several flaws to the technology in its current state. The top technological issues facing facial recognition systems currently are:

[4] https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/

- **Low Accuracy Rates:** Many currently-deployed facial recognition systems have been shown to be completely inaccurate. A trial of facial recognition software at the Robert F. Kennedy Bridge in New York in 2018 failed with a total of 0% faces correctly detected.[5] In London, facial recognition software has mistakenly identified members of the public as criminals 96% of the time.[6]
- **Biased Datasets:** In several cases, facial recognition technology has also been shown to return worse results for women and darker-skinned individuals due to underrepresentation of these individuals in training data sets. Several government tests found that even the best-performing facial recognition systems misidentified black individuals at rates 5-10 times higher than that for white individuals.[7] This can lead to individuals from certain demographic groups to be wrongly implicated for crimes.
- **Data Privacy:** There are several open questions and concerns about data privacy. Some major ones: where will this facial recognition data live? Who will have access to it? How do we prevent the data from being misused?

Conclusion

Despite the several concerns and open questions about facial recognition technology, there have been minimal laws and regulations set out to govern it. As the usage of facial recognition technology rapidly increases, it is more important than ever for lawmakers and other stakeholders to take action.

[5] https://www.technologyreview.com/f/613284/new-yorks-mass-face-recognition-trial-on-drivers-has-been-a-spectacular-failure/

[6] https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html

[7] https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/