Gary Kuepper
CST 300
Summer 2024

Law Enforcement Use of Facial Recognition Technology

Introduction/Background

Facial recognition technology (FRT) has evolved from being a concept in science fiction films, where main characters use their faces to securely access vaults, into a valuable tool for modern law enforcement to quickly identify criminals and solve cases in unprecedented ways. One of the earliest and most publicized uses of FRT in law enforcement occurred during Super Bowl XXXV in 2001, held in Tampa, Florida. The deployment of FRT at this high-profile event aimed to enhance security by scanning the faces of attendees and comparing them against a database of known criminals and terrorists (Woodward, 2001). This marked an early example of in the integration of biometric technology into public safety efforts.

While the use of FRT at the Super Bowl demonstrated its potential to assist in crime prevention, it also sparked a heated debate over privacy and the ethical implications of such surveillance. Opponents argue that the use of FRT without individuals' consent violates privacy rights and could lead to misuse and discrimination. Proponents, on the other hand, emphasized its effectiveness in enhancing security and preventing crimes. The technology's ability to quickly identify and apprehend suspects has made it an attractive option for law enforcement agencies worldwide, but it has also raised significant concerns about civil liberties and the potential for abuse (Ng, 2024).

In recent years, the prevalence of FRT has been expanded beyond law enforcement, including border control, airports, and even to unlock personal devices. With advances in artificial intelligence (AI) and machine learning FRT has significantly improved the accuracy and efficiency of FRT and is projected to increase its presence in the public's everyday life.. An example of FRT is now commonly used at international borders to streamline the identification process and enhance security measures. Airports use FRT to expedite passenger check-ins and boarding procedures, improving overall travel efficiency. On a personal level, FRT is integrated into smartphones and other devices, allowing users to unlock their devices and authorize payments with just a glance. As FRT becomes more prevalent in everyday life, its integration into various aspects of society continues to grow, bringing both benefits and challenges (National Academies of Sciences, Engineering, and Medicine, 2024).

The widespread adoption of FRT has led to increased scrutiny and debate over its ethical implication. While the technology offers numerous advantages in terms of security and convenience, it also poses significant risks to privacy and civil liberties (Bala & Watney, 2019). The potential for misuse, such as unauthorized surveillance and data breaches, has raised concerns among privacy advocates and the general public. As police departments and other organizations continue to implement FRT, it is crucial to address these ethical concerns and find a balance between leveraging the technology's benefits and protecting individual rights. This paper explores the ethical dimensions of police use of FRT through the perspectives of two opposing stakeholders: privacy concerned public and police/security concerned public. It aims to dissect the controversy and provide a balanced analysis of the arguments from both sides, ultimately leading to a reasoned position on the issue.

Stakeholder Analysis

The root of this issue lies in the delicate balance between ensuring public safety and protecting individual privacy rights. As police departments increasingly rely on FRT for surveillance and crime prevention, concerns about privacy, accuracy, and potential misuse have emerged. For instance, the city of San Francisco still maintains a ban on the use of FRT by city government agencies including the police (Vigliarolo, 2024). This paper explores the ethical dimensions of police use of FRT through the perspectives of two opposing stakeholders: privacy concerned public and the combination of law enforcement and safety concerned public. It aims to show a snapshot of the latest views on both sides as well as argue each position using ethical frameworks.

Stakeholder 1: Privacy Concerned Public

The general public, particularly privacy concerned, values the protection of individual privacy and civil liberties. They prioritize the right to privacy and the ethical use of personal data. For these groups, the collection and use of biometric data without explicit consent is a significant infringement on individual rights. They emphasize the need for transparency, accountability, and stringent regulations to safeguard personal information from misuse and unauthorized access (Rainie, Funk, Anderson, & Tyson, 2022)

Privacy advocates argue that FRT violates individual autonomy and privacy. They highlight the potential for misuse and wrongful convictions due to biases in the technology. They have concerns about how facial biometric data is collected for example training data sets have been built using images taken from social media and other online sources without any prior consent (National Academies of Sciences, Engineering, and Medicine, 2024). They believe that the deployment of FRT without sufficient oversight can lead to discriminatory practices and an erosion of civil liberties. They call for either a complete ban or strict limitations on FRT use by law enforcement to prevent potential abuse and protect individual rights.

To support their position, privacy advocates use various types of claims. They employ claims of fact to highlight documented instances of FRT errors and biases, demonstrating the technology's potential for harm (Rainie, Funk, Anderson, & Tyson, 2022). Claims of value are used to emphasize the importance of individual privacy and civil liberties over the perceived benefits of FRT. Additionally, they use analogy to compare the potential misuse of FRT to historical abuses of surveillance technologies, warning against repeating past mistakes. These arguments aim to persuade policymakers and the public of the need for strict regulations or a ban on FRT in law enforcement (Bala & Watney, 2019).

Stakeholder 2: Law Enforcement/Safety Concerned Public

Law enforcement and safety concerned public prioritize public safety, crime prevention, and the efficient enforcement of laws. They value the potential of FRT to enhance law enforcement capabilities, enabling quicker identification and apprehension of suspects. For this group, the primary concern is the protection of the community from crime and the effective use of technology to support law enforcement efforts. They believe that technological advancements, like FRT, are essential tools in maintaining public safety and order (Gonzales, 2023).

Proponents from the police and security sectors argue that FRT significantly enhances public safety and prevents crime. For example, FTR was crucial in identifying Jarrod Ramos, gunman behind the 2018 Capital Gazette shootings, when Jarrod refused to identify himself after police placed him in custody (Witte, 2021). They emphasize that the technology allows for the quick identification of suspects, which can be crucial in solving crimes and preventing further harm. They believe that the benefits of FRT in terms of crime reduction and increased efficiency in law enforcement outweigh the privacy concerns raised by opponents. They advocate for the regulated use of FRT, arguing that with proper safeguards, the risks can be mitigated while maximizing the benefits (Bala & Watney, 2019).

To support their position, proponents use claims of fact, highlighting statistics that show reduced crime rates and faster resolution of criminal cases due to FRT. They also use claims of definition to clarify the regulated use of FRT, stressing that it is not intended for mass surveillance but targeted crime prevention. Claims of value are employed to argue that the safety and security of the public take precedence over individual privacy concerns. By presenting evidence of FRT's effectiveness in improving public safety, they make a compelling case for its regulated use (Janesch, 2024).

Argument Question

Should police forces be allowed to use facial recognition technology given the balance between public safety and privacy concerns?

Stakeholder Arguments

Stakeholder 1: Privacy Concerned Public

Immanuel Kant’s duty-based ethics emphasizes moral actions performed out of duty and respect for individuals' rights. This ethical framework highlights adherence to moral rules and the inherent dignity of every person. Kantian ethics is deontological, focusing on the inherent morality of actions rather than their consequences. The major principles of this framework include the categorical imperative, which mandates that actions should be universally applicable and respect the autonomy of individuals.

Applying the tenets of Kantian ethics to the privacy concerned public's position, the use of FRT by police is seen as a violation of individuals' rights to privacy and autonomy. According to this framework, actions are considered morally right if they respect the inherent dignity and autonomy of individuals. The deployment of FRT without individuals' explicit consent involves surveillance and data collection that disrespects their autonomy.

From the privacy concerned public's perspective, the correct course of action on the issue is to either completely ban or impose strict limitations on the use of FRT by law enforcement. This is because the technology, as it stands, fails to respect the privacy and autonomy of individuals, which are fundamental ethical principles according to Kantian ethics. By advocating for a ban or stringent regulations, privacy advocates aim to prevent the potential misuse of FRT and protect civil liberties.

If the decision aligns with the privacy concerned public's position, they stand to gain significant protections for individual privacy and civil liberties. This would prevent unauthorized surveillance and potential misuse of biometric data. On the other hand, if the decision favors unrestricted use of FRT, this stakeholder risks the erosion of privacy rights and the potential for discriminatory practices and wrongful convictions, exacerbating existing biases in the criminal justice system.

Stakeholder 2: Law Enforcement/Safety Concerned Public

Utilitarianism is an ethical framework that evaluates actions based on their consequences, aiming to maximize overall happiness and well-being. Utilitarianism is consequentialist, meaning the morality of an action is judged by its outcomes. The major principle of this framework is the greatest happiness principle, which suggests that actions are right if they promote the greatest good for the greatest number of people.

Applying the tenets of utilitarianism to the law enforcement and safety concerned public's position, the use of FRT is justified if it enhances public safety and prevents harm. According to this framework, the deployment of FRT should be evaluated based on its ability to reduce crime rates and increase the overall safety of the community. If the benefits of using FRT, such as quicker identification and apprehension of suspects, outweigh the potential risks to privacy, then its use can be considered ethically permissible.

From the law enforcement and safety concerned public's perspective, the correct course of action on the issue is to regulate the use of FRT with proper safeguards. This approach ensures that the technology is used effectively to enhance public safety while minimizing the risks to individual privacy and misidentification. By advocating for regulated use, proponents aim to maximize the benefits of FRT, such as crime reduction and increased efficiency in law enforcement, while addressing the ethical concerns raised by opponents.

If the decision aligns with the police and security concerned public's position, they stand to gain significant improvements in crime prevention and public safety. The regulated use of FRT would enable law enforcement to quickly identify and apprehend suspects, reducing crime rates and enhancing community safety. However, if the decision favors a complete ban on FRT, this stakeholder risks losing a valuable tool that could significantly enhance law enforcement capabilities and improve public safety outcomes.

Student Position

I support the regulated use of facial recognition technology by law enforcement. I believe the benefits of FRT in enhancing public safety and crime prevention outweigh, the valid privacy concerns. I also stand firm that it is crucial to implement stringent regulations and oversight to concerns raised by opponents. A balanced approach can ensure that the technology is used responsibly and ethically while serving the public good.

My position aligns closely with the law enforcement/safety concerned public due to the observed increase in crime in urban areas. I see the potential advantages of FRT to tackle crime and especially when the crime is recorded with full view of the suspects face. While I acknowledge the importance of protecting individual privacy, I believe that with proper regulations and oversight, the benefits of FRT can be realized without compromising civil liberties.

To solve the issue, I recommend that FRT should be used under probable cause, the same restriction we have when stopped by a police officer while driving. When there is probable cause, the officer may perform a search of the vehicle and/or person. While there are active debates on what determines probable cause, I think FRT can be lumped into this approach. With FRT the definition of probable cause and the approach used by law enforcement requires increased scrutiny to ensure this immense power does not get abused. Implementing such regulations would foster public trust and demonstrate a commitment to ethical policing practices.

References

Bala, N., & Watney, C. (2019, June 20). *What are the proper limits on police use of facial recognition?* Retrieved from Brookings: https://www.brookings.edu/articles/what-are-the-proper-limits-on-police-use-of-facial-recognition/

Feeney, M. (2019, May 13). *Should Police Facial Recognition Be Banned?* Retrieved from CATO Institue: https://www.cato.org/blog/should-police-facial-recognition-be-banned

Gonzales, B. (2023, July 27). *US cities weigh value of facial recognition for police*. Retrieved from Biometricupdate.com: https://www.biometricupdate.com/202307/us-cities-weigh-value-of-facial-recognition-for-police

Janesch, S. (2024, February 17). *Limiting police use of facial recognition technology gaining support in Maryland General Assembly*. Retrieved from The Baltimore Sun: https://www.baltimoresun.com/2024/02/17/limiting-police-use-of-facial-recognition-technology-gaining-support-in-maryland-general-assembly/

National Academies of Sciences, Engineering, and Medicine. (2024, January 17). *Facial Recognition Technology: Current.* Washington DC: The National Academies Press. doi:10.17226/27397

Ng, A. (2024, January 19). *Washington takes aim at facial recognition*. Retrieved from Politico: https://www.politico.com/news/2024/01/19/washington-takes-aim-at-facial-recognition-00136498

Rainie, L., Funk, C., Anderson, M., & Tyson, A. (2022, March 17). *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns.* Retrieved from Pew Research Center: https://www.pewresearch.org/science/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/

Vigliarolo, B. (2024, May 20). *Can I phone a friend? How cops circumvent face recognition bans*. Retrieved from The Register: https://www.theregister.com/2024/05/20/cops_circumvent_facial_recognition/

Witte, B. (2021, September 28). *Maryland newspaper gunman gets more than 5 life prison terms*. Retrieved from Associated Press: https://apnews.com/article/jarrod-ramos-courts-maryland-newspapers-annapolis-2ec0cf15047f1e9530f68066be09601e

Woodward, J. D. (2001, May). *Super Bowl Surveillance: Facing Up to Biometrics*. Retrieved from RAND Corporation: https://www.rand.org/pubs/issue_papers/IP209.html