Exploring Ethical and Legal Complexities of Facial Recognition in Law Enforcement

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Tammy Ngo

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

William F. Stafford, Jr., Department of Engineering and Society

Abstract

The integration of facial recognition technology into law enforcement practices in the United States has sparked intense debate and scrutiny. While touted as a powerful tool for identifying suspects and enhancing investigative capabilities, concerns over its reliability, ethical implications, and potential for misuse have emerged. I delve into the multifaceted landscape of facial recognition technology, examining its adoption by law enforcement agencies, public sentiment, and justifications provided for its use. Through a comprehensive review of literature and a case study focusing on Pinellas County, Florida, I will highlight the complexities surrounding facial recognition technology. Despite acknowledging its potential benefits, including aiding in criminal investigations, establishing probable cause, and protecting vulnerable populations, I will underscore widespread concerns regarding privacy infringement, racial bias, and false arrests. Pinellas County's proactive approach in addressing criticisms and striving for responsible implementation serves as a model for navigating the ethical and legal complexities inherent in facial recognition technology. As the debate unfolds, the need for a regulatory framework, collaboration among stakeholders, and public awareness becomes increasingly apparent to ensure the responsible and ethical use of facial recognition technology in law enforcement while upholding principles of justice and individual liberties.

Introduction

The relentless march of technology has left an indelible mark on numerous industries in the United States, and within the realm of law enforcement, this transformation has manifested in the

continual enhancement of investigative tools through the integration of cutting-edge technologies. Among these tools, facial recognition systems have emerged as a recent addition to law enforcement's intricate toolkit, aimed at not only identifying victims but also pinpointing potential criminals. This technological advancement, however, stands at a crossroads, with the reliability of facial recognition systems being scrutinized in the wake of cases that have resulted in wrongful charges and arrests. Such instances have ignited a contentious debate, prompting calls for a reevaluation of the technology, and even advocating for a ban.

The landscape of facial recognition technology in law enforcement is complex and multifaceted. Recent reports indicate that nearly half of the 42 federal law enforcement agencies have embraced facial recognition technology, signaling a widespread adoption of this tool in the pursuit of justice (Simerman, 2023). However, the shine on this technological marvel is dulled by disconcerting revelations, such as Detroit Police Chief James Craig's admission that their facial recognition system, obtained from DataWorks Plus, incorrectly identifies individuals approximately 96% of the time (Koebler, 2020). This startling revelation raises significant questions about the accuracy and reliability of facial recognition systems, contributing to growing skepticism among the public.

Public sentiment, as gauged by a study conducted (Rainie, et al. in 2022), reflects a palpable conflict of interest, with only 46% of U.S. adults expressing belief in the wisdom of integrating facial recognition technology into law enforcement's toolkit. This skepticism is not unfounded, given the instances of wrongful charges and arrests attributed to the facial recognition system. This juncture marks a critical moment in the ongoing narrative of technology intersecting with justice, where the benefits promised by facial recognition technology collide with its potential drawbacks.

The question this report will primarily address is how has law enforcement, specifically in the US, justified their use of facial recognition? I delve beyond the surface-level debates surrounding technology and law enforcement, venturing into the nuances of reliability, ethical considerations, and the overarching societal impact of these systems. As the reliance on facial recognition technology becomes increasingly prevalent, a comprehensive exploration of its implications is imperative, laying the groundwork for a nuanced discussion that goes beyond mere technological fascination to address the ethical, legal, and social dimensions that underpin its use in the realm of law enforcement.

Literature Analysis

In the ever-evolving landscape of law enforcement and technology, facial recognition technology stands as a contentious and complex tool, offering both promises of enhanced security and profound ethical quandaries. This discourse delves into the multifaceted implications surrounding the use of facial recognition in criminal investigations. Central to our exploration are the intertwined themes of reliability, transparency, and equity within the deployment of facial recognition technology. Through a critical lens, we examine the compounding errors inherent in algorithmic and human components, the pervasive biases ingrained within facial features, and the imperative for increased transparency in law enforcement practices. Moreover, we scrutinize the disproportionate impacts of facial recognition on marginalized communities, particularly regarding issues of racial bias and the erosion of individual rights. Amidst these complexities, we aim to navigate the ethical dimensions of facial

recognition technology, grappling with its potential benefits and the imperative for responsible and accountable deployment in the pursuit of justice and public safety.

In a synthesis of interdisciplinary research spanning computer science, psychology, forensic science, and legal studies, compelling evidence emerges challenging the reliability of facial recognition technology as a cornerstone of identity evidence in criminal investigations. The amalgamation of algorithms and human intervention in facial recognition searches not only amplifies the potential for errors but also compounds the mistakes made by both entities. Furthermore, the pervasive biases inherent in facial features, encompassing demographics, expressions, and presumed behavioral traits, present a formidable obstacle in mitigating bias and inaccuracies (Garvie, 2022). This underscores the urgent need for increased transparency within law enforcement practices as well as creating further regulatory measures for using this technology, particularly given the inherent unreliability of facial recognition as a source of identity evidence. The convergence of errors in algorithmic and human components only empathizes the same necessities. With biases deeply ingrained in demographics and perceived behavioral traits, eliminating such biases and errors proves to be a formidable challenge that must be addressed and acknowledged by law enforcement.

The extensive findings presented in this report present the many points of what the public response may be towards law enforcement's use of facial recognition systems. They stand to expose the significant challenges and shortcomings in law enforcement's use of facial recognition technology, emphasizing a great need for critical examination and reform (Garvie, Bedoya, et al., 2016). Noted as a key finding, we can see that there is quite a widespread use for the technology by law enforcement despite the risks that facial recognition systems can pose, such as their use in real-time surveillance as well as driver's license databases. This aligns with

the broader discourse on the multifaceted implications of facial recognition technology in criminal investigations. As we delve further into the complexities of facial recognition technology, it becomes evident that its use raises profound ethical quandaries that law enforcement will have to acknowledge and address to move forward.

It doesn't help then that these facial recognition systems are also viewed as further marginalizing communities, particularly Black people due to the increased inaccuracies and overrepresentation seen in databases. These concerning inaccuracies are only further emphasized by the lack of adequate measures to ensure the accuracy of these facial recognition systems, coupled with the reliance on non-standardized human oversight. This will be an issue that law enforcement will have to address as this can call into question the reliability and equity of the systems due to these higher inaccuracies on Black people. Moreover, the lack of proper regulatory measures only further exacerbates these public concerns, emphasizing the need for equitable practices to be implemented by law enforcement when deploying the use of facial recognition technology in investigations.

The absence of audits for misuse within major face recognition systems, despite their extensive usage by law enforcement, contradicts assertions of responsible and controlled implementation. Thus, there is a pressing need for law enforcement to form justifications, aligning with the creation of comprehensive regulations, transparency measures, and accuracy assessments, so that they are held accountable and responsible for their utilization of this technology.

On the other hand, while it is easy to see the negative effects of facial recognition technology due to events such as wrongful arrests of Black people in the US and the persecution of a

minority in China, specifically Uighurs, there are still justifications that can be made behind the US law enforcement's continued use of the technology. This is shown by cases in which law enforcement have used facial recognition in helping to identify posted images of child sex trafficking victims on the internet far faster than any human could do, saving tens of thousands of children from further incident. An example is then given that if a facial recognition system is more biased towards correctly identifying White people over other races, its use for the fight against human trafficking can actually lead to a net positive for these minorities rather than for the White people, meaning if these minorities are being trafficked more, the technology may be biased towards these same groups in this situation rather than against (Rudin, et al., 2021).

Thus, this shows how there is no true black or white situation when it comes to working with facial recognition technology. Much like other technologies and tools among others, there is nuance behind its use in law enforcement as there can be good and bad that comes from the use of this technology even if it is at the stake of losing out on equity. After all, without the use of this technology, the many children that may have been saved from further trafficking may still be doing it today and never be identified and saved. By continuing the use of this technology, we can identify the benefits and risks of the systems and either remedy the risks discovered through fixing them directly or enforcing regulatory policies to prevent such fallacies from occurring.

While facial recognition technology has permeated various facets of society, serving purposes from ensuring secure access to smartphones to aiding law enforcement in identifying criminal suspects through surveillance images, the indiscriminate use of facial recognition algorithms has seen concerns voiced by citizens' rights advocates, social justice groups, and the research community (Perkowitz, 2021). The uncritical deployment of the algorithms has led to undesirable societal consequences, including instances of false arrest and heightened government

surveillance. To reiterate once more though as it is still seen largely as a big issue and is stated as such in multiple articles including this one, these consequences have disproportionately impacted people of color within the United States.

One significant factor contributing to this disproportionate impact is the inherent racial bias embedded in facial recognition algorithms. Studies have revealed that these algorithms tend to be less accurate when applied to individuals of color, exacerbating the risk of misidentification and false accusations. Furthermore, the integration of facial recognition systems into existing systems and institutions with historical disparities has compounded the challenges, perpetuating inequalities in the justice system. This only continues to fuel the necessity for law enforcement to step up and fix these ongoing issues as the public continues to bring up this issue for good reason as well as be transparent about what action they are taking to resolve these biases.

In the article though, there does appear to be ongoing research that is aimed towards drawing insights from older forensic technologies, such as fingerprint identification. By learning from the historical evolution of fingerprint technology and others, analyzing its improvements over time, there is great potential to enhance the real-world deployment of facial recognition systems and mitigate the adverse impacts on marginalized communities.

Case Study

The case study will focus on the rationale behind Pinellas County of Florida, where facial recognition technology has been strongly adopted into its local law enforcement. Pinellas County stands out as a prominent user of this technology within the US, having reported approximately

24.9 million mugshots and 22 million state driver's license photos available for facial recognition searches. The county has also disclosed an estimate of 8,000 searches per month as of 2016, making it a noteworthy player in the utilization of facial recognition technology (Garvie, Bedoya, et al., 2016).

The county's law enforcement officials have embraced facial recognition technology, attributing their decision to the increasing demand for such advancements, especially given that facial data has become the most extensively collected biometric in contemporary times (Jowell et al., 2014). This technology allows authorities to identify and verify individuals by analyzing unique facial features, providing a potentially powerful tool for criminal investigations.

The justification provided by law enforcement emphasizes the need for effective tools in the face of evolving criminal methodologies. Facial recognition is seen as an asset, particularly in situations where there is a lack of alternative physical evidence. In instances where traditional investigative methods may fall short, facial recognition technology offers an additional layer of identification that can aid in solving cases.

However, the adoption of facial recognition technology has raised concerns within the county, notably regarding its access to a vast repository of civilian images. Critiques made from residents of the county worry about the potential invasion of privacy and the scope of data collection, as facial recognition systems often rely on extensive databases that include images of individuals who may not be involved in criminal activities. The ethical and legal implications of utilizing such datasets have become a focal point of the debate surrounding facial recognition technology.

Despite these concerns, law enforcement argues that facial data encounters relatively fewer constraints when it comes to sharing information compared to other biometric data. This flexibility is considered advantageous for law enforcement, allowing for more effective collaboration and information sharing across jurisdictions. The law enforcement continues to assert that the technology's potential benefits, such as improved public safety and faster identification of suspects, outweigh the associated risks.

As the county grapples with the ethical and legal considerations surrounding facial recognition technology, it becomes crucial to strike a balance between leveraging its capabilities for law enforcement purposes and safeguarding individual privacy rights.

Despite the perceived benefits, the adoption of facial recognition technology in Pinellas County has not been without controversy. Acknowledging concerns raised by critics and privacy advocates, law enforcement officials address issues such as the extensive access to civilian images and the ethical use of datasets. The use of mugshots and driver's license photos, which are part of a vast repository, raises questions about the potential invasion of privacy and the responsible handling of sensitive information.

The county has also highlighted their engagement with emerging facial recognition tools and processes, emphasizing the potential benefits for law enforcement, the military, and federal agencies. Despite early criticisms of the system, the county has effectively used the public scrutiny that has been thrown as a tool to refine and guide the future use of facial recognition systems. Presently, the county stands as leaders in recognizing the efficacy of facial recognition technology in law enforcement. They advocate for law enforcement to have a realistic understanding and expectation of the technology as well to minimize the misuse of the

technology. They have also shown great progress in initiating a partnership expansion program that has fostered collaborative growth and development (Williams et al., 2013).

Furthermore, just as law enforcement sees the benefits to the technology, they have also acknowledged the potential concerns related to facial recognition systems, such as having access to civilian images and ethical considerations. In turn, this has demonstrated a willingness to engage in a nuanced discussion about the responsible utilization of this technology as well as showing accountability for the flaws and continue improving the technology for continued use. Pinellas County's ability to use early criticisms as a tool for improvement and refinement showcases a commitment to transparency and a desire to address public apprehensions, serving as a strong example for other counties to follow suit when implementing facial recognition into their own local law enforcement stations.

The country's leadership role in recognizing the efficacy of facial recognition technology not only impacts their local law enforcement strategies but also contributes to a larger narrative on the responsible integration of such tools. The initiation of a partnership expansion program indicates a forward-looking approach, fostering collaboration and development in the ongoing evolution of facial recognition systems within law enforcement practices as well as within other government agencies.

Conclusion

In conclusion, the integration of facial recognition technology into the arsenal of law enforcement agencies marks a critical juncture where technological advancement intersects with

the pursuit of justice. The tumultuous landscape painted by the reliability issues, instances of wrongful charges, and public skepticism underscores the need for a nuanced and comprehensive approach in evaluating the future trajectory of facial recognition systems in law enforcement. In this context, the overarching question looms large: Should facial recognition technology continue to be a pivotal component of law enforcement, or does the prevailing doubt necessitate a reconsideration of its role in the pursuit of justice?

The conflicting perspectives presented in both the literature review and the Pinellas County case study highlight the complex dynamics and interplay surrounding this technology. On one hand, there is acknowledgment of its potential benefits, such as contributing to investigative leads, establishing probable cause, and aiding ongoing inquiries. On the other hand, the widespread concerns over its negative societal impacts, including privacy breaches, racial bias, and false arrests, cast a shadow on its efficacy and responsible use.

The proactive stance taken by Pinellas County involves actively engaging with public scrutiny as a tool for refinement and improvement of their facial recognition technology implementation. In response to public scrutiny, the police department in Pinellas County conducted regular evaluations of their facial recognition practices, assessing their effectiveness, and addressing any concerns raised by the public or stakeholders. This included reviewing the accuracy of the technology, evaluating its impact on community relations, and considering any potential biases in its use. Additionally, they actively sought feedback from community members and civil liberties organizations to inform their policies and procedures. This transparent approach allowed for continuous adaptation and refinement of their methods based on real-world feedback and concerns, thereby demonstrating a commitment to responsible implementation.

Realistic expectations, in this context, refer to acknowledging the limitations and potential risks associated with facial recognition technology. This involves understanding that while technology can be a valuable tool for law enforcement, it is not without flaws or ethical considerations. Realistic expectations entail recognizing that facial recognition is not a panacea for all law enforcement challenges and may have limitations in accuracy, particularly in identifying individuals from certain demographic groups. By maintaining realistic expectations, law enforcement agencies can mitigate the risk of misuse or over-reliance on the technology, ensuring that it is used judiciously and in accordance with ethical principles.

However, the path forward is far from clear-cut. The complex nature of facial recognition technology necessitates a delicate balance between its advantages and potential societal consequences. As the debate unfolds, regulatory measures become paramount to guide the responsible use of this technology.

In navigating this complex landscape, collaboration becomes crucial. It requires a concerted effort between technology developers, law enforcement agencies, legal experts, and civil liberties advocates to strike a balance that upholds justice while safeguarding individual rights. Public discourse and awareness are equally vital components, fostering an informed society that actively participates in shaping the ethical and legal boundaries of facial recognition technology in law enforcement.

In essence, the conclusion drawn from the intricate interplay of technological advancement and justice underscores the need for ongoing evaluation, refinement, and a collective commitment to ethical considerations. The future of facial recognition technology in law

enforcement hinges not only on technological enhancements but also on the ethical and legal frameworks that guide its responsible implementation, ensuring a harmonious coexistence with the principles of justice and individual liberties.

References

Garvie, C. (2022). A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations. Center on Privacy & Technology at Georgetown Law. https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf

Garvie, C. & Bedoya, A. (2016). The Perpetual Line-Up: Unregulated Police Facial Recognition in America. Georgetown Law: Center on Privacy & Technology. https://www.perpetuallineup.org/

Jowell, S. & Ruberto, J. (2014). What's Driving the Need for Facial Recognition? Pinellas County Sheriff's Office. https://www.nacdl.org/getattachment/d215b76f-0de0-4209-99ac-55e10d2582cc/1125_jowell_connectid-2014-fr-presentation.pdf

Koebler, J. (2020). Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time. Vice. https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time

Perkowitz, S. (2021). The Bias in the Machine: Facial Recognition Technology and Racial Disparities. MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2021. https://doi.org/10.21428/2c646de5.62272586

Rainie, L., Funk, C., Anderson, M., Tyson, A. (2022). AI and Human Enhancement: Americans' Openness Is Tempered a Range of Concerns. Pew Research Center.

https://www.pewresearch.org/internet/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns/

Rudin, C. & Bushway, S. (2021). A Truth Serum for your Personal Perspective on Facial Recognition Software in Law Enforcement. Translational Criminology, Fall 2021, (pp. 2-5). George Mason University. https://cebcp.org/wp-content/uploads/2021/10/TC21-Fall2021.pdf

Simerman, J. (2023). What is facial recognition technology, and how do police use it? 5 things to know. Nola. https://www.nola.com/news/crime_police/whats-facial-recognition-tech-and-how-do-police-use-it/article_352ce43a-888a-11ed-a486-db6b661d0829.html#:~:text=The%20U.S.%20Government%20Accountability%20Office,by%20police%20in%20May%202020

Williams, S. A. & McCallum, S. (2013). Advances in Facial Recognition Inter-Agency Collaboration. Pinellas County Sheriff's Office. https://www.nacdl.org/getattachment/d203c136-f498-44c0-bbed-f8da2a41d795/061013_10_30_fr_complete.pdf