Amazon Rekognition: Addressing Privacy Concerns and Bias (Technical Report)

Exploring Ethical and Legal Complexities of Facial Recognition in Law Enforcement (STS Report)

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Tammy Ngo

October 12, 2023

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.

Tammy Ngo

ADVISORS

MC Forelle, Department of Engineering and Society

Briana Morrison, Department of Computer Science

Introduction

Technology's rapid growth has significantly impacted many US industries, including law enforcement, which has continued to improve its investigative kits with new tools. A tool that has been recently included in the law enforcement's intricate kit is the facial recognition systems, which seek to identify both victims and criminals alike. Nearly half of 42 federal law enforcement agencies have been reported to be using facial recognition technology (Simerman, 2023). As more districts are taking on this new technology, the systems' reliability has been called into question due to cases that have caused wrongful charges and arrests, which, in turn, has become one of the many leading reasons for banning the technology. This can be noted with how even Detroit Police Chief James Craig admitted that their facial recognition system, obtained from DataWorks Plus, identifies people incorrectly approximately 96% of the time (Koebler, 2020). It's no wonder why then there is a conflict of interest as only 46% of U.S. adults believe that the implementation of this new tool into law enforcement's toolkit is a good idea (Rainie et al., 2022).

Despite these staggering numbers though, law enforcement continues to keep and maintain their use of facial recognition systems. While the court has not established whether the use of facial recognition systems should be considered admissible as evidence or probable cause under the Fourth Amendment, this debate often does not appear in court as officers will usually resort to instead using the facial recognition systems as only an investigative lead (Garvie, 2022, pp. 6) or preventing poor quality images or footage from being used in the systems (Rudin & Bushway, 2021).

In the technical portion of my prospectus, I will be discussing the reliability of facial recognition technology and how its accuracy and reliability may be improved, relating to my

extensive coursework on machine learning and image analysis as well as various studies and experiments I have compiled. By improving the technology, this can alleviate some of the problems concerning the system itself, and this could, in turn, lessen the number of wrongful charges caused by the facial recognition system. For my STS portion, I will be describing how law enforcement has justified their use of facial recognition and how the law has supported the use, albeit through certain regulatory measures. By revealing their justifications for utilizing facial recognition technology, this can bring to light the important practices that law enforcement has taken to use facial recognition responsibly.

Technical Topic

Just as there is a call for being accountable and responsible in the utilization of the facial recognition system, there is a duty to increase the reliability and accuracy of facial recognition technology. As facial recognition technology has grown in prevalence and advancement, more of its flaws have come to light to the public. Complaints range from being racially and gender biased to being invasive and ruining individual privacy. That is why instead of hiding the bias that facial recognition technology holds, it should be acknowledged as a flaw to the technology. By further analyzing facial recognition systems and bringing to light the flaws that these systems have, this can inform the common people of the flaws it does have and hopefully, in turn, encourage them to put more accountability on the people creating the systems as well as the people using the systems and propose an improvement on these systems.

Without placing sufficient emphasis on the successes and failures of the facial recognition technology, the developers in control of this will not take accountability, and the number of wrongful charges will continue to persist and grow. This issue continues to devastate

people's lives unjustifiably, especially people of color, such as the unjust arrest of Robert Williams, a Black man who was arrested in front of his family by the Detroit police before being jailed overnight. Later, police compared Williams' face to the surveillance video image of a man selling expensive watches before soon realizing that his face did not match up with the man in the image (Perkowitz, 2021).

Georgetown Law has also raised concerns about facial recognition technology, revealing that the technology is seeing few checks on the technology's accuracy. Of particular concern though is whether these systems are accurate and what this may mean for African Americans due to the racially biased error that can be found in these systems (Garvie, Bedoya, & Frankle, 2016). Addressing these issues is crucial to preventing further injustices and protecting the rights of individuals, particularly those from marginalized communities.

To examine the reliability of facial recognition and bring to light its advantages and disadvantages, my previous knowledge that has been collected through my coursework will be used alongside studies and experiments that I have managed to compile from reliable sources. By gaining a better understanding of how machine learning and image analysis works in further detail based on my ongoing and previous classes, I have been able to gain insight into how important it is to choose or create a dataset that the facial recognition system will be trained on. If the data is not properly cleaned of faulty incorrect records and other possible nuances, this can lead to issues in the training process of the system.

Just as important is that the collected data is unbiased and is expansive enough that it holds a lot of diversity. If limited in scope, when used in real-world applications, it will contain a significantly lower accuracy as opposed to if the data had been properly diversified. In the focus of facial recognition, this means that there should be an equal amount of picture data that depicts

people of various genders, races, ages, etc. This appears to be a big issue in facial recognition systems today due to the biased nature of the data that they are trained in, and proper considerations were not made in closely analyzing the data in question due to false assumptions made. An example of this is the CelebA database, which is a dataset that consists of celebrities' pictures, which is severely biased when systems are trained on it due to the data having a far greater quantity of Caucasian people in comparison to people of color.

This approach of dissecting the complex process of how facial recognition systems is developed and created will reveal the weaknesses found in the systems. This can be difficult though due to the limited information that is available online on how big company facial recognition systems are created, and there are a multitude of companies who have developed their systems differently. I anticipate though that in the end, I will be focusing on the development of one facial recognition system, and, from there, I will analyze the reliability of the system. Along with observing carefully how the system is created from what data the developers have chosen or compiled, it would also be crucial to study what procedures they may have used when cleaning the data and creating their system.

STS Topic

Over the years, law enforcement has learned and gained new investigative tools that have helped them in solving various cases from the simple primitive technique of matching bullet casings to guns to now having DNA and luminol testing. Facial recognition has become one of the latest new additions to the toolkit that law enforcement may be able to use.

What is undeniable though is that facial recognition systems have become a turning point in the US, and the system has now become a topic of political debate due to its relation to

privacy and how it may serve as a tool that continues to further the divide between white people and people of color. With the great influence and impact facial recognition systems have had, this has led me to relate the system to Winner's belief that technical artifacts inherently hold political aspects that can represent forms of power and authority (Winner, 1980). Due to the overarching wrongful arrests made on black people due to this technology, this has continued to depict the power that white people continue to have over people of color.

Despite these clear flaws though, law enforcement has been able to find ways to make this technology useful in their investigations, and that is the question I hope to answer. How has US law enforcement justified their use of facial recognition technology?

While it is crucial to critique the shortcomings of facial recognition systems, it is also important to consider the perspective of law enforcement professionals who actively employ these technologies in their investigations. Understanding how these systems are utilized in solving cases and the positive impact they can have on society is essential to continuing the path of justice. Focusing solely on instances where facial recognition has failed may lead to calls for bans without acknowledging its potential benefits, potentially hindering law enforcement's ability to solve cases that might otherwise go cold due to a lack of evidence or investigative tools.

An illustrative example of law enforcement endorsing their use of the technology comes from Pinellas County Capt. Jim Main, who explains how they have been able to successfully integrate the facial recognition technology into their work, utilizing the technology to identify suspects who attempt to conceal their identity. Furthermore, this provides officers with valuable information of the individuals they may encounter (*Florida Facial Recognition System Unmasks Identity, Boosts Arrests*, 2010).

An additional significant example comes from the NYPD, which has publicly disclosed their regulations and procedures regarding facial recognition technology in its patrol guide (*Facial Recognition Technology*, 2020). Yet another example is council member James Tate, who provides justification for the approval of facial recognition technology within the Detroit Police Department. Tate argues that facial recognition technology is just like any other investigative tool, emphasizing that while all tools have shortcomings when used alone, they become more effective when utilized with other tools. This investigative tool can enhance the likelihood of generating potential leads and, more importantly, also help in ruling out those who are innocent of the crimes under investigation (Tate, 2020).

To analyze this justification, I will be using the model of sociotechnical imaginaries (Sadowski & Bendor, 2019). An important factor of sociotechnical imaginaries is that they form an imaginary on what the world should look like. In this case, I will explore the imaginary of why law enforcement feel justified in their use of facial recognition technology and what imaginary they hope to create with this technology. This will essentially build on why they believe facial recognition systems are what communities need and why this technology can lead to a better future for law enforcement.

The main challenge that I will face in researching this will be the limit to how many police press releases are available relating to facial recognition technology as it is still an up-and-coming system, and only some states have accepted the use of facial recognition technology in law enforcement. I predict that I will be delivering some discussions related to the justifications police present in the press releases as well as some news reports that described secondhand accounts of police statements.

Conclusion

What I anticipate I will deliver with my technical portion is analyzing the development and results of how a big company's facial recognition system was created, which will reveal how reliability and accuracy can be influenced based on the development of a facial recognition system. On the other hand, my STS portion will depict why law enforcement believe they are justified in their utilization of facial recognition in the US based on the imaginaries they have for this technology.

If I'm able to successfully deliver what I wish to produce, these results will serve to contribute to giving a more dimensional perspective to the reader of the implications facial recognition technology can hold for the US's law enforcement and allow the reader to gain a further understanding on what the prospect of using facial recognition technology may be outside of the many criticisms that the technology has already received.

References

Facial Recognition Technology. (2020). New York Police Department. https://www.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf

Florida Facial Recognition System Unmasks Identity, Boosts Arrests. (2010). TechBeat, Winter 2010. https://www.ojp.gov/pdffiles1/nij/nlectc/230005.pdf

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/

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

Sadowski, J. & Bendor, R. (2019). Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary. Science Technology and Human Values, 44(3), 540-563. https://doi.org/10.1177/0162243918806061

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.

Tate, J. (2020). *My statement regarding the recent approval of the facial recognition technology used by the Detroit Police Department*. Facebook. https://m.facebook.com/CouncilmemberTate/posts/10158350299611928/

Winner, L. (1980). *Do Artifacts Have Politics?* Daedalus, 109(1), (pp. 121–136). http://www.jstor.org/stable/20024652