Investigating the effects of biased facial recognition AI algorithms used by law enforcement in criminal investigations on people of color

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

Sneha Iyer

Spring 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

Advisor

Rider W. Foley, Department of Engineering and Society

INTRODUCTION TO FACIAL RECOGNITION TECHNOLOGY

Facial recognition is a biometric technology that is used to identify a person's identity by mapping out data points of a person's facial features. It uses AI algorithms to learn how to identify a specific person and verify them against images and videos in a database (Symanovich, 2021). The most widely known application of facial recognition technology is a sign in tool for devices such as smartphones. Most phones nowadays come equipped with face recognition biometric software and even apps like SnapChat and TikTok utilize face recognition for their filters. Applications of facial recognition exist in fields such as healthcare, education, security/law enforcement, and entertainment. Additionally, unlike other biometric systems, such as fingerprint recognition, facial recognition can be used for general surveillance by analyzing feeds from public video cameras.

U.S. law enforcement has used facial recognition technology (FRT) since the 2000's and one in four US state or local police departments had access to facial recognition technology (Horowitz, 2020), however the efficacy and accuracy of algorithms used for law enforcement is questionable and there have been several instances of wrongful arrest, false imprisonment, and loss of employment due to inaccuracies of this technology (Hill, 2021). Thus, due to the disparities in accuracy rates and current uses of FRT, there are significant risks of disparate impact and surveillance abuse of minority groups by law enforcement.

A survey by the Pew Research Center shows a mixed opinion on the effects facial recognition would have on false arrests. Some 53% of U.S. adults say police probably or definitely would make more false arrests if use of facial recognition technology was widespread among police, while 45% say this probably or definitely would not happen. Based on the survey results, it was also clear that there were some notable differences among racial and ethnic groups

on these issues: 48% of Black adults think police definitely would use facial recognition technology to monitor Black and Hispanic neighborhoods much more often than other neighborhoods, compared with 37% of Hispanic adults, and about 18% White adults (18%) who say the same (Rainie et al.,2022).

As AI algorithms become more critical for facial recognition technology, ensuring diversity in learning data, models and in the development teams creating it is essential to avoid "learning bias" which would skew the results of any AI model. Additionally, law enforcement and government agencies should be held responsible for their uses of FRT and the consequences stemming from that (Goodwin, 2021). These institutions in particular are the main players involved in regulating FRT as necessary to protect privacy and ensure accuracy. Overall, it is important to investigate the consequences of biased AI in facial recognition technology, think critically about data design and develop more ethical AI to make fairer decisions, and educate/regulate law enforcement on proper ways to use said technology to deliver fair justice. This paper focuses on examining biased facial recognition AI algorithms used by law enforcement in criminal investigations on people of color.

ACTOR NETWORK THEORY STS FRAMEWORK

Latour's actor-network theory (ANT) is used to investigate this topic. Latour's argument serves as the midpoint between technological determinism and social construction of technology where even the smallest actor in a network is able to affect other actors. The actor-network theory is useful to analyze relationships between actors in a specific network as well as what happens if we add or remove certain actors (Latour, 1992). It also considers both human and

nonhuman actors and the characteristics of every actor to determine how systems are built and managed (Ratnayake et al., 2017).

Latour also argues that when we analyze the social structure of society, we must consider "nonhumans" or rather technology. But not just the technology itself but also the ideas and morals behind the technology and how the technology affects our lives. One of his key points is that technologies are only effective when used in the proper manner. A key idea presented by Latour is the principle of general symmetry, where he asserts that one should treat human and non-human actors symmetrically. Since ANT treats the social and natural worlds as networks of relationships, with generalized symmetry, one can see that laws, processes, policies, etc. have the potential for symmetrical power and influence with regard to social groups or organizations.

Parts of Latour's arguments especially valuable when considering the effects of FRT are delegation, program of action, and prescription. Delegation is when humans give work to technology. In other words, delegation to nonhuman is when an artifact takes over the manual work of humans. In this case, using FRT delegates the task of identifying suspects from the human to the nonhuman AI. Program of action is about inscribing moral values into technology. Regarding the use of FRT, it will be important to investigate ethics and accuracy, and how developers can fairly develop AI technology as well as how users can fairly use said AI technology. Prescription involves the behavior imposed back on the human by the nonhuman. While humans are the ones who develop AI, it develops us in return. When we evaluate what AI enables us to achieve, what/how we use it, and when certain AIs discriminate for/against certain values, a better understanding of this will help grow potential for humans to learn from and collaborate with algorithms in an ethical manner. Thus, ANT can also help us understand the network by analyzing differing actor perspectives and emerging effects (Cresswell et al., 2010).

We can analyze each actor's role in a network involving AI, law enforcement agents, government, as well as the accused and investigate the consequences of biased algorithms in this industry by looking at different scenarios where inaccurate assumptions lead to wrongful arrests. We can also use ANT to help evaluate the power dynamics between different actors in this network and that analysis will help us describe responsibilities each actor has regarding fairness in criminal cases. Additionally, we can consider AI technologies as moral agents, meaning that AI can act as agents to which humans delegate different areas of interests, and which act on our behalf. They would be regarded as modules that distribute information as well as manage informational relationships between a variety of actors.

Overall, with ANT, I was able to better comprehend how law enforcement agencies, FRT AI agents, and the government interact in criminal justice cases. It is also useful for evaluating the extent to which facial recognition AI algorithms are helpful to law enforcement as well as when they discriminate for/against certain values and the consequences of doing so.

CASE CONTEXT

There is widespread concern about the challenges and responsibilities of developers in developing unbiased FRT algorithms, analyzing the ethical consequences of using such technology, and the need for regulation by the government. There is also little information about how developers, the government, and law enforcement can work together to create and use FRT responsibly and ethically.

Bias in FRT algorithms themselves is a main issue. According to a prior study conducted by Computer scientist Joy Buolamwini and Gebru in 2018 at the Massachusetts Institute of

Technology (MIT), researchers found that the data sets used to train popular commercially available FRT mostly consisted of light-skinned subjects (79.6% and 89.2%), which led to the model classifying differently based on gender and race with only a 0.8% error rate with white males but up to 34.7% error rate for dark females (Gentzel, 2021). Another study by the National Institute of Standards and Technology (NIST) of 189 commercial facial recognition programs found that algorithms developed in the United States were significantly more likely to return false positives or negatives for Black, Asian, and Native American individuals compared to white individuals (Lee & Chin, 2022). Thus, there is a great need for engineers to develop more accurate technology and use unbiased datasets to accomplish their goals. It is also very important for the engineers and computer scientists who develop this technology to seriously think about the real-world implications of their work. If a technology is utilized in a manner that disproportionately harms a minority group, then at least some of the responsibility falls to the developers who coded the algorithm.

Law enforcement is one of the largest consumers of FRT technology. While there are useful applications of FRT to help with criminal investigations, there certainly are bias, privacy, and trust issues present with facial recognition's current application in law enforcement. One common criticism of law enforcement's uses of FRT is with privacy. People do not like the idea of having some "big-brother" watchdog constantly tracking them. The question arises of how far facial recognition should be allowed to go in surveillance. On one hand, facial recognition can be useful to identify people with warrants when they are seen on a surveillance camera. On the other hand, a vast majority of people who are law abiding citizens will also unknowingly be monitored. Additionally, it is crucial to take into account the consequences stemming from a scenario where FRT is wrong or used incorrectly. A mistaken arrest has the potential to affect the

victim's future freedom, well-being, relationship with family members, finances, and employment status (Jones, 2021). Even a small false-positive result may affect multiple lives adversely.

There are also issues with data and security. When images and video are captured, how that data is used and whether anonymity is considered is unclear. According to a study by the U.S. Government Accountability Office (GAO), many federal agency employees rely on systems owned by other entities, including non-federal entities, to support their operations. GAO found that 13 of 14 agencies that reported using non-federal systems do not have a mechanism to track them. The authors of the study asserted that numerous risks to federal agencies and the public can accompany the use of FRT and that there exists a risk that nonfederal system owners will share sensitive information about an ongoing investigation with others.

In terms of the responsibilities of the government when it comes to FRT, there are ongoing movements in support of legislation to establish FRT standards. Although the Fourth Amendment's application to FRT specifically remains largely unsettled, the Court in recent years has adopted a more privacy-conscious approach to new digital surveillance technologies. Recent legislation also includes the Commercial Facial Recognition Privacy Act of 2019, which prohibits commercial organizations from collecting or using user information without documentation of their technology and the explicit consent of the user. However, the bill does not address the use of facial recognition in non-commercial settings including law enforcement.

RESEARCH QUESTION AND METHODS

The research question this paper covers is: What are the detrimental effects of biased facial recognition AI algorithms used by law enforcement in criminal investigations on people of color? This question is important to ask because FRT, which has become one of the most critical and commonly used technologies in law enforcement, poses special risks of disparate impact for historically marginalized communities.

In order to answer this question, I investigated media accounts, online articles, and prior research of widely known examples of wrongful arrest due to FRT inaccuracy. I investigated both the development and application of FRT, and the challenges associated with creating complex, unbiased "smart" technology. Additionally, I interviewed Dr. Sheng Li, a professional researcher who has done extensive research in the field of facial recognition technology. I asked him several questions including "How difficult it might be to make good algorithms that reduce bias in FRT and how do you define 'good'", "What are some of the challenges that come with creating and using FRT?", "What do you think of law enforcement use of FRT?", and "How do you think engineers can work to improve FRT technology to prevent inaccuracies?". These questions were chosen in order to get a better understanding of the scope of the challenges that come with creating and using FRT, gain insight into this problem of bias and its relevance in industry and research, as well as how future engineers can improve this technology to prevent inaccuracies and wrongful arrests. Finally, I investigated three cases where FRT has been inaccurate or has led to wrongful arrests due to a person having darker skin: Robert Williams, Michael Oliver, and Nijeer Park (Johnson, 2022). By analyzing these cases, I point to how FRT discriminated against people based on the color of their skin and how that issue can and should be addressed.

RESULTS

The advancement of facial recognition technologies and artificial intelligence algorithms, coupled with the use of these FRT systems by law enforcement, have led to several ethical and social controversies. Analyzing the current state of FRT, and the interactions between the main actors helped to think about the future challenges and how each group has a need to accept a joint obligation to better create and utilize FRT in a safe and ethical manner. The social and cultural contexts in which FRT is deployed has exacerbated existing biases, such as in law enforcement settings, where FRT has disproportionately affected certain minority groups. Bias has arisen among several different actors: the developers of the technology, the people who create and prepare the training data, and the organizations or individuals who apply the technology. Additionally, delving into specific cases showed a pattern in law enforcement use of FRT and how the investigation process can and should be adjusted to accommodate the use of assistive FRT technology in a beneficial way.

Applying the Actor Network Theory

Once we apply Latour's Actor Network Theory to the use of FRT by law enforcement, we can start to understand the perspectives and roles of each actor and the relationships between different entities within the larger network they are a part of. Below, Figure 1 shows an overview of the network, briefly highlighting each actor and motives on using FRT in criminal investigations/law enforcement cases. Concerning nonhuman actors, the FRT system itself interacts with all the other actors in the network in this scenario. Next, the dataset itself is

important as it is the foundation of the system itself and determines the accuracy. Finally, the laws and rules on the use of FRT affect how and when it is used in society. Going into the human actors, law enforcement is a primary user of FRT. They seek to utilize such technology to keep people safe efficiently and effectively. Recently, they have come under heavy scrutiny by activists and lawmakers who point out problems such as bias in this technology. Technology companies that create and distribute facial recognition technology look to advance society through automation, while also making a profit. These companies also influence the extent to which FRT can be used and how regulated it is. Next, legislators seek to regulate both the use and misuse of FRT and try to define what contexts FRT should be used in. Activists advocate for safer protocols and stricter regulations on FRT technology so that minority groups do not suffer disproportionately. Finally, proponents of FRT look to optimize and push for further automation/use of AI technologies.

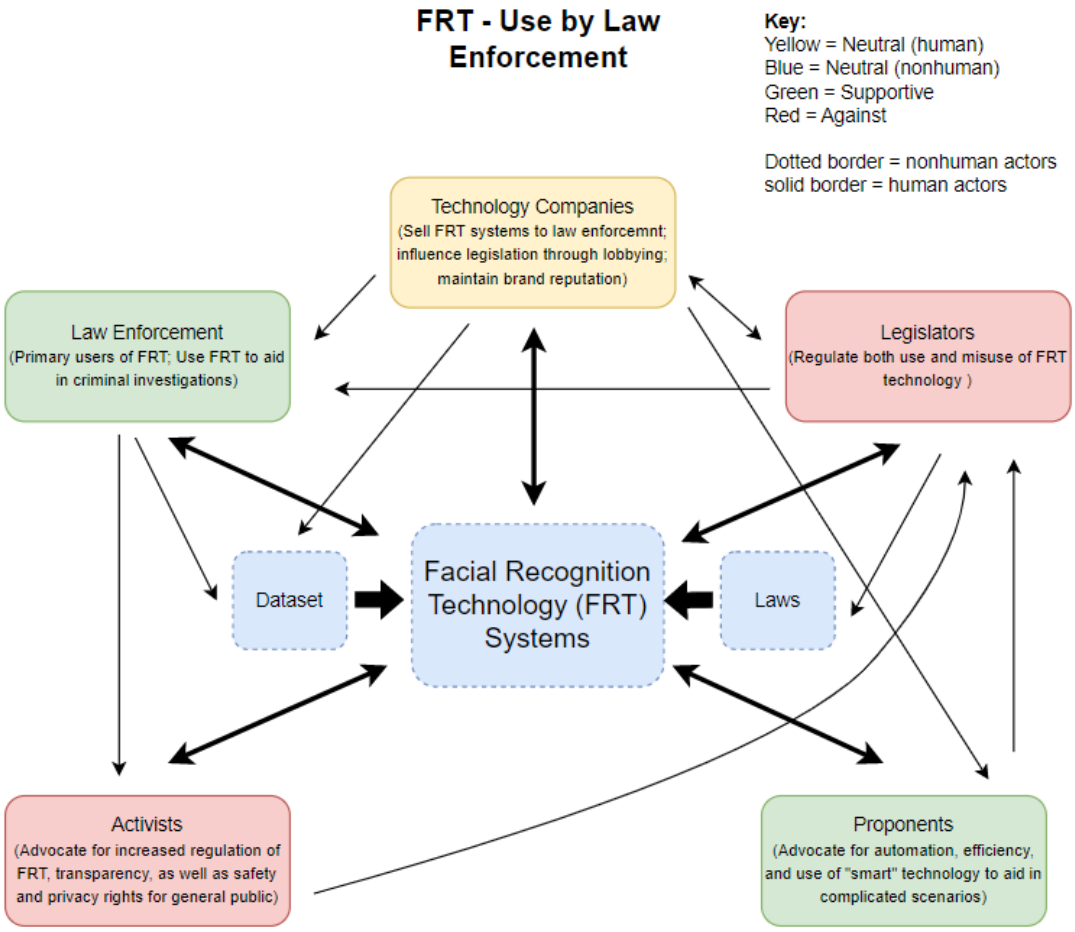

Figure 1. Main actors involved in FRT use by law enforcement, their agendas, and interactions with other actors (Iyer, 2023).

Analysis of the Main Actors

Law enforcement agencies across the country and globally rely on facial recognition for both surveillance and for aiding in criminal investigations. Police officers generally use these systems to try to match a photo of a person against a database of images. There are also techniques that allow law enforcement to use facial recognition to verify a specific person. For example, at airports, facial scanners have been used to biometrically confirm travelers' identities

(GAO, 2022). Moreover, some cities have even signed contracts for live facial recognition technology, which has the potential to change the way surveillance is conducted. Police departments say they should have access to facial recognition technology and note that it is the officers who decide who to arrest, but in some cases, the technology could provide a crucial assist. However, with this technology being largely unregulated, there are rising concerns about misuse and bias, especially when the algorithms are trained using datasets which are not diverse enough (Horowitz, 2020). Additionally, many believe that law enforcement use of these FRT algorithms crosses ethical boundaries and creates data security and privacy issues.

Law enforcement agencies acquire facial recognition systems from technology companies. However, there is little transparency into how facial recognition software developed by big technology companies is being used by law enforcement. For example, Amazon has not disclosed how many and which law enforcement agencies use Rekognition, its FRT technology (Feiner & Palmer, 2021). Moreover, some smaller companies, like Clearview AI, scrape billions of photos of people off social media, without public knowledge, to build their facial recognition system (Lively, 2021), which raises concerns about misuse of public data.

Following the Black Lives Matter protests, IBM, Amazon, and Microsoft took a stand to regulate FRT: They stopped sales of their FRT technology to U.S. police departments, and called on the government to regulate FRT. However, while these large corporations are taking a stand, it is important to note that they do not represent a major part of the FRT industry. Smaller companies like Clearview AI and Ayonix continue to sell FRT to law enforcement (Solon, 2020). What is also interesting is that many executives at these firms said the decisions made by larger corporations were motivated by political considerations (Horowitz, 2020).

Clearview AI specifically sold its algorithms to approximately 2,400 law enforcement agencies in the U.S., claims that their models are trained on data that is obtained lawfully, and plan to continue providing their technologies to police departments. NEC Corp., another company heavily involved in selling FRT to law enforcement, claims its technology could combat racism, by helping to "correct inherent biases, protect privacy and civil liberties, and fairly and effectively conduct investigations for social justice" (Fowler, 2020). However, instances of wrongful arrest due to the FRT system giving incorrect results, disputes the claims made by the companies.

Unfortunately, the focus on "big tech" companies has resulted in the media and the public focusing on the wrong actors that are only minorly involved in selling facial recognition algorithms. Recently, many activists and researchers have argued that if companies like Clearview AI continue providing the technology to police departments and attention does not shift to these companies, then new legislation will be the only way to stop facial recognition in policing (Fowler, 2020). In terms of legislation and regulation, within the United States, numerous laws have been passed at the state and local levels to regulate FRT. For example, Boston held a hearing about adopting a ban, during which Police Commissioner William Gross opposed the use of FRT because it was faulty. However, nothing much has been done at the federal level – which is arguably more important if any effective change is to be made (MacCarthy, 2021).

Proponents of FRT technology assert its usefulness in aiding to catch criminals, pointing to its usefulness in helping to track down missing children as well as violent felons. Among the success stories of FRT is the 2017 arrest of Walter Yovany-Gomez, an MS-13 gang member who was on the FBI's Ten Most Wanted Fugitives list after evading authorities for years (Simerman,

2023). Additionally, advanced technology in general helps with efficiency. With the use of facial recognition, mundane tasks that take a long time to do (like going through large databases of photos, biometric data, and other information) can be accomplished in a fraction of that time, at much lower costs.

On the other hand, activists and opponents of facial recognition technology say that in addition to the basic issue of bias in the software, the problems go beyond that. Joy Buolamwini, an FRT researcher who founded an organization called the Algorithmic Justice League, made the point that it "isn't just that facial recognition systems can misidentify faces, it's that the technology itself can be used in biased ways by governments or corporations" (Fowler, 2020). For example, surveillance with FRT could be pointed at minority neighborhoods, used to aim at immigrants, or even target people who join protests about police brutality.

Overall, it has become more clear that while there have been movements towards creating unbiased technology, little has been done to address the issues of use of such technologies in unethical ways and little has been done in terms of regulation at a national level. Firstly, establishing a standard of ethics in developing and selling FRT is necessary to avoid bias in the technology itself. Engineers can work towards utilizing new techniques to mitigate the problem of bias in FRT. But arguably it seems more important to have more accountability at higher levels with regard to FRT, especially on the involved tech companies and law enforcement agencies. Even if algorithms become more accurate and less discriminatory towards minority groups, that does not necessarily mean that the application of this technology will be fair and non-exploitative. Such a powerful technology could indeed turn out to be dangerous if used for the wrong purposes. In order to handle this issue, the evident approach is federal regulation of the creation and use of FRT by private and public entities and more safeguards to protect

individual privacy. Trust in FRT will follow once people see that algorithms treat every group fairly and that their rights are protected.

Interview Results

In addition to analyzing media articles and online reports, I interviewed Dr. Sheng Li, an artificial intelligence researcher at the University of Virginia. Li has a background in computer and data science. He has done research work in the areas of facial recognition and visual intelligence. Li gave insight into the complexity of facial recognition, asserting that there are a lot of variables in facial data such as different color, shape, variations, etc. Altogether, face structure is quite diverse compared to object or hand detection. He discussed the future of FRT, which Li believes will involve more Deep Learning, due to this type of machine learning being able to handle a variety of variables/features and more accurately give a final prediction.

While Li mentioned that he personally doesn't have much experience or knowledge about law enforcement use of FRT in particular, he expressed that fairness is definitely important, especially across different ethnic groups. He stated that what is missing in many FRT technologies today is a feedback module which explains how a decision is made – models now only give final results. He also said that with AI technologies in particular, we want to have confidence associated with a prediction. Because if an AI system makes a mistake in law enforcement scenarios, the consequences are much more serious. Thus, in law enforcement scenarios, if FRT gives a low prediction confidence score, then we should not rely on the system too much.

Li offered what makes a "good" FRT technology and how that can be evaluated. He explained that previously people only focused on accuracy of FRT (with a validation data set). But the problem with that is there could be bias in the dataset itself. Therefore, while accuracy is a very important metric, it is not enough. FRT should be fair and able to give consistent performance for diverse groups of people. So, reliability is another important metric to consider and test. FRT should be able to recognize people in different environments, e.g. occlusions, expression changes, different glasses, colored skin, etc. Li asserted that a "good" FRT system will need to consistently produce reliable predictions in a variety of environments.

Finally, he asserted how engineers can work to improve FRT technology to prevent inaccuracies. Previously, computer scientists would design algorithms to create or improve FRT. But in this process, they only have limited observations from datasets (and datasets were collected from someone else) so this resulted in developers a limited and partial observation of the true world, which hindered their abilities to create reliable technology. Instead, a more beneficial approach would involve combining the observations/feedback from experts with engineers' thoughts, to improve the overall design of FRT. Engineers can and should be involved in collecting data and testing, as well as development.

Case Analysis– Nijeer Parks, Robert Williams, and Michael Oliver

In Woodbridge, New Jersey in January 2019, Nijeer Parks was accused of shoplifting snacks and candy from a Hampton Inn gift shop. According to police reports, the shoplifter left a fake Tennessee driver's license at the scene and that photo from the fake ID was sent to a real-time crime center, which used a facial recognition system to identify Parks as a "high-profile"

match. Days later, Parks was arrested. He was able to find evidence that proved his innocence. However, even after showing that proof, charges were only dropped several months later (Johnson, 2022). This case demonstrates first how the in-house FRT systems failed to correctly identify a suspect, but also how the police officers failed to corroborate/prove the claim by FRT. This reliance on technology and failure to justify the arrest or gather further evidence, ended up in a wrongful arrest, which negatively impacted Parks' life.

Next, Robert Williams was accused of stealing $3,600 in watches from a Shinola store. He was arrested and taken to the Detroit Detention Center but a live Instagram video of him 50 miles away around the time of the theft proved he didn't commit the crime. Even with that evidence, charges against him were only dropped two months after his arrest. Williams eventually filed a suit in federal court in Michigan against former police chief James Craig, the city of Detroit, and Bussa. He stated: "The technology got relied on so heavily that they didn't even do any investigative work to find the person," (Johnson, 2022). This case also shows how reliance on technology and failure to justify the arrest or gather further evidence, ended up in a wrongful arrest.

Finally, Michael Oliver was arrested in Ferndale, Michigan in 2019, two months after Detroit police issued a warrant for his arrest for allegedly grabbing a smartphone from a teacher and throwing it on the ground. He was identified by facial recognition software based on a screenshot shared with police from the video by the teacher. Additionally, the teacher initially identified a former student as the suspect but later picked Oliver from a photo lineup. However, Oliver has several tattoos, while the person in the video has no visible tattoos. Wayne County prosecutors ultimately agreed with this evidence and dropped the charges. Afterwards, Oliver claimed that as a result of the arrest, he lost his job, and it took about a year for his life to return

to normal (Johnson, 2022). According to Patrick Nyenhuis, Oliver's public defender, the detective investigating the case appeared to take shortcuts, including failing to question Oliver or review a video of the incident before his arrest.

These cases are all instances where FRT has been inaccurate or has led to wrongful arrests due to a person having darker skin. However, looking deeper into it, there is a failure by multiple parties involved throughout the investigation process. Indeed, lawyers representing Oliver and Williams say what happened to their clients reflects both an overreliance on facial recognition and poor investigative work. Based on these cases, it seems that a dependence on this type of "smart" technology is a driving factor in wrongful arrest situations. On top of the technology being inaccurate, the application and use of FRT by law enforcement suggests that there is a flaw in decision making, situational awareness, and a sense of overconfidence in technology. In order to remedy these issues, one idea is introducing training to police officers on how to use FRT technology, especially emphasizing the technology's role as an assistant, not an ultimate decision maker. Another promising idea is having the Department of Justice investigate state and local agencies' use of face recognition for potential disparate impacts that violate their duty to avoid bias in policing.

DISCUSSION

The creation and application of facial recognition technology has potential to grow, and actions need to be taken to make sure every party involved benefits from such technology. Latour defines discrimination as when actors are excluded from a network, or when certain actors are given preferential treatment over others. From the actor network analysis we can see

how the FRT system itself does not discriminate against any actor, but the dataset it is trained on results in less accurate results for certain groups such as people of color. Developers and manufacturers have vested interests in the widespread use of their technology, and this results in bad training data and inaccurate technologies being deployed without adequate testing. The resulting exclusion from the network of accurate identification is a form of discrimination, when the technology is applied broadly (such as in law enforcement). Moreover, law enforcement agencies have the power to decide how and when to use the technology, and which individuals to target. They may exert their power in unfair ways by utilizing FRT to target certain groups of people, such as marginalized communities and specific racial groups. This can lead to unfair treatment and unequal access to justice, which is a form of racial discrimination. Overall, the use of facial recognition technology by law enforcement raises important issues related to discrimination.

FRT is not the only artificial intelligence technology that is raising concerns. There are plenty of examples that point to the discriminatory harm by AI tools to already marginalized groups. The main reason behind this is that AI is built by humans and deployed in environments that have ingrained discrimination (e.g. criminal legal system, housing, workplace). That's why it is important to take steps to bring up ethics, fairness, and equity when discussing technology policies, and to actively address any issues these technologies bring (Akselrod, 2021).

There were some limitations to this research. First, it would have been beneficial to be able to get feedback and insight from professionals in the law enforcement field. However, it is difficult to gain access to any material related to an investigation or to obtain interviews with law enforcement, especially concerning issues of bias. Moreover, it is also difficult to get interviews from big tech companies without a broad network or direct connections. Thus, for this project it

was easier to interview research professionals associated with my university who have also done work with FRT. Additionally, I would have liked to have more interviews done, but due to timeline/scheduling differences and unavailability of professionals, this was not possible. Overall, the conclusions of this research should be further explored, with insights from a more diverse group being taken into consideration.

In terms of future research, there are a few extensions that would be valuable. Firstly, it would be better to conduct interviews and gather information from a more diverse population. Especially getting information from law enforcement professionals would be beneficial to understand their outlook on this issue. I would also focus more on getting viewpoints from both supporters and opponents of law enforcement's use of FRT to fairly evaluate both the pros and cons of FRT (this research paper is heavier on the cons of FRT). Secondly, another way to evaluate this research question would be to survey the general population about their thoughts/opinions on facial recognition technology. The issues of privacy and data security when using FRT for surveillance are important concepts that can be analyzed, and surveys on the public can help address that. Thirdly, looking into specific companies that produce facial recognition technology, such as Clearview AI, Amazon, or Idemia, could provide insight into the creation of FRT, the complexity of the algorithms, and bias that arises while developing such technology. To better understand the responsibilities of those creating such technology and how engineers can combat this bias, looking into specific companies that produce FRT may provide more details.

Throughout this research process, I was able to delve into this issue by exploring a variety of sources as well as discussing it with experienced professionals. Even informally, watching news clips about facial recognition and documentaries such as "Coded Bias" was

helpful in understanding this research question. Being exposed to many different sources of information was useful in considering the impacts of FRT and the challenges that lie ahead in making/using it ethically, safely, and efficiently. Engineers play an important role in providing solutions to some of the biggest global challenges and they'll have a huge impact on the future. Thus, it is really important for engineers to understand how their inventions will impact society and be mindful of all the potential consequences (including dangers) their designs have. Moreover, users of technology also have a large role in how it affects all of us. Overall, in the widely connected world we live in, it's definitely useful to have meaningful discussions about the implementation and implications of technology we create.

CONCLUSION

Facial recognition technology is powerful and could have lasting effects on the way law enforcement performs surveillance and conducts criminal investigations. Analyzing the creation and use of FRT as well as using frameworks like ANT to explore the actors and their relationships is beneficial to visualize ways we can improve it as well as future challenges that lie ahead. We can see where improvements should be made. First of all, it is important that the public is educated about potential biases in facial recognition technology and its limitations. This will raise awareness about the risks of using this technology and empower individuals to protect themselves and their privacy. We also have to work to increase diversity in both the datasets used for training the algorithm and also on development teams themselves, to mitigate bias. Based on research and analysis, key requirements of the successful implementation of FRT use by law enforcement include clear ethical standards for development, regulating the creation and use of FRT by both private and public entities, as well as introducing training for police officers

to use FRT as an assistive technology in addition to other evidence/investigation. Collaboration between the different actors is also essential to advance FRT. With these factors in mind, FRT has the potential to positively impact society, when utilized for criminal investigation by law enforcement. Next steps could involve delving deeper into existing regulations as well as what the federal government can do to better protect individual rights while also keeping the benefits of FRT.

REFERENCES

Akselrod, O. (2021). How Artificial Intelligence Can Deepen Racial and Economic Inequities News & Commentary. American Civil Liberties Union. Retrieved from: https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can-deepen-racial-and-economic-inequities

Feiner, L., & Palmer, A. (2021). Rules around facial recognition and policing remain blurry. CNBC. Retrieved from: https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html

Fowler, G. A. (2020). Black Lives Matter could change facial recognition forever — if Big Tech doesn't stand in the way. Washington Post. Retrieved from: https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/

Gentzel M. (2021). Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy. *Philosophy & technology*, 34(4), 1639–1663. https://doi.org/10.1007/s13347-021-00478-z

Goodwin G. (2021). Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees. United States Government Accountability Office GAO-21-105309. Retrieved from https://www.gao.gov/assets/gao-21-105309.pdf

Hill, K. (2020). Another arrest, and jail time, due to a bad facial recognition match. The New York Times. Retrieved from https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

Horowitz, J. (2020). Amazon and Microsoft stopped working with police on facial recognition. For others it's still big business. CNN Business. Retrieved from: https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html

Johnson, K. (2022). How Wrongful Arrests Based on AI Derailed 3 Men's Lives. Wired. Retrieved from: https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

Jones C. (2021). Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation. *North Carolina Journal of Law & Technology*, 22, 777-815. Retrieved from https://scholarship.law.unc.edu/ncjolt/vol22/iss4/6

Klosowski, T. (2020). Facial recognition is everywhere. Here's what we can do about it. Wirecutter: Reviews for the Real World; The New York Times. Retrieved from https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

Latour, B. (1992) 'Where are the missing masses? The sociology of a few mundane artifacts', in Bijker, W. E. and Law, J. (EEs) *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Cambridge, MA, MIT Press, pp. 225-258.

Lee N., Chin C. (2022). Police surveillance and facial recognition: Why data privacy is imperative for communities of color. Retrieved from

https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

Li, S. (2023, February 28). *Personal Interview*

Lively, T. K. (2021). Facial Recognition in the US: Privacy Concerns and Legal Developments. ASIS. Retrieved from: https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/

MacCarthy, M. (2021). Mandating fairness and accuracy assessments for law enforcement facial recognition systems. Brookings. Retrieved from: https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/

Ratnayake, R., Kankanamge, N., Silva, C., Steen, J., & Czarniawska, B. (2017).How can I use actor network theory? Retrieved from https://www.researchgate.net/post/How_can_I_use_Actor_Network_Theory

Simerman, J. (2023). What is facial recognition technology, and how do police use it? 5 things to know. NOLA. Retrieved from: 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=Facial%20recognition%20technology%20has%20allowed

Solon, O. (2020). Big Tech juggles ethical pledges on facial recognition with corporate interests. NBC News. Retrieved from: https://www.nbcnews.com/tech/security/big-tech-juggles-ethical-pledges-facial-recognition-corporate-interests-n1231778

Symanovich S. (2021) What is facial recognition? How facial recognition works. Norton. Retrieved from https://us.norton.com/blog/iot/how-facial-recognition-software-works#

U. S. Government Accountability Office. (2022). Facial Recognition Technology: CBP Traveler Identity Verification and Efforts to Address Privacy Issues. GAO. Retrieved from: https://www.gao.gov/products/gao-22106154#:~:text=As%20of%20July%202022%2C%20CBP%20has%20deployed%20FRT%20at%2032

Williams, T. (2015). Facial Recognition Software Moves From Overseas Wars to Local Police. The New York Times. Retrieved from: https://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html