Rohan Anand
4/24/24
DS 380
Professor Wildman

A Case for a More Comprehensive Policy Surround Facial Recognition

The rapid advancement of facial recognition technology has led to its adoption in a number of sectors. This technology, which uses computer algorithms to identify individuals based on their unique facial features, has allowed companies to streamline user identification, offering more efficient and intuitive interactions. For example, both iPhone and some Android devices have moved away from fingerprint scanning, while social media platforms such as Meta are implementing it to automatically tag friends in photos. Additionally, airports utilize these programs to identify suspicious individuals and retailers to gather more information about consumer habits and preferences. However, the integration of this relatively new, unrefined technology has raised many ethical concerns, particularly regarding the potential invasion of privacy as governments and companies store user profiles without their explicit consent as well as the bias perpetuated by these algorithms. For example, the use of facial recognition in law enforcement has led to the wrong arrest of a minority due to the decreased accuracy rate of identification for people of color. In addition to the difficulty of expunging his record, the event could have potentially caused significant psychological distress to both himself and his family, who witnessed him being dragged away without apparent cause, in addition to an increased distrust in government institutions that are responsible for protecting citizens. As a result, the aim of the deployment of these softwares should be reevaluated, as it should be treated as a tool to correctly identify and remove perpetrators of crime, instead of the solution to streamlining arrests. In order to do so, the facial recognition algorithm must be able have consistent accuracies across all demographics of the U.S., as well as strict standards of accountability to prevent the abuse of this technology by police departments. As facial recognition technology continues to become more heavily integrated with policing, a comprehensive policy that aims to promote accuracy and fairness in its algorithms with respect to the civil liberties of citizens, as well as guidelines that ensure accountability and transparency regarding its use will allow it to be used as a tool to establish safer communities.

Facial recognition algorithms have been slowly developing for the last quarter of a century. However, its widespread use can be credited to two factors: the recent developments in AI and government funding to streamline police investigations. On the former, the invention of deep convolutional neural networks, a self-training machine learning algorithm, is particularly adept at identifying faces, due to its ability to recognize general patterns and textures in its images (NIJ). The similarity of the human facial structure allows the algorithm to discern easily recognizable qualities, and the complexity of the network is able to distinguish variations in cheekbone structure, eye shape, etc. to correctly identify a single person in a sea of individuals. On the latter, the National Institute of Justice has provided funding, both internally to other universities, such as Carnegie Mellon, on the condition it be used to advance similar software. However, as with any machine learning algorithm, the amount of data is key benchmark in determining its accuracy. As a result, the FBI has been using "… over 641 million photos—including driver's licenses, passports and mug shots…" in order to train its algorithms (Melton). Recently, the ubiquitous use of social media has also been beneficial for training data, as law

enforcement is able to access multiple angles of the same individual as well as their associate with others, mirroring the still frames as part of an ongoing video feed. Despite the seemingly magical ability of these algorithms, its accuracy is not consistent across predominant demographics in the U.S. According to a professor at the University of Calgary, "[when using] facial recognition technology, there is over 99 per cent accuracy rate in recognizing white male faces. But, unfortunately, when it comes to recognizing faces of colour, especially the faces of Black women, the technology seems to manifest its highest error rate, which is about 35 per cent." Similarly, according to the Gender Shades Project, in the majority of facial recognition algorithms realized by prominent tech companies, those with darker skin complexions have consistently lower accuracy (Najibi). Extrapolating to the larger U.S. racial demographic, the algorithm could potentially fail on upwards of 37% of people, comprised of Hispanics/Latinos, African Americans and Asians, etc. (Jensen, Jones, Rabe, Pratt, Medina, Orozco, and Spell).

However, the skewed accuracy is not a deterrent for its increased adoption by police departments. Police in Lima, Ohio have already implemented the use of a mobile device capable of sound, facial and license plate recognition. The technology is being described as a "force multiplier", adding labor force to a department plagued by manpower shortage. Once deployed on the streets, it will reduce response times significantly, allowing less officers to patrol a larger area (Grundy). An increase in crime prevention efficiency with less officers is seen as an achievement by the public, but the streamlining of these algorithms to replace police work can lead to over policing, harming the same community that this technology is meant to protect. According to a report by the U.S. Government Accountability Office, 7 agencies in the Department of Homeland Security and Justice used facial recognition without requiring their staff to submit to training, which only increased to a measly 2 in April of 2023 (GAO). As a result, law enforcement agencies, who are not privy to the inherent biases present in these algorithms, have made arrests based on to false suspect identifications. For example, Robert Williams, a black man in Detroit, "spent more than a day in custody at a Detroit detention center in January after an incorrect facial recognition match led to his wrongful arrest", due to the system incorrectly flagging his driver's license. The event left him feeling "humiliated", and could have potentially caused psychological distress to his young daughters, who saw him dragged off in handcuffs without apparent reason. Although "the American Civil Liberties Union alleges this is the first known wrongful arrest in the U.S. because of facial recognition technology", the misuse of these algorithms can escalate this singular mistake into a pattern of abuse across the nation.

Theoretically, the pool of individuals who could be potentially affected by false arrests can be all private citizens, as "more than half of American adults were enrolled in a face recognition network searchable by law enforcement" (Georgetown). However, the stakeholders that are most at risk are those in high-crime neighborhoods in densely populated areas. Police office shortages are rising across the country amid negative general sentiment, particularly affecting areas such as New York City, where the active number of police officers have decreased 3.5% in 10 years, and in 2023, the organization had 600 more officers leave than join (Mastronardi). As a result, the department searches for cost-effective measures to replace them, leading to the adoption of facial recognition. As a result, the technology is deployed in more crime-heavy areas, including Mott Haven, Bronx, where 93% of residents are Hispanic or African-American, and Bedford-Stuyvesant, Brooklyn, where over 40% of the population is African American (Furman). The inherent bias in the algorithm will lead to an increased number of false arrests, adding unnecessary complications to an already struggling community. However,

this is not to say that similar circumstances cannot occur in higher-income neighborhoods. The prevalent use of social media has led to the accumulation of millions of identifying photos of its users, which the platforms are unreluctantly allowing law enforcement to utilize for its algorithms. Although less likely, the average citizen can oneself victimized due to facial recognition. To address this issue, a more comprehensive policy that regulates this technology and protects the data of private citizens from unconsented use needs to be implemented.

Such as policy must guarantee four main changes: an increase in accuracy to justify its use on the general population, laws requiring training to mandate responsible use, and informed consent regarding the use of social media data. The general rule on the accuracy of machine learning models is as follows: "The precision of a machine learning model is very sensitive to the quantity of the training data. In most cases, the model's accuracy improves as the size of the training dataset grows" (Marshall). As a result, the discrepancy in accuracy in current facial recognition algorithms is not inherent, but can be addressed by training on more multi-racial datasets that have an equal distribution of all of the major racial demographics in the U.S. Racial demographics also vary year-to-year, which also requires that both the training data be updated frequently. Similarly, new advances in AI should also be incorporated into existing algorithms, as these can also improve accuracy. In order to ensure the consistent reliability of these systems, independent, third-party data scientists should perform regular audits to establish acceptable error margins on identification and standardize any results across multiple algorithms. Doing so will ensure that any algorithms that national or local law enforcement decides to use will have consistent accuracies to prevent any discrimination. The results of these audits should also be published in publicly available reports to garner support for the reliability of these algorithms in policing. Additionally, real-time monitoring should be in place to catch any systemic errors that could lead to false arrests. Implementing these changes will provide a fairer and more equitable algorithm that policy can rely on.

However, guarantees of a more accurate algorithm can foster streamlining in police work, causing officers to rely on facial recognition to name perpetrators, rather than finding suspects to interview and rule out. As a result, the policy needs to mandate, on a national level, training for officers who will engage with this technology in order to be informed about its capabilities and limitations as well as be versed its ethics to prevent misuse. The current trend in policing indicates that facial recognition is used as a criminal locator, which is dangerous because it can cause substantial harm to innocent people, as seen in the Detroit case. However, with an informed view of its uses, departments can transition to using the algorithm as a product that outputs potential suspects, which they can then research and interview for an alibi before booking them. This way, officers are using facial recognition as a tool instead of a substitute for detective work, maintaining the dignity and civil liberties of every citizen. To alleviate this issue further, state governments should allocate more resources towards the police, so that officers are able to comfortably do the necessary work before making arrests. The release of financial constraints will help the sentiment that the technology should be making the arrests, instead of the officers. Similarly, departments will also be aware of lower accuracies for people of color, and can exercise the appropriate amount of caution before arresting them. There is also a stark difference between the training data, mugshots, driver's licenses, passport photo, which are taken in a well-lit area, illuminating the features necessary for the algorithm to develop a high accuracy, and potentially blurry stills from a security camera, which can lead to false positives from the algorithm. As a result, on a department basis due to the variance of footage from different types of cameras, there must be a minimal baseline of image and resolution quality

before using facial recognition to prevent false positives. Since facial recognition can also be used to spy on law-abiding individuals, officers need to be educated on the ethics of abusing such a program. In order to do so, partnerships with local colleges can be forged so professors can inform them about the distrust generated by the public if their law enforcement were caught spying.

Lastly, the policy should include a national law requiring local police departments to ask its citizens whether they consent to provide their social media being used to enhance their facial recognition algorithms. In addition, law enforcement agencies should disclose the specific information on the model and partnerships with companies that provide any algorithms and training data. Similarly, local departments should build a profile of images, data, etc. that citizens can request, in order to promote transparency in policing methods. Doing so will build public trust in the seemingly invasive policing methods. By employing a national policy that encompasses the three mentioned facets, facial recognition can be responsibly employed as an innovative tool to support police departments that is accurate, anti-discriminatory, and respectful of the private data of citizens.

However, it is important to recognize that the proposed policy changes are not intended to expand the use of facial recognition, but rather ensure that is used in a responsible and transparent fashion. Proponents who argue this rebuttal are concerned about facial recognition becoming a blanket surveillance measure that can be abused by the government. While this concern is valid, and there is precedent in the form of Edward Snowden whistleblowing on the NSA, the difference is the ability of citizens to request data from their respective police departments (Reed). This transparency acts as a check on the ability of the police to endless collect data, and any misstep can lead to mass protests, prompting the larger federal government to implement changes. Similarly, another criticism that could be levied is the additional funding needed for police departments can come at the expense of arguably more helpful community resources, such as homeless shelters, or mental health crisis intervention. However, this can be alleviated by increasing taxes on the wealthy, whose disposable income will not be severely impacted. This way, departments can get the funding they need without harming other outreach resources.

In conclusion, the rapid advancement and adoption of facial recognition technology in various sectors, most notably law enforcement, has raised significant concerns regarding accuracy, fairness, accountability and privacy. As a result, a comprehensive policy overhaul is needed to improve the accuracy of these across all demographics by training them on representative datasets, while also mandating training for officers to educate them about the technology's capabilities, limitations, and ethical considerations, as well as promote transparency regarding the use of social media data from citizens. By adopting such a policy, facial recognition algorithms can be transformed into a valuable, innovative tool for law enforcement that respects civil liberties and promotes safer communities for citizens of all backgrounds.

Works Cited

"Crime-Detection Tech a 'force Multiplier' for Lima, Ohio, PD." *GovTech*, GovTech, 30 June 2022, www.govtech.com/public-safety/crime-detection-tech-a-force-multiplier-for-lima-ohio-pd.

"History of NIJ Support for Face Recognition Technology." *National Institute of Justice*, nij.ojp.gov/topics/articles/history-nij-support-face-recognition-technology. Accessed 24 Apr. 2024.

Jensen, Eric. "The Chance That Two People Chosen at Random Are of Different Race or Ethnicity Groups Has Increased since 2010." *Census.Gov*, 11 Oct. 2023, www.census.gov/library/stories/2021/08/2020-united-states-population-more-racially-ethnically-diverse-than-2010.html.

"Law Professor Explores Racial Bias Implications in Facial Recognition Technology." *News*, 22 Aug. 2023, ucalgary.ca/news/law-professor-explores-racial-bias-implications-facial-recognition-technology#:~:text=In%20some%20facial%20recognition%20technology,is%20about%2035%20per%20cent.%E2%80%9D.

"Man Wrongfully Arrested Due to Facial Recognition Software Talks about 'humiliating' Experience." *NBCNews.Com*, NBCUniversal News Group, www.nbcnews.com/business/business-news/man-wrongfully-arrested-due-facial-recognition-software-talks-about-humiliating-n1232184. Accessed 24 Apr. 2024.

"Man Wrongfully Arrested Due to Facial Recognition Software Talks about 'humiliating' Experience." *NBCNews.Com*, NBCUniversal News Group, www.nbcnews.com/business/business-news/man-wrongfully-arrested-due-facial-recognition-software-talks-about-humiliating-n1232184. Accessed 24 Apr. 2024.

Marshall, Kayley. "How Does the Size of the Training Data Affect the Accuracy?" *Deepchecks*, 14 Feb. 2023, deepchecks.com/question/how-does-the-size-of-the-training-data-affect-the-accuracy/#:~:text=The%20precision%20of%20a%20machine,of%20the%20training%20dataset%20grows.

Mastronardi, Ashley. "Police Union Officials Say NYPD in a Staffing Crisis." *NYC PBA*, www.nycpba.org/news-items/news-12-brooklyn/2024/police-union-officials-say-nypd-in-a-staffing-crisis/#:~:text=The%20NYPD%20is%20understaffed%20by,decrease%20from%2010%20years%20prior. Accessed 24 Apr. 2024.

Melton, Monica. "Government Watchdog Questions FBI On Its 640-Million-Photo Facial Recognition Database." *Forbes*, www.forbes.com/sites/monicamelton/2019/06/04/government-watchdog-questions-fbi-on-

its-640-million-photo-facial-recognition-database/?sh=5f621837121f. Accessed 24 Apr. 2024.

"Mott Haven/Melrose Neighborhood Profile." *NYU Furman Center*, furmancenter.org/neighborhoods/view/mott-haven-melrose. Accessed 24 Apr. 2024.

Najibi, Alex. "Racial Discrimination in Face Recognition Technology." *Science in the News*, 26 Oct. 2020, sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

Office, U.S. Government Accountability. "Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties." *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties | U.S. GAO*, www.gao.gov/products/gao-23-105607. Accessed 24 Apr. 2024.

"Perpetual Lineup." *Georgetown Law*, www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/. Accessed 24 Apr. 2024.

Reed, Betsy. "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations." *The Guardian*, Guardian News and Media, 11 June 2013, www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.