Laura South
1600 W Plum St
Fort Collins, CO 80521

May 5th, 2017

Chief John Hutto
2221 S. Timberline Road
Fort Collins, CO 80525

Dear Chief Hutto:

As a computer science student at Colorado State University with a passion for fair implementation of criminal justice practices in the town of Fort Collins, I would like to offer the following report to all interested law enforcement officials and technologists. As chief of police, I'm certain you are conscious of the need to balance safe and regulated policing techniques with the need for modern technology that provides officer with rapid reaction times in critical situations. My paper outlines some of the risks inherent in facial recognition technology, a particular type of biometric technology that has recently grown in popularity within American law enforcement agencies. I also provide a set of recommendations that can be used by law enforcement officers and technologists alike to improve the use and creation of technology that has the potential to perpetuate social problems.

Many police departments in the Unites States have taken advantage of the commercial availability of facial recognition and detection systems. These systems can provide officers with lists of suspects very quickly in moments where quick action is critical to public safety, but all officers who use this technology have a responsibility to understand how it works and how it can be abused if used improperly. As with all forms of technology, it is imperative that the validity of the systems used by thousands of police officers each year is fully tested and fully understood by those using the technology.

Fort Collins is lucky to have a team of dedicated law enforcement officers who are willing to risk their lives to keep our community safe. I hope to help your department maintain its positive reputation by ensuring you to understand how facial recognition technology works and some of the issues still present in its functionality. This will hopefully help to ensure that facial recognition technology is used in a safe and respectful manner that works in the best interest of the Fort Collins community.

Thank you for your time and support.

Sincerely,

Laura South

Algorithmic Injustice:

An Examination of Police Reliance on Facial Recognition Software

Laura South

lsouth@rams.colostate.edu

JTC 300-001 (R02)

May 5th, 2017

Table of Contents

List of Figures

Algorithmic Injustice:

An Examination of Police Reliance on Facial Recognition Software

Abstract

Facial recognition software systems have been used by the U.S. government in war zones for years to identify threats and target suspects, but recently similar applications of computer vision software have been adopted by federal, state, and local governments and law enforcement agencies. This paper examines the connection between facial recognition systems and law enforcement in the United States and identifies areas of concern related to the validity of this technology. Several types of sources were consulted, including academic studies on the legitimacy of commercially available facial recognition packages and existing demographic biases in law enforcement departments. My analysis clearly illustrates a dangerous connection between American police departments and potentially biased facial recognition technology. When considered in the larger context of over-incarceration of people of color in the U.S., law enforcement's reliance on an untested and unregulated form of technology like facial recognition software is especially concerning. My report ends with a set of recommendations that is twofold; technologists need to put more effort into creating reliable, non-discriminatory facial recognition systems and law enforcement officers must be dedicated to understanding the technology they are relying on to make decisions that have the potential to permanently alter the lives of people in their community.

Algorithmic Injustice:

An Examination of Police Reliance on Facial Recognition Software

Introduction

According to a 2016 report published by the Georgetown Center on Privacy and Technology, over 117 million U.S. adults are included in a law enforcement face recognition network (Garvie et al.). In at least 26 states, these networks are based off of driver's license or other ID photos, not police photographs (Garvie et al.), so subjects are often not aware of their inclusion in these systems. In October of 2016, the ACLU publicly voiced concerns about the risks of facial recognition technology in a letter to the Department of Justice, stating that "…law enforcement use of face recognition technology is having a disparate impact on communities of color, potentially exacerbating and entrenching existing policing disparities" (American Civil Liberties Union, 1). A report written by Government Accountability Office in July of 2015 seconded these concerns, stating that if the use of facial recognition systems "became widespread, it could give businesses or individuals the ability to identify almost anyone in public without their knowledge or consent and to track people's locations, movements, and companions" (Government Accountability Office, 1). The same report also noted that "no federal privacy law expressly regulates commercial uses of facial recognition technology" (Government Accountability Office, 1). In addition, computer scientists have identified potential racial bias in the computer vision algorithms behind facial recognition software, but the severity of this issue is still largely untested and has not drawn much support from the technical community. The purpose of this paper is to examine existing research on the implicit biases of facial recognition as it relates to police actions, identify potential areas of concern in the application of facial recognition

technology to police matters, and recommend actions to be taken by technologists and police officers alike who are concerned about this issue.

Perspectives on Facial Recognition and Law Enforcement

How facial recognition technology works

At their most basic level, algorithms are simply mathematical sets of instructions that can be given to computers in the form of software. Most often their role is simple and relatively risk-free, like storing, sorting, or displaying data. However, recent increases in processing power have allowed for more complex algorithms, including ones that can analyze millions of data sets all at once. Facial recognition software is a prime example of a complex algorithm with outcomes that can carry profound real-world consequences – like whether someone is considered a suspect in a criminal investigation. This type of software requires computers to compare live video feeds with millions of images stored in a database every second.

Machine learning

This seemingly insurmountable amount of analysis is tractable because of a field of computer science called machine learning. Arthur Samuel, an early founder of the field, defined machine learning in 1959 as the "field of study that gives computers the ability to learn without being explicitly programmed" (Samuel, 210). This burgeoning field of computer science involves the analysis of algorithms that "train" computers to solve a problem through trial and error and a basic reward system. To train a machine learning algorithm, a researcher must expose it to what is known as a learning set – basically a miniature version of the world that the algorithm will encounter when it is put into practice. The program studies this learning set closely and begins to

make assumptions about the connections present within this snapshot of the outside world. Then the program is given a small amount of information about a user and asked to predict other pieces of information about that person, based off its learning set of information. If the computer is correct, it receives a positive signal and adjusts the "weights" in its internal judgement algorithms to account for a success. After thousands of repetitions, the program ends up with a sophisticated ability to discern between various types of people and even match faces with identities.

Overfitting and other risks in facial recognition algorithms

Algorithms are viewed as precise and scientific creations, incapable of the same demographic biases that humans have cultivated throughout existence. In fact, algorithms often can be found to hold the same implicit assumptions as their creators when tested. This is particularly evident in machine-learning based algorithms due the previously mentioned learning set that is used to train the machine. Research has shown the dangers of a phenomenon called "overfitting", which occurs when the learning set used to train the machine learning program is not representative of the population it is exposed to in practice (Garvie et al., 9). When applied to facial recognition technology, this usually means a learning set that is not diverse in terms of race, age, and gender.

Facial recognition algorithms face several other unique risks, even when compared to other common forms of biometric authentication. The most well-knowns type of biometric authentication is fingerprinting, which has been used by law enforcement officials for decades. According to Professor Laura Donohue, an expert on technology law at Georgetown University, finger printing falls into a category of identification methods known as "Immediate Biometric Identification" (IBI). IBI is defined to include all identification systems involving "the use of

biometrics to determine identity at the point of arrest, following conviction, or in conjunction with access to secure facilities" (Donohue, 415). Facial recognition systems, on the other hand, fall into a category called "Remote Biometric Identification" (RBI), meaning they "give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner" (Donohue, 415). This illustrates an important difference between the two common biometric identification systems: fingerprinting is a one-time activity that gives officers a specific amount of information about a person, whereas facial recognition has the potential to be continuous and invasive, if not properly regulated by law enforcement officials and law makers.

Identifying bias in algorithms

In academic settings, the experimental design and testing process of new algorithms are often readily available to all who are interested. However, many algorithms used in government or in private industry are not clearly documented or made available to the public, even though they affect more people and can have devastating consequences if errors are made. Research on demographic biases within computer vision algorithms is sparse, but the papers that have been published have found evidence of various demographic biases, including racial differences, in recognition accuracies. One of the first studies on this topic was completed by computer science researchers at Colorado State University in 2003 who analyzed several popular facial recognition algorithms and compared their performance across various groups, covering demographics like race, gender, and age. As can be seen in Figure 1, their research has showed that the facial recognition systems tested had different levels of success at "identifying" subjects of different

races (Givens et al., 6). This result was confirmed by a more recent study, completed in 2012, that examined three commercially-available computer vision packages and found that "all three commercial algorithms were consistent in that they all exhibited lower recognition accuracies on the following cohorts: females, Blacks, and younger subjects" (Klare et al., 13). Researchers believe this is due to "overfitting" – the unintended consequence of choosing a training set mostly comprised of white faces when building the machine learning algorithms that govern the decisions made by facial recognition software.

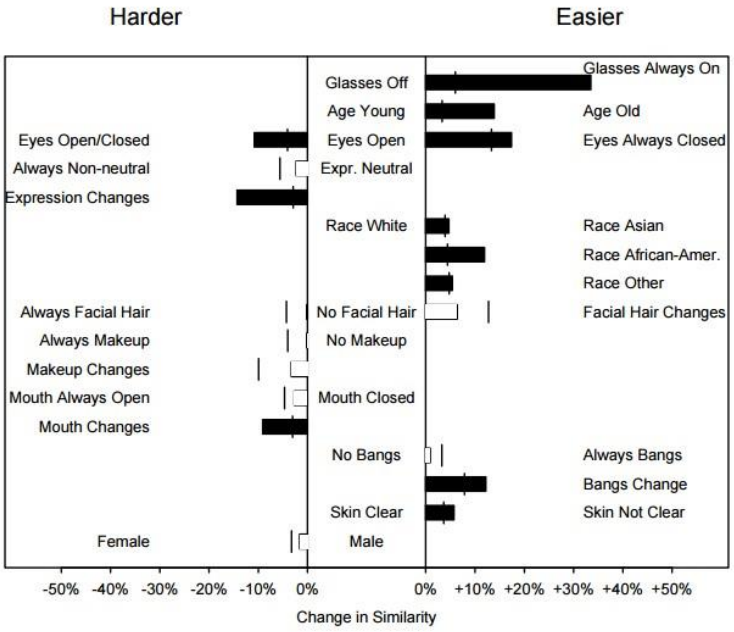

Figure 1: Results demonstrating significant differences between recognition rates of various demographic groups (Givens et al., 6)

This theory is supported by results obtained from a separate component of the same study, where researchers ran separate experiments with different "trainable" facial recognition algorithms that could be customized to train from different learning sets. They found that the recognition accuracy of these algorithms was improved when a diverse training set was used. To put it simply, this research suggests that a computer trained on a mostly white dataset (like several commercially available products) is more likely to incorrectly identify non-white subjects in the future. Due to the sociopolitical relevance of this technology, even a slight deviation along demographic lines should not be acceptable.

The role of facial recognition technology in law enforcement

Background

A report published by the Georgetown Center on Privacy and Technology estimated that "more than one in four of all American state and local law enforcement agencies can run face recognition searches of their own databases, run those searches on another agency's face recognition system, or have the option to access such a system" (Garvie et al., 25). Significant variation exists among departments in terms of how the software is used and how much consideration is given to the results of the recognition tests. Research done by Georgetown Center for Privacy and Technology surveyed 52 police departments that use facial recognition technology and found that only 25% of these departments require "individual suspicion" (meaning either probable cause or reasonable suspicion) prior to ordering a facial recognition search for a suspect (Garvie et al., 37). This means that the remaining 75% either have

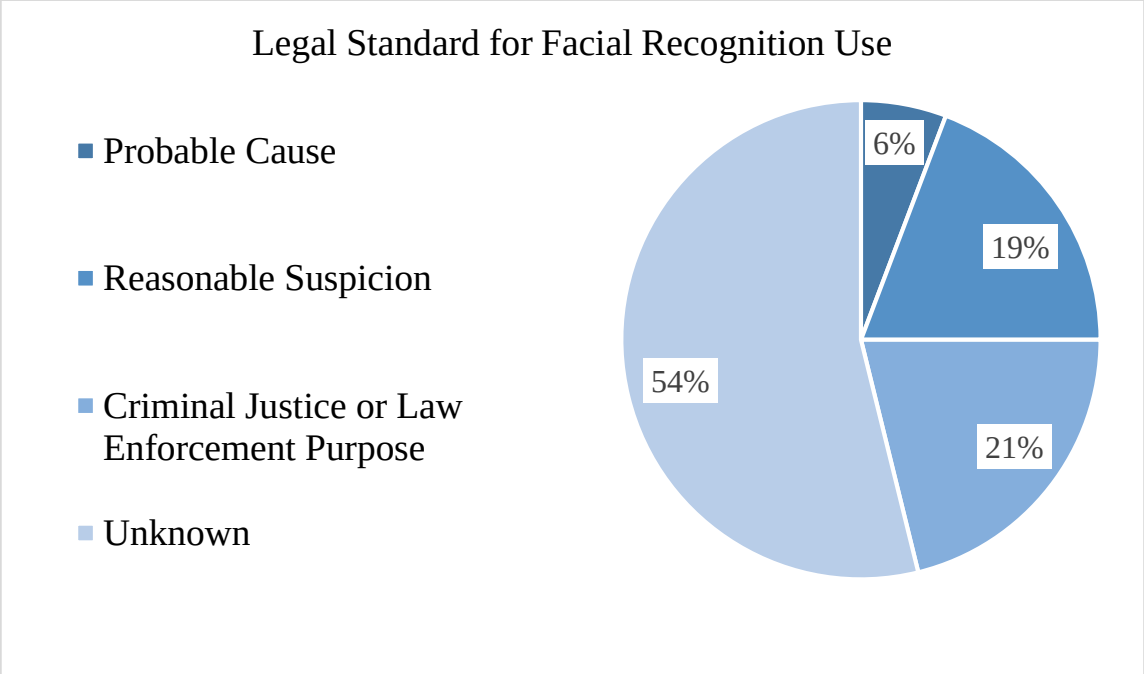

Figure 2: Results of facial recognition use policy survey administered to 52 police departments in the United States (Garvie et al., 38)

undocumented policies for the use of this technology or can use it for any purpose related to law enforcement. These results can be seen in Figure 2 (for more details, please see the Appendix). If this sample is reflective of the larger attitude within law enforcement towards the use of this powerful technology, it represents a serious area for potential conflicts of interest and abuse of power. When considered in conjunction with research supporting the presence of bias within the networks used by these departments, this is even more concerning.

Recent cases where facial recognition was used by police officers

Police departments across the country are particularly sensitive to public opinion right now, due to recent incidents where police officers have acted in ways that were unfavorable to many citizens. Several of these incidents have involved the use of facial recognition technology, so it is important to consider these cases when examining the proper use of facial recognition technology in the criminal justice framework. In May of 2014, Steve Talley was arrested in a particularly violent manner in Denver as a suspect for a recent case involving a bank robbery after being identified by an FBI facial recognition network (Kofman). His charges were dropped in November after officials determined that the facial recognition network's results were inaccurate. Talley, however, was arrested a second time just one month later, when a separate facial recognition search once again identified him as the perpetrator. This was proven to be a false identification when the sole witness to the crime testified that Talley was not the same man who robbed the bank where she was working as a teller. Similar cases have cropped up across the United States. The best way for police departments to avoid public outcry through misuse of facial recognition technology is to dedicate themselves to understanding the risk areas present

within this technology and to use it in a responsible, critical manner when dealing with their community.

Societal Implications

Several prominent organizations have spoken out about the societal risks posed by police overreliance on facial recognition technology, including the American Civil Liberties Association and the Government Accountability Office, as mentioned earlier in this report. It is important to bring attention to connection between biased technology in the hands of law enforcement and existing problems with the overincarceration of minorities in the United States. According to a report sponsored by the National Association for the Advancement of Colored People, "African American and Hispanics comprised 58% of all prisoners in 2008, even though African Americans and Hispanics make up approximately one quarter of the US population" (NAACP). If American law enforcement officers continue to rely on demographically biased forms of biometric identification, like facial recognition technology as it exists today, the overincarceration problem could get even worse, as more people of color are falsely identified by algorithms that were never built to accurately categorize non-white faces.

Conclusion

Facial recognition technology is an important potential tool for police officers in the United States. It has been developed and refined out of machine learning research for many years, but there are still crucial problems that can easily go unnoticed when this technology is used by people who lack a fundamental understanding of the hidden machinations behind each tool. The solution to this problem is twofold; technologists have a responsibility to create

reliable, non-discriminatory facial recognition systems and law enforcement officers have a responsibility to understand the technology they are relying on to make decisions that have the potential to permanently alter the lives of people in their community. Technology is no longer an optional part of society. It’s time to work together to ensure that technology works to erode our implicit biases and social problems, rather than subtly reinforcing them.

References

1. American Civil Liberties Union. “Coalition Letter to U.S. Department of Justice Civil Rights Division Calling for an Investigation of the Disparate Impact of Face Recognition on Communities of Color”. 18 October 2016.
2. Donohue, Laura K. "Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age." Minn. L. Rev. 97 (2012): 407.
3. Garvie, Clare et al. “The Perpetual Line-up: Unregulated Police Face Recognition in America.” Georgetown Center on Privacy and Technology (2016).
4. Givens, Geof, et al. "A statistical assessment of subject factors in the PCA recognition of human faces." *Computer Vision and Pattern Recognition Workshop, 2003. CVPRW'03. Conference on*. Vol. 8. IEEE, 2003.
5. Government Accountability Office. “Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law”. GAO-15- 621. July 2015.
6. Klare, Brendan F., et al. "Face recognition performance: Role of demographic information." *IEEE Transactions on Information Forensics and Security* 7.6 (2012): 1789-1801.
7. Kofman, Ava. "How A Facial Recognition Mismatch Can Ruin Your Life". *The Intercept*. N.p., 2016. Web. 5 May 2017.
8. National Association for the Advancement of Colored People (NAACP). “Criminal Justice Fact Sheet”. 2017.
9. Samuel, A. L. "Some Studies In Machine Learning Using The Game Of Checkers". *IBM Journal of Research and Development* 3.3 (1959): 210-229. Web.

Glossary

Immediate Biometric Identification (IBI) - all biometric identification systems involving "the use of biometrics to determine identity at the point of arrest, following conviction, or in conjunction with access to secure facilities" (Donohue, 415).

Remote Biometric Identification (RBI) – all biometric identification systems that "give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner" (Donohue, 415)

Overfitting – modeling error that occurs in facial recognition algorithms when the learning set used to train the machine learning program is not representative of the population it is exposed to in practice

Machine learning – a rapidly growing research area of computer science that "gives computers the ability to learn without being explicitly programmed" (Samuel, 210) and plays a key role in the algorithms that govern facial recognition systems.

Appendix

In a report published in 2016 by the Georgetown Center on Privacy & Technology, 52 American police departments were surveyed about their usage policies for facial recognition technology. The chart below summarizes the findings, listing the name of each department that was included in the study. In this instance, "medium risk deployments" are defined to be targeted searches for a specific individual run against a limited database (i.e. not including law-abiding citizens) and "high risk deployments" are defined to be targeted searches for a specific individual run against a database that does include law-abiding citizens (Garvie et al., 19).

	LEGAL STANDARD	ALL AGENCIES	MODERATE RISK DEPLOYMENTS	HIGH RISK DEPLOYMENTS
INDIVIDUALIZED SUSPICION REQUIRED	PROBABLE CAUSE	Maryland DPS Michigan State PD Albuquerque PD, NM	Albuquerque PD, NM	Maryland DPS Michigan State Police
	REASONABLE SUSPICION	Carlsbad PD, CA Chula Vista PD, CA SANDAG, CA San Diego PD, CA Honolulu PD, HI Iowa DPS *Cumberland Co., ME* King County SO, WA Seattle PD, WA South Sound 911	Carlsbad PD, CA Chula Vista PD, CA SANDAG, CA San Diego PD, CA Honolulu PD, HI *Cumberland Co. SO, ME* King County SO, WA Seattle PD, WA South Sound 911	Iowa DPS
INDIVIDUALIZED SUSPICION NOT REQUIRED	CRIMINAL JUSTICE OR LAW ENFORCEMENT PURPOSE	FBI FACE Services Pinellas Co. SO, FL Chicago PD, IL *Illinois State PD* Prince George's Co., MD Michigan State Police Minnesota DPS Lincoln PD, NE Ohio BCI Virginia State PD NOVARIS, VA WVI/FC	Chicago PD, IL Prince George's Co., MD Minnesota DPS Virginia State PD NOVARIS, VA WVI/FC	FBI FACE Services Michigan State Police Pinellas Co. SO, FL *Illinois State PD* Lincoln PD, NE Ohio BCI
	UNKNOWN	Maricopa Co. SO, AZ *Arizona DPS* LA Co. SO, CA Los Angeles PD, CA San Diego Co. SO, CA San Francisco PD, CA *San Jose PD, CA* Daytona Beach PD, FL Jacksonville SO, FL Miami PD, FL Palm Beach Co. SO, FL Tampa PD, FL Hawaii CJDC *Auburn PD, MA* *New Bedford PD, MA* *Plymouth Co. SO, MA* Maryland State PD Baltimore PD, MD Montgomery Co. PD, MD Kansas City PD, MO Nebraska State PD Pennsylvania JNET Pennsylvania State PD Carlisle Borough PD, PA Philadelphia PD, PA Texas DPS Fairfax Co. PD, VA *Pierce County SO, WA* Snohomish Co. SO, WA	LA Co. SO, CA San Diego Co. SO, CA San Francisco PD, CA *San Jose PD, CA* Hawaii CJDC *Auburn PD, MA* *New Bedford PD, MA* *Plymouth Co. SO, MA* Kansas City PD, MO Texas DPS Fairfax Co. PD, VA *Pierce County SO, WA* Snohomish Co. SO, WA	Maricopa Co. SO, AZ *Arizona DPS* Los Angeles PD, CA Daytona Beach PD, FL Jacksonville SO, FL Miami PD, FL Palm Beach Co. SO, FL Tampa PD, FL Maryland State PD Baltimore PD, MD Montgomery Co. PD, MD Nebraska State PD Pennsylvania JNET Pennsylvania State PD Carlisle Borough PD, PA Philadelphia PD, PA

Figure 3: Expanded results summary from police facial recognition use survey (Garvie et al., 38)