Using Care Ethics to Examine Police Use of Facial Recognition Technology

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Ross Bonnin

March 1, 2020

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.

Signed: 

Approved:
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

On January 24th, 2020, the New Jersey attorney general officially banned the use of Clearview AI, a controversial facial recognition app. Clearview AI is utilized by many law enforcement agencies, most notably London's Metropolitan Police Service. Despite being used by many different police forces, Clearview has received significant backlash in their utilization of social media profiles and pictures for their facial recognition database, even receiving cease and desist letters from Twitter, Google, Youtube, Venmo, and Facebook (Tarantola, 2020). New Jersey's ban of Clearview AI by police forces has received a polarized reaction from the general public, with many praising the decision, citing the public's discomfort with what is considered to be a breach of privacy, and their worry about the potential for abuse of power by law enforcement agents with access to a large database of personal information (Gurman, 2016). Others, including Clearview's CEO, maintain that all information held by Clearview was, "at one point, placed in the public domain" (O'Sullivan, 2020), and that the technology is solving crimes and finding child victims of sex-trafficking (Hill & Dance, 2020). However, neither of these reactions account for the moral duty of care that New Jersey's law enforcement owes to the citizens of New Jersey, and how the attorney general's actions upheld or breached that duty of care. If the power dynamics between the New Jersey police force and its citizens, and the resulting duty of care that the police force owes the citizens are ignored, an important ethical aspect of New Jersey's ban of Clearview AI will be lost.

I will demonstrate that the New Jersey legislature acted morally in its ban of police utilization of Clearview AI, because the use of facial recognition technology breaches law enforcement's duty of care towards its citizens with respect to the competence and

responsiveness of the care. I will examine the use of facial recognition software by law enforcement by using the ethical framework of care ethics, and explain that the use of facial recognition software by police forces breaches their duty of care to the citizens they protect and serve.

Literature Review

The use of facial recognition technology (FRT) by police agencies has been the subject of significant scrutiny from scholars. A large majority of the analysis centers on the morality of FRT's use by law enforcement based on whether or not its use is a violation of privacy.

In *Super Bowl Surveillance: Facing Up to Biometrics*, John Woodward Jr. (2001) highlights an example of when FRT was used by police during Super Bowl XXXV. At the Super Bowl "surveillance cameras surreptitiously scanned spectators faces to capture images" and then "this faceprint was then instantly searched against a computerized database of suspected terrorists and known criminals to recognize a specific individual. A match would have alerted police to a potential threat" (Woodward, 2001). Woodward argues that the use of facial recognition during the Super Bowl would be constitutional and not breach the public's right to privacy. In fact, Woodward argues, compared to a metal detector or a public checkpoint, the facial recognition implemented at the Super Bowl was not physically invasive or intrusive, and thus protected the physical privacy of those that might deal with higher scrutiny from law enforcement (Woodward, 2001).

Adam Schwartz, of the American Civil Liberties Union of Illinois (2013), looks at Chicago's police surveillance system, and contends that unregulated police surveillance, when coupled with FRT, is a significant violation of privacy. Schwartz warns that "if the government

systematically monitors *where* we are in public places, the government will learn *who* we are," and if left unchecked, that the government would be able to scrutinize the entirety of our lives. He asserts that a reasonable member of the general public does not expect law enforcement to keep track of their whereabouts, "whether they are entering a political or union meeting, viewing a controversial movie or art exhibit, visiting a psychiatrist or a fertility clinic or a plastic surgeon, attending church or mosque or synagogue, distributing leaflets, or meeting a criminal defense attorney" (Schwartz, 2013).

While both scholars make compelling arguments about the potential legality or constitutionality of the government's use of FRT, neither argument appropriately accounts for the care that law enforcement owes its citizens based on the power differential of their relationship. While it is important to consider the public's right to privacy with respect to the implementation of FRT, it is also important to understand whether the act of implementing FRT by the police is inherently moral or immoral. I will analyze the morality of New Jersey's facial recognition ban through the lens of the care that police forces owe their citizens.

Conceptual Framework

The morality of New Jersey's decision to ban Clearview's facial recognition app can be analyzed using the theory of care ethics, and how it dictates the relationship between New Jersey's police force and the citizens they serve. Care ethics stemmed from Carol Gilligan's work, and emphasizes the importance of context and emotional interaction with respect to the development of moral principles (van de Poel & Royakkers, 2011). Care ethics recognizes the role that dependence and vulnerability play in relationships, particularly in relationships with unequal power distribution. Scholars of care ethics believe that when there is an asymmetry of

power in a relationship, it is significantly more important to be conscious of one's role in that relationship and to understand how much care is owed to the other party. Care can be defined as "a species activity that includes everything we do to maintain, continue, and repair our 'world' so that we can live in it as well as possible" (Tronto, 1995). Put simply, care is naturally associated with attentiveness, responsibility, competence, and responsiveness (Tronto, 1995).

With respect to care ethics, attentiveness deals with the awareness that care is required in a particular situation. Responsibility can have many definitions, but can most simply be thought of an obligation to provide adequate care based on need (Verhoek, 2014). Competence, the third aspect of care, deals with the quality of care given. To adequately care for another, it is not enough to attempt to give care; the care needs to adequately meet the other's needs. Finally, responsiveness involves an understanding of one's position with respect to others. With responsiveness, an understanding of relationship power differentials is imperative in order to not abuse relationships where one member is at a disadvantage.

I will examine New Jersey's ban on Clearview AI's facial recognition app with respect to care ethics by explaining the care that law enforcement owes its citizens, and then utilizing Tronto's aspects of care to demonstrate how facial recognition software breaches the care owed to citizens by police forces.

Analysis

The New Jersey government acted morally in its ban of police use of Clearview AI's facial recognition software. It is well established that police and law enforcement agencies have a duty of care to the citizens of their municipalities; the state police of New Jersey states as much in the mission statement they have on their website, specifically "to protect, preserve, and

safeguard the constitutional and civil rights of all citizens through impartial and courteous law enforcement," and to "ensure the highest quality service to the public" (New Jersey State Police [NJSP], n.d.). The implementation of FRT can lead to a detriment of the quality of service to the public, and the utilization of large databases of private information frequently leads to abuse of power. Based on the definition of care with its four subcomponents, the implementation of FRT by the New Jersey government would breach the competence and responsiveness aspects of care. The following sections examine how law enforcement's care is not competent or responsive when FRT is used.

Competence

Implementation of FRT would result in a failure of New Jersey's police force to meet the competence aspect of care ethics and cause them to not meet the care they claim to provide. In care ethics, competence involves providing adequate care. The care that the New Jersey police force owes to its citizens has been well defined through mission statements like the one of the New Jersey State Police mentioned above. The competence of New Jersey's police can be defined on how closely their actions match the care that they have self-prescribed. For example, South Wales Police of the United Kingdom recently reported on a facial recognition trial at a sporting event. The FRT of the trial found 2,470 matches, of which 2,297 were false positives (Zeng et al., 2019). The error rate of this trial, around 92%, is incredibly high, but concerningly is not an isolated event. London's Metropolitan Police had false positives in 34 of its 42 matches, making for an error rate of over 80% (Zeng et al., 2019). The inaccuracy of FRT is of serious concern to police forces. If police are overwhelmed with false positives, they will spend a significant amount of time investigating innocent people, possibly disturbing their lives and

wasting the increasingly valuable time of police officers. The police will be significantly less effective at their job, which will result in law enforcement being unable to provide "quality service," and could fail at its protection of innocent citizens breaching the competency of their care. If the police cannot trust the matches that FRT outputs, the technology will likely remain unutilized and, if the technology is highly inaccurate, unable to be utilized in court (Zeng et al., 2019). Underutilization of FRT would be a waste of police resources and unduly stress the budgets of police forces, which further reduces the scope of care the police can give the public. Ultimately, the combination of inaccurate facial matches and ethical questions of FRT can undermine public perception of the legitimacy of the police (Neyroud & Disley, 2008). When the legitimacy of the police is in question, the public is less likely to obey or cooperate with the police, and legitimacy is very closely tied with trust or distrust of police. Lack of police legitimacy and distrust of police cripples the ability of law enforcement to function effectively (National Institute of Justice, 2013). When police lose their authority, legitimacy, and their ability to effectively protect the public, the care they give to the general populace loses all competence.

As I have argued, FRT has negative consequences on the quality of care that can be given by police forces, including their legitimacy in the eyes of the public. The decrease in quality of policing means that police forces are not showing competence in care. However, not everyone sees FRT as a detriment to the quality of care given by law enforcement. Some, using a technological mediation framework, believe that an inherent "technological impartiality" (Woodward, 2001) to FRT would allow officers to delegate certain ethical decisions to technology, and would be a benefit to the quality of care given by police forces. Woodward uses

delegation to consider the current issue of racial profiling that many law enforcement officials have to deal with. “While humans are adept at recognizing facial features, we also have prejudices and preconceptions” (Woodward, 2001). These prejudices manifest themselves when police stop a disproportionate amount of members from a certain ethnic, racial, or religious group. Woodward believes that FRT’s lack of bias would lessen the impact of any prejudices or preconceptions. “With biometrics,” Woodward claims, “human recognition can be relatively ‘human-free’ and therefore free from many human flaws” (Woodward, 2001). What this view fails to consider is that technology is not impartial or bias free; many scientists and engineers, knowingly or unknowingly, insert their own biases into the technology that they create. In Langdon Winner’s famous paper, *Do Artifacts Have Politics?* he lays out how many technical artifacts can benefit certain groups while marginalizing others (Winner, 1980). The biases of these technologies do not have to be intentionally designed into the artifacts; the biases can be unintentionally put into the artifacts - as Winner says, it is possible that “the technological deck has been stacked long in advance to favor certain social interests, and that some people were bound to receive a better hand than others” (Winner, 1980). To this effect, a study in 2011 found that facial recognition algorithms developed in East Asia recognized East Asian faces with more accuracy than Caucasian faces, with the opposite result being true for FRT created in Europe and the United States (O’Toole et al., 2010). In fact, recent research has shown that facial recognition might actually perform worse on demographics who have experienced disproportionate amounts of police attention, particularly African American men and women (Garvie & Frankle, 2016). This means that African Americans would be more likely to be misidentified by facial recognition software, which will lead to an unequal amount of innocent African Americans being

investigated by the police. Police interrupting the lives of innocent citizens at an increased rate already begins to breach the competence of care, but when those innocent citizens already experience disproportionate scrutiny by the police, it completely breaches the police's self-proclaimed care to protect "all citizens," and to provide "impartial" law enforcement. (NJSP, n.d.)

Responsiveness

The implementation of FRT by New Jersey's police force would also result in a failure to meet the care ethics aspect of responsiveness. As Tronto, and care ethicists as a whole define it, responsiveness deals with the power dynamic between two groups when care is owed. Responsive care ensures that one group does not use its position of power to take advantage of or abuse the other group. It is clear that law enforcement agencies already hold a significant amount of power over citizens, but with FRT, this power differential is significantly increased. All facial recognition technologies utilize a large database of personal information, which police officers would have access to. Police access to an even larger amount of personal information shifts the already one-sided power dynamic even more one sided, but there is a very concerning trend of law enforcement officials abusing their access to databases of private information. Over the course of 2 years, more than 325 police officers were fired, suspended, or resigned due to misuse of databases full of private information (Gurman, 2016). As reported by the Associated Press "a Denver officer became acquainted with a hospital employee during a sex-assault investigation, then searched out her phone number and called her at home. A Mancos, Colorado, marshal asked co-workers to run license plate checks for every white pickup truck they saw because his girlfriend was seeing a man who drove a white pickup." These examples illustrate the very real

possibility of misuse and abuse of police databases. Concerningly, in over 90 cases, the punishment imposed was not specified, if any punishment was given at all (Gurman, 2016). Furthermore, many departments did not give the Associated Press any records of database misuse; according to Gurman (2016), "some states refused to disclose the information, siad they don't comprehensively track misuse or produced records too incomplete or unclear to be counted. The databases that the Associated Press considered only consist of information about criminal history or driver information. The implementation of FRT would provide an additional, much more intimate, database of personal information. This information, when used for personal gain of law enforcement officers, could result in additional, more significant abuses of the power disparity in the relationship between the police and citizens. Police use of FRT, after a clear trend of personal information database abuse, would be incredibly irresponsible, and breach law enforcement's responsiveness of care.

Abuse of database information is especially concerning with respect to the police force of New Jersey and Clearview AI. Instead of realizing the potential of abuse when police are given access to a vast database of the public's faces and information, Clearview actually encouraged police officers to use the database for personal use. Buzzfeed news acquired an email to the Green Bay Police department, where Clearview encouraged abuse of its own database:

> Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney
>
> Your Clearview Account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. (Mac et al., 2020)

Clearview's casual encouragement for police to "run wild" with their searches shows a callous disregard of the potential for abuse of power to occur due to the use of their software. Encouraging officers to search their friends and family brings up innocent citizen's personal information, and the jump from friends and family to romantic interest or workplace rival is not very difficult. Through their actions, Clearview is enabling and encouraging the misuse of their database. Rather than understanding that having access to a significant amount of very personal information can and has caused issues with abuse of power, and creating ways to ensure the database is not being misused, Clearview has not shown any understanding of the delicate balance when law enforcement has access to personal data in order to optimize the technology. Police utilization of a database that is owned by a company that shows such little regard for the potential of misuse by police will lead to a significant abuse of power, and entirely breaches any semblance of responsiveness of care.

Conclusion

The morality of the New Jersey government's decision to ban Clearview AI's Facial Recognition software can be understood using care ethics to determine that New Jersey acted morally in banning police use of Clearview AI's FRT. Using Joan Tronto's elements of care, it becomes clear that police use of facial recognition breaches the care that law enforcement owes its citizens with respect to competence and responsiveness. Many scholars discuss FRT based on its implications to privacy and public safety. This can cause argumentative gridlock, because people do not all agree on the respective importances of privacy and public safety. By looking at this situation from a moral viewpoint, it becomes easier to see how citizens are affected by the decision to implement facial recognition software by the police.

Word Count: 2957

References

Garvie, C. & Frankle, J. (2016, April 7). Facial-recognition software might have a racial bias problem. *The Atlantic*. https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/

Gurman, S. (2016, September, 28). *AP: Across US, police officers abuse confidential databases*. AP. https://apnews.com/699236946e3140659fff8a2362e16f43

Hill, K. & Dance, G. (2020, February 7). Clearview's facial recognition app is identifying child victims of abuse. *The New York Times*. https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html

Mac, R., Haskins, C., & McDonald, L. (2020, January 28). *Clearview AI once told cops to "run wild" with its facial recognition tool. It's now facing legal challenges*. Buzzfeed News. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits

National Institute of Justice. (2013). *Race, trust, and police legitimacy.* https://nij.ojp.gov/topics/articles/race-trust-and-police-legitimacy

New Jersey State Police. (n.d.) *Mission statement*. https://www.njsp.org/about/mission-statement.shtml

Neyroud, P. & Disley, E. (2008) Technology and policing: Implications for fairness and legitimacy. *Policing: A Journal of Policy and Practice, 2*(2), 226-232. https://doi.org/10.1093/police/pan017

O'Toole, A. J., Phillips, P. J., Narvekar, A., Jiang, F., & Ayyad, J. (2010) Face recognition algorithms and the "other-race" effect. *Journal of Vision, 8*(6), 256-256. https://doi.org/10.1167/8.6.256

O'Sullivan, D. (2020, February 10). *This man says he's stockpiling billions of our photos*. CNN. https://www.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html

Schwartz, A. (2013). Chicago's video surveillance cameras: A pervasive and poorly regulated threat to our privacy. *Northwestern Journal of Technology & Intellectual Property, 11*(2), 47-60.

Tarantola, A. (2020, February 2). *Why Clearview AI is a threat to us all*. Engadget. https://www.engadget.com/2020/02/12/clearview-ai-police-surveillance-explained/

Tronto, J. (1995). Care as a basis for radical political judgements. *Hypatia, 10*(2), 141-149.

van de Poel, I. & Royakkers, L. (2011). *Ethics, technology, and engineering: An introduction*. Wiley-Blackwell.

Verhoek, M. (2014). *Practicing care: The relationship between justice and care assessed and put into practice*. [Master's thesis, Radboud University]. Radboud Educational Repository.

Woodward, J. D. (2001). *Super Bowl surveillance: Facing up to biometrics*. RAND Corporation. https://www.rand.org/pubs/issue_papers/IP209.html

Winner, L. (1980). Do artifacts have politics? *Daedalus 109*(1), 121-136. Retrieved January 27, 2020 from https://www.jstor.org/stable/20024652?seq=1#metadata_info_tab_contents

Zeng, Y., Lu, E., Sun, Y., & Tian, R. (2019) Responsible facial recognition and beyond. *arXiv preprint arXiv:1909.12935*.