Analysis of NYPD Officers with Virtue Ethics

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

By

Adam Hershaft

May 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: __Adam Hershaft________________

Approved: ______Benjamin Laugelli___________________ Date ______5/1/2020___________
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

In recent months, several NYPD officers have been using a facial recognition application, Clearview AI, which was rejected by the department for a number of concerns by the department's facial recognition unit. The Clearview app scrapes images from social media sites, and uses a massive database to identify individuals for law enforcement purposes.

The use of facial recognition technology (FRT) by law enforcement has been analyzed on the department level to determine whether FRT is adequate and accurate for police use. However, such analyses fail to consider the moral dimensions of the NYPD officers using software rejected by the department's Facial Identification Sector.

If we neglect to see the moral dimensions of the officers, we may never understand how we are being robbed of our civil liberties to privacy. Additionally, by not understanding the moral implications of the scenario, we may fall victim to misconceptions about FRT and the benefits it can bring.

I argue that the NYPD officers acted immorally in their use of the Clearview app, ignoring the rejection of the software by their organization. I will use virtue ethics to evaluate the morality of the police officers using the app. More specifically, I will demonstrate how the officers lack three core character virtues of the NYPD: Reducing fear, exhibiting a high standard of integrity, and having respect. Through a lack of practice and performance of these virtues, I will show how the officers can be deemed morally irresponsible and unprofessional.

Background

Dozens of police officers from the New York Police Department (NYPD) have been actively using a facial recognition application, Clearview AI, disobeying direction from the organization. The Department's facial recognition division tested the application over a 90-day period in early 2019, and deemed the software unfit for use for a myriad of concerns. Despite the rejection of the software, NYPD officers have continued to use the application.

Clearview AI utilizes a database of images scraped from social media sites and public sources in order to promote the functionality of its facial recognition capabilities. Twitter released a cease and desist for Clearview AI claiming that its image collection violates Twitter's terms of service. Other organizations such as Google, YouTube, and Facebook released their own cease and desist letters shortly after, and threaten action if Clearview AI continues to violate their policies. Clearview creator Hoan Ton-That was previously involved with the viddyho.com phishing scam in 2009.

Literature Review

Scholarly research has recently started to discuss the use of FRT and predictive algorithms at the law enforcement level as governmental departments have begun to incorporate this technology into their operations. One analysis has been done on the public support of law enforcement agencies incorporating facial recognition software with body worn cameras (BWC). Another analysis discusses how FRT poses a potential threat to citizens' right to privacy, and mentions a need for consensus on how facial data should be used in the private and public sectors. While several scholars have examined public reaction to FRT, and the existence of a right to privacy of biometric data, scholars have not yet adequately discussed the morality behind officers from the NYPD utilizing the Clearview application despite the department's facial recognition unit passing on the technology.

Authors Daniel Bromberg, Étienne Charbonneau, and Andrew Smith discuss the concerns surrounding facial recognition and its adoption in *Public support for facial recognition technology via police body-worn cameras: Findings from a list experiment*. This work argues that despite various organizations trying to discredit FRT as inaccurate and invasive of civil liberties, facial recognition is already approved in some form by a majority of states, and is already in use by police departments of eight major cities (including New York City). The authors claim that FRT and its integration with the widely accepted use of body-worn cameras is an inevitable reality. In the experiment conducted, it was determined that a majority of survey respondents support facial recognition with BWCs, however support decreased once respondent's answers were anonymous (Bromberg, Charbonneau, & Smith, 2020). While the authors do determine that there exists support for the adoption of facial recognition by law enforcement agencies, they fail to discuss the morality of officers who use technology that their department disapproves of.

Sharon Nakar and Dov Greenbaum analyze FRT, its uses on the state and commercial levels, and the concerns regarding the technology and privacy. The article, *Now you see me. Now you still do: Facial recognition technology and the growing lack of privacy*, mentions the theories of the right to be forgotten (control over identifying data) and the right to anonymity (anonymity in a public space), and how these legal frameworks can be applied to ease privacy fears regarding FRT. The authors claim that governmental intervention is necessary to set standards for how FRT data should be collected and handled by government agencies and private companies to prevent privacy infringements (Nakar & Greenbaum, 2017). While the article mentions valid concerns regarding a need to protect privacy during use of FRTs, the article fails to address the moral implications of law enforcement officers who use FRT against the rules set in place by their organization.

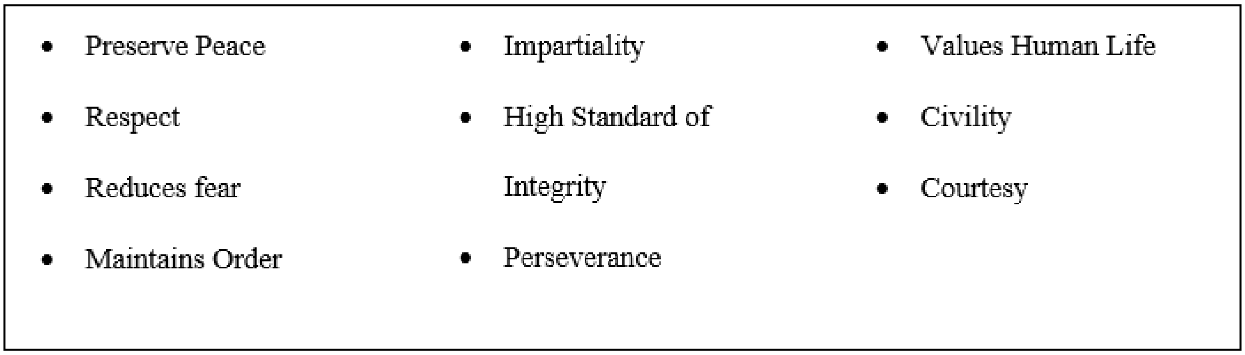
While public support for FRT is important to understand how citizens feel with regard to the use of their biometric data, it is insufficient in looking at the morality behind the use of disapproved FRT software. Additionally, while it is valuable scholarship to discuss how legislation and rules should be applied to set standards for FRT, it does not provide insight on the morality of individuals who use FRT in an unprofessional manner. My analysis will fill in the gaps of previous literature to discuss the morality of NYPD officers using the Clearview application despite the NYPD facial recognition unit passing up on the technology.

Conceptual Framework

My analysis of the NYPD police officers utilizing the Clearview AI application draws on the ethical framework of virtue ethics, which allows me to study the moral character of the officers in question. The concept of virtue ethics focuses on the moral character of an actor in order to judge whether or not he/she is a morally good and responsible individual (van de Poel & Royakkers, 2011). First developed by Aristotle, this ethical framework claims that humans should strive to live a harmonious life of reason and wisdom, known as “The Good Life”, where an individual acts according to a series of virtues.

In order to live to the highest good, an actor must practice and perform the appropriate virtues when called upon. However, each virtue exists as the median between two extremes. For example, the cardinal virtue of courage sits at the equilibrium between cowardice and recklessness. In making the right choices for a particular action, an actor must implement practical wisdom in order perform a particular virtue and not fall victim to the outlying vices.

Aristotle argues that what is good can sometimes be ambiguous. Given this, how can actors be held morally accountable if the virtues are not explicitly stated or implicitly understood? I argue that with regards to an individual acting as an actor under a larger organization, that actor should be held accountable for the promotion and practice of the organization's core values, which function as a set of virtues that govern professional practice. Since the actors are police officers under the NYPD, I will judge the morality of these individuals based on their adherence to the mission, vision, and values set forth by the department. In analysis of the mission of the NYPD, the following virtues are expected of each officer (New York Police Department [NYPD], n.d.):



- Preserve Peace
- Respect
- Reduces fear
- Maintains Order
- Impartiality
- High Standard of Integrity
- Perseverance
- Values Human Life
- Civility
- Courtesy

Figure 1: Virtues Identified from NYPD Mission, Vision, and Values

In his discussion of the virtues and responsibilities for engineers, Michael Pritchard mentions, with reference to a list of virtues for engineering professionals, that “lacking them [virtues] detracts from responsible engineering practice in general, and exemplary practice in particular” (Pritchard, 2001). I expand on this idea of Pritchard, claiming that for any professional, divergence from a list of virtues for that profession deems an individual irresponsible and thus immoral by the standard of virtue ethics.

I will use the framework of virtue ethics to analyze the adherence or divergence of the NYPD officers to the above list of virtues set forth by the NYPD. In doing so, my analysis will discuss particularly the virtues of reducing fear, having a high standard of integrity, and respect in order to better understand the morality of the officers' actions.

Analysis of Evidence

I argue that the NYPD officers who have used or continue to use Clearview AI's application are morally irresponsible because they lack the practice of necessary virtues set forth by the NYPD. Through a failure to practice and perform these virtues, virtue ethics deems these officers morally unprofessional. In the sections to follow, I will lay out how the officers' actions fail to meet the state of virtuous equilibrium for reducing public fear, maintaining a high standard of integrity, and having respect for the facial recognition unit and social media platforms involved with the Clearview platform. In doing so, I will demonstrate how in lacking proficiency of these three virtues required by the NYPD, the respective officers can be understood to be insufficient of outstanding moral character.

Reducing Fear

The police officers who continued to use the Clearview AI application despite the disapproval of the software by the NYPD demonstrated a failure to perform the department's core virtue of reducing fear. The responsibility of a police officer in reducing fear requires multiple considerations. Along with crime prevention, the entirety of a policing body must act to maintain the existence and perceived existence of safety among the community in order to reduce fear. Additionally, reducing fear requires that a law enforcement body understand with upmost comprehension the civil liberties so as to not infringe upon the explicit and implicit rights of citizens. As a result, one or more officers acting out of line with respect to reducing fear has the capability to incite fear with respect to the entire policing body, and thus taint the reputation of the entire department with respect to a core virtue.

The accuracy of facial recognition technology has been tested multiple times by various different organizations. Companies who specialize in FRT claim their algorithms are accurate, however in a December 2019 study by the National Institute of Standards and Technology (NIST), a wide range of accuracy was found among different developers. The results of this test identified demographic differentials among false positives by magnitudes of 10 to 100 times more likely for certain groups, showing "false positive rates are highest in West and East African and East Asian people, and lowest in Eastern European individuals" (Grother, Ngan, & Hanaoka, 2019). These findings identify facial recognition as an imperfect science characterized by racial bias and inaccuracy.

Similarly, a study by the American Civil Liberties Union (ACLU) tested Amazon's Rekognititon software, which falsely matched 28 members of congress to individuals arrested for crimes. Along with the general inaccuracy, the test also identified racial bias shown below (Snow, 2018):

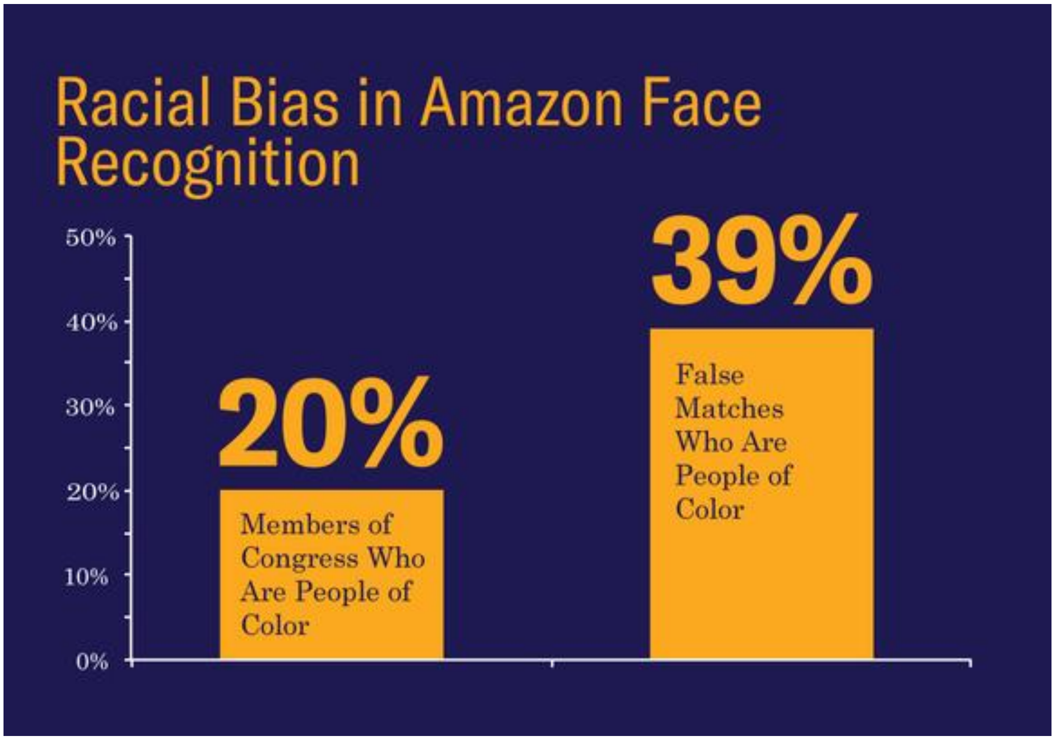


Figure 2: Racial Bias in Amazon Face Recognition

In both the NIST and ACLU studies, racial bias towards minority groups is evident. As such, FRT inherently can cause public fear in its use by law enforcement agencies. Without adherence to systems in place that prevent biasing tendencies of FRT, minority groups will be at risk of racial profiling, and thus an environment of fear will develop.

Knowing the variable accuracy of FRT, the NYPD implements various safeguards to mitigate inaccuracy. These safeguards include having facial recognition be done exclusively by the Facial Identification Section of the Detective Bureau, utilizing solely arrest photos to mitigate the likelihood of false positives, requiring additional matching evidence be present in order to arrest an individual, and by ensuring "Facial 'landmarks' are compared without reference to race, gender, or ethnicity" (O'Neill, 2019). Overall, this proves that the NYPD works to protect privacy and liberty concerning one's personal data, thus acting to reduce public fear regarding the technology's racially biasing tendencies. However, the ability of the NYPD to continually reduce fear of FRTs depends on the unwavering adherence by its officers to the safeguards set forth.

With the use of the Clearview AI app, police officers act as rogue actors and jeopardize the reputation of the entire NYPD. The use by these individuals directly disregards the safeguards of the NYPD, which stipulate that facial recognition and identification be done exclusively by the Facial Identification Section of the Detective Bureau. This alone is enough to raise public distrust of the entire policing body, and institutes a level of fear among civilians who are concerned that their personal data will be used without their consent and in an unethical manner. The facial recognition unit deemed the Clearview app unfit in meeting standards that the department set forward to prevent false positives and racial bias. When officers use the app on their own devices to conduct personal searches, they violate every safeguard the department has in place. New York City residents will be unable to determine whether their data is being used appropriately by the facial recognition unit, or unethically by these actors. As such, the use of Clearview AI promotes public fear of the NYPD and distrust of the entire department's ability to act morally responsible and promote safety.

Through the use of the Clearview application, police officers disregard the NYPD's safeguards in preventing the racially profiling tendencies of FRT systems. As these systems are in place to reduce public fear, the actions of the officers against these systems violate the department's core virtues, and thus demonstrate unethical character. Some may argue that by limiting the facial recognition database to exclusively arrest photos, the NYPD is limiting the capability of their facial recognition software to identify only previous crime offenders. These individuals would argue that in using Clearview AI's application, which utilizes an immense database of images scraped from numerous social media sites, police officers can better prevent crime by being able to identify first-time offenders and more accurately match individuals. While utilizing only arrest photos may limit searches to repeat offenders, a larger image database actually decreases the effectiveness of facial recognition software in preventing false positive matches. Patrick Grother, a computer scientist with the NIST and co-author of the study mentioned earlier claims "The larger you go, the greater the chance of a false positive…Inevitably if you look at a billion people, you will find somebody that looks quite similar" (Sydell, 2016). According to Grother, the uniformity of images in the database are important to ensure accurate results. Thus, given the variability of images from social media sites, the Clearview AI app is susceptible to misidentifying individuals and experiencing racial bias. By limiting the image database to exclusively arrest photos, the NYPD improves its ability to prevent false positive investigation. However, the entire system of safeguards, as well as the safety of civilians, rests on the compliance of the officers to the system.

High Standard of Integrity

The police officers lack the virtue of a high standard of integrity through their use of the Clearview application. This virtue is mentioned in the NYPD's mission, which pledges to "Maintain a higher standard of integrity than is generally expected of others because so much is expected of us" (NYPD, n.d.). Although how does one define discrete characteristics that make up integrity? For this, I turn to the New York State Police (NYSP) values for the similarity between the two organizations in proximity and mission. The NYSP breaks integrity up into the qualities of honesty, courage, and intolerance of unethical behavior (New York State Police

[NYSP], n.d.). I will use this concept of integrity to judge whether or not the NYPD officers truly exhibited higher standards of integrity.

The NYPD Facial Identification Section declined to use the Clearview application for multiple reasons, including the fact that it could not control who had access to the images once police uploaded one into Clearview database (McCarthy, 2020). Since the NYPD has no control of the destination and access to the images submitted, these officers are making an uneducated decision that puts the security of the entire department at risk, as well as jeopardizes the personal privacy of the citizens captured by the particular image submitted. By placing their own desires above the security and privacy of the NYPD and civilians, the officers demonstrate a lack of courage to uphold public safety, and thus possess low standards of integrity.

Since the NYPD ensures that facial recognition searches are done exclusively by the facial identification sector, it can be reasonably assumed that the level of research and understanding of FRT by the officers is limited. In using the Clearview app on their own accord, the officers are acting out of their expertise and are risking harm to civilians and the NYPD. This constitutes professional negligence, which is defined as a breach of duty of care between professionals and their clients, in which the duty of care “protects individuals from others that engage in activities that could potentially harm others if proper precautions are not taken” (“Professional Negligence Facts,” 2019). By acting negligent towards stakeholders that rely on their trustworthy actions, the officers exhibit clear signs of dishonest and unethical character.

In order the prevent such misuse of software, the NYPD ensures that unapproved software is prohibited from being installed on department phones. However, the Clearview application needs a law enforcement email address in order to be used. To get around this barrier, the “NYPD officers are loading [Clearview] onto their personal devices because they aren’t allowed to install unapproved software on their department phones.” (McCarthy, 2020). This raises a number of ethical red flags. For one, the use of Clearview on a personal device entails collection of investigative images on the officer’s personal device. This alone is an immense security concern and is both unprofessional and unethical. The NYPD claims that they ensure they use biometric technology without infringing on the public’s right to privacy, however the existence of investigative images on an officer’s personal device is an incredible invasion of a civilian’s right to privacy. Additionally, one cited concern for the use of the Clearview application was the “potential to abuse the system for extracurricular searches,” such as conducting a search of an ex-significant other to see who they are dating (McCarthy, 2020). Through the use of the app on the officers’ personal devices, the concern and potential for such abuse is magnified as personal images can be more easily sent to the Clearview database. Overall, these officers downloading the app and using it on their personal device to get around the unapproved software gateway are dishonest and unethical per se. The increased risk of these officers conducting facial recognition searches with personal images, and the possession of investigative images on their personal devices is a massive invasion of privacy, and thus demonstrates the unethical character of the officers.

The police officers using the Clearview app acted unethically in their collection of investigative images and use with disapproved software on their personal devices. This demonstrates lower standards of integrity by the officers, and jeopardizes the reputation of the NYPD as well as the safety of citizens. A contrasting argument may be posed that a facial recognition application would allow the officers to more quickly collect images to search. As a result, the processing time of finding lead suspects may be reduced, and the time from offense to arrest would decrease. However, I argue that the officers could collect images from their department phones and send encrypted messages to the Facial Identification Sector for processing without having to return to the precinct. This would reduce the time to arrest as well, however would not compromise the privacy of individuals in the investigative image. Additionally, by exclusive utilization of the facial recognition unit, the NYPD can continue to ensure no extracurricular searches are done, and that their biometric scans remain impartial, and private.

Respect

In the case of NYPD officers using the Clearview application, there exists an abundant lack of respect for various parties that the officers interact with. First, the use of the application displays a lack of respect for the citizens of New York City. As I have demonstrated in the previous sections, the use by the officers presents multiple infringements on the right to privacy of individuals, and compromises the safeguards that the NYPD has implemented with regards to biometric data and FRT. As a result, this lack of respect for privacy also opens up a door for false-positive identification, racial bias, and a sense of communal fear of the police force.

The use of the Clearview app demonstrates a lack of respect for the NYPD and more specifically, the Facial Identification Sector. The department, and this sector of the Detective Bureau took ethical means to ensure privacy of civilian data and use FRT responsibly. Through the disapproved use of the software, the officers show a blatant lack of respect for the judgement of the sector devoted to FRT, as well as for the reputation of the entire NYPD.

Finally, the use of the Clearview app shows a lack of respect for various social media sites. Twitter, Facebook, YouTube, and Google all have sent cease and desist letters to Clearview for violating their company’s terms of service. Clearview creator Hoan Ton-That claims “it’s his First Amendment right to collect public photos,” (Ng & Musil, 2020). However, it is clear from the outward disapproval by the social media sites, various legislators, and the creator’s involvement in a previous phishing scam that Ton-That and the Clearview application may be invading the privacy of the media companies and the general public. By using the app, the officers are aiding in a technology that violates these sites policies, showing a lack of respect for their organizations.

The lack of respect by the officers for the right to privacy of the public, the judgement and reputation of the NYPD and the facial recognition unit, and social media sites and their policies display poor moral character. According to virtue ethics, this failure of practice and performance of a key virtue of the NYPD attests to the professional and moral irresponsibility of the officers involved.

Conclusion

Through the context of virtue ethics, I have argued that the NYPD officers failed to perform key virtues of the NYPD of a morally responsible officer. Through a lack of respect, failure to reduce fear, and a low standard of integrity, I have shown that the cops demonstrated morally irresponsible, and unprofessional behavior, of which jeopardizes the reputation of the NYPD, and the safety of NYC civilians.

Law enforcement agencies are given a great deal of power over citizens to maintain order and keep the peace. With this power, society also places a great responsibility on law enforcers to act morally in a society that does not always follow the same moral code. Without understanding whether or when officers act immorally, we are unable to uphold society to higher standards of moral responsibility. By understanding the immoral actions of the officers, we can better protect ourselves from the abuse of power by such officers, and provide a context for the NYPD in determining whether any action needs to be brought against the officers for their immoral character.

Word Count: 3794

References

Bromberg, D., Charbonneau, E., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly, 37*(1), 1-8. https://doi.org/10.1016/j.giq.2019.101415

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FVRT) part 3: Demographic effects. *National Institute of Standards and Technology Interagency/Internal Report (NISTIR 8280)*. https://doi.org/10.6028/NIST.IR.8280

McCarthy, C. (2020, January 23). *Rogue NYPD cops are using facial recognition app Clearview*. New York Post. https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/

Nakar, S., & Greenbaum, D. (2017). Now you see me. Now you still do: Facial recognition technology and the growing lack of privacy. *Boston University Journal of Science & Technology Law. 23*(1), 88-123.

New York Police Department. (n.d.). *Mission*. About NYPD. https://www1.nyc.gov/site/nypd/about/about-nypd/mission.page

New York State Police. (n.d.). *Vision, mission, and values*. About NYSP. https://www.troopers.ny.gov/Introduction/

Ng, A. & Musil, S. (2020, February 5). *Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection*. CNET. https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/

O’Neill, J. (2019, June 10). *How facial recognition makes you safer*. NYPD Newsroom. https://www1.nyc.gov/site/nypd/news/s0610/how-facial-recognition-makes-you-safer

Pritchard, M. (2001). Responsible engineering: The importance of character and imagination. *Science and engineering ethics*, *7*(3), 391-402. https://doi.org/10.1007/s11948-001-0061-3

Professional negligence facts. (2019, December 13). LAWS. https://negligence.laws.com/professional-negligence

Snow, J. (2018, July 26). *Amazon's face recognition falsely matched 28 members of congress with mugshots*. ACLU. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Sydell, L. (2016, October 25). *It ain't me, babe: Researchers find flaws in police facial recognition technology*. NPR. https://www.npr.org/sections/alltechconsidered/2016/10/25/499176469/it-aint-me-babe-researchers-find-flaws-in-police-facial-recognition

van de Poel, I., & Royakkers, L. (2011*). Ethics, technology, and engineering: An introduction*. Hoboken, NJ: Blackwell Publishing Ltd.