Scott Hirabayashi
DATA690: Lippe

Your Face is Yours: An Ethical Look at Facial Recognition Technologies

Introduction

In 2019, Edweek reported that in the United States, there were 25 shootings on school grounds, and 51 people killed by gun violence in schools. At a time when schools have faced increasing risks of school shooters and gun violence, reasonable solutions become imperative for protecting schoolchildren. With the usage of smart, sustainable new technology, the hope is that we can improve safety for schools, common areas, businesses, and larger society. One possible answer lies in the usage of facial recognition technology.

Broadly, facial recognition is “Biometric technology that uses cameras (still images or video) to match stored or live footage of individuals with images from databases” (Feldstein, 2019). These facial recognition technologies are relatively new, and can provide safety and security benefits for parts of society, such as schools. However, as will be discussed, they also come with risks and are confronted by significant ethical issues relating to privacy and system bias, important considerations for those behind the engineering and innovating of facial recognition systems.

The scope and focus of this analysis will be to illuminate on these potential benefits and issues surrounding facial recognition technology, as well as analyzing the use of facial recognition technologies from the ethical lenses of Kantianism, Utilitarianism, Social Contract Theory, and Virtue Ethics. It will conclude with a short summary of the issues and ethical treatments presented.

Discussion of Specific Considerations for Facial Recognition Technology

Across the country, facial recognition is being adopted in US school systems. However, results for the usage of cameras have been variable. Ropek (2019) states that, in the Putnam City school district in Oklahoma, schools are equipped with cameras and facial recognition technology, which has been met with warm reception by the school system and community. The school system supported the privacy trade-off with the belief that Though the technology was improving, the hope was to expand the recognition technology to detect firearms through object recognition, adding additional layers of protection to protect campuses. However, Lockport School District in New York has met with less-positive results.

Ropek (2019) also cites backlash against the systems for their invasive tracking of students within a school. Moreover, he states multiple cases on University campuses where the technologies have been used to collect data outside the scope of the technology. Additionally, there are issues with the lack of oversight and discussion that experts say should be required for expensive, and potentially intrusive technologies. However, Ropek listed few significant problems had occurred to date.

In terms of broader security, facial recognition as a tool of larger biometric technology can yield positive benefits. Nguyen (2018), writes that biometric data can be used to protect national interests, such as in counterterrorism and national security. She considers this as a “comforting feeling”, one where we believe that we perceive “the government is watching others for us” (p. 73), though with the caveat that we assume that the government is not actually watching us, ourselves. Secondarily, she writes that, by embedding biometric data into elements of our daily lives, can improve them due to the accuracy and ease of access, for tracking medical records, financial instruments, and other elements of our daily lives.

In the medical field, Jeon et al. (2019) wrote of the specific benefits that biometric data embedding itself into current medical systems could yield positives. They conducted a pilot study to use a facial recognition mobile application for hospital patients in a hospital in Seoul, embedding facial recognition in the patient process. By testing and utilizing an application that allowed patients to log-in with facial recognition and follow them throughout their medical access and treatments, the pilot service yielded positive results compared to traditional alternatives. Impressively, the accuracy of this system was 99.99%, with a sensitivity of 99.7% and specificity of 100%.

The high accuracy of the system was captured by the fact that Jeon et al. (2019) found that inpatients were recognized “even after facial surgery” by facial recognition systems. These accuracy numbers were meaningful, as they could outperform previous methods of tracking patients. Ultimately, in this pilot study of facial recognition, they stated, “Facial recognition technology is a convenient and secure alternative compared with other biometrics for patient verification because the app requires only a mobile phone.” A minor downside mentioned was the potential issue in cases when light could decrease the accuracy of facial recognition technology due to physical limitations of the phone cameras, but with improving phone camera technologies, such problems could likely be improved as the technologies improve.

Downsides of Facial Recognition- The Privacy Trade-Off

There are more significant trade-offs to the equation of whether or not to allow these services, as well. The first major issue is the expansion of the state and invasion of privacy. China, with its embrace of facial recognition and biometric tracking, is a strong example for the fine line between protecting the population, and controlling it. Shen (2019) describes China’s full leap into Artificial intelligence and embrace of facial recognition technology. She reports that facial recognition technologies are commonplace in China, and expanding with technologies such as “Sharp Eyes 雪亮 (Snow Bright)”, a system which aims to cover all public spaces with live surveillance cameras.

Paired with the advancing capabilities of facial recognition technology- these systems afford little privacy. Reviewing Chinese facial recognition surveillance, Wright (2018) notes cases where Chinese authorities were able to detect a criminal from a crowd of 60,000 people and arrest the suspect. He cites other examples of Chinese high schools that are using the advanced technologies to scan students’ faces every 30 seconds- enough to detect students’ facial expressions.

In China, which already controls the flow of information online, the power of data collection from these technologies has been a tempting instrument for social control. Shen (2019) contends that China has created a “panopticon” - a prison where inmates don’t know if they are watched but act as if they are, in order to control behavior, Shen warns of the potential ramifications higher-levels of intrusiveness are causing in regards to society. Chillingly, she concludes “...the intrusiveness of the technologies China’s dreams of AI development are inextricably linked with the use of AI as a tool for social engineering. If China should succeed at both — vastly expanding its AI capabilities and universally deploying those capabilities towards controlling its citizens — its AI dream could turn into a nightmare for any who dare to dissent.” While the reality in many western countries is likely less dystopian, what could be a technology to protect and save could just as easily become a technology to control, even in freer societies.

Additionally, a related issue is the potential for uneven performance for minority groups that could lead to racial bias. In a review of current facial recognition technologies, Singer (2019) writes that, as a whole, facial recognition technologies may contain bias. Citing multiple studies that found poor accuracy, particularly in regards to people of certain genders and skin colors, Singer writes of a backlash against current facial recognition technologies as being error-prone for minorities, and having not improved even upon retesting. Feldstein (2019) adds to this point, saying that “under ideal conditions, facial recognition can perform very well. But when unexpected variables are thrown in… error rates begin to shoot up… facial recognition also has been unable to shake consistent gender and racial biases”. In a larger study of facial recognition, a 2019 NIST study conducted by Grother et al., found conclusions on current facial recognition technologies such as higher false positive rates in Asians, African Americans, Native groups, and African American women. Algorithmic detection was uneven, with some algorithms performing well, and others performing poorly, with equitability correlating with overall accuracy. As a whole, these studies suggest that many current facial recognition systems contain bias, and are not fully accurate.

Bias is additionally dangerous because these systems can lead to decisions in policing and law enforcement. Especially when these errors appear to occur more often with specific minority groups, it is concerning to make significant policing decisions based on mistaken or incomplete data. Widespread use of facial recognition technologies, especially in cases where they are provided as evidence, or making decisions about people, must be ensured to be extremely accurate across all groups of people. Great importance must be placed on accurate data sources and algorithms for facial recognition, to prevent biased policing and law enforcement.

Kantianism in Regards to Facial Recognition

Beginning with Kant’s quest for goodness, Kant raises the question of the categorical imperative- what is an unconditional rule that we could create (Quinn, pg. 67)? Could we unequivocally agree that using facial recognition technologies was always good? As discussed previously, there is questionable accuracy from facial recognition systems, and evidence of bias as well. Thus, we cannot universalize a rule about current facial recognition systems because the systems themselves are currently flawed. Were we to allow a flawed system into society, they would not always equitably or fairly provide safety for all, especially if they are misidentifying citizens in order to exacerbate existing bias within the current system.

Kant’s second categorical imperative asks whether or not we are using people as means to an end- if we are, then we cannot ascribe the rule as ethical. With the interest of societal security, the US is considering, and China has seemingly chosen, whether we are willing to sacrifice rights of privacy in order to achieve additional societal safety. Even if these facial recognition systems were perfectly accurate, we would still be trading the privacy of citizens in public spaces for the hope of safety. As seen with China’s “panopticon”, citizens’ behavior was changed because they knew they could be surveilled at any time; certainly, their citizens are an end to the prospect of greater safety.

Even from the perspective of a perfect facial recognition surveillance system, it would be difficult to argue that Kantian ethics could support the usage of the systems unless they were perfectly controlled and understood by those under its watchful eye. As a weakness of Kantian ethics is the conflict between rules, and the existence of facial recognition surveillance systems is a trade-off between the agreed-upon rights of privacy, and the state’s responsibility to protect its citizens, Kantianism runs into the additional trap of how to reasonably balance both questions in the form of a universalized rule, which could both be argued as ‘perfect duties’ (Quinn, p. 71).

Utilitarianism in Regards to Facial Recognition

In contrast, from a utilitarian standpoint, the primary question lies in which option creates the most net social good. Do we create more utility of ‘good’ using facial recognition technology in the public space, or does the negative trade-off, sacrificing privacy, outweigh it?

In China’s case, there is a strong belief that ultimately, “Many Chinese accept automated monitoring as a small price to pay for stability, prosperity, and social harmony” (Shen, 2019). However, in the case of the United States and western societies, where facial recognition has not saturated as much of public life. Certainly, there are safety benefits from facial recognition technologies. If these technologies lead to people feeling safer, reducing crime within communities, and a feeling of more-security, this could be a societal net-benefit. Societies have laws, and law enforcement so that we can feel more safe, which increases our happiness. With perfectly-accurate systems that are protecting citizens and enforcing laws against criminals within the system, a majority of society may agree with China's acceptance of the stability trade-off.

However, the counterargument against this positive is that the utilitarian argument is difficult to quantify. First, it is difficult to know what people are *not* doing because of being surveilled. If we were to enact the system in-full, would participants in the system feel more happiness because of their belief in the perceived benefits of safety, or would they feel worse due to their understanding of the "panopticon" effect mentioned previously, where those surveilled control and modify their actions because of their understanding that they could be surveilled? Knowing that the government may always be watching could have a profound effect on stress- as Nguyen (2018) wrote, we want to think the government is looking at *others*, but we do not want them to be looking at *us*.

I would argue that, in terms of true social good created, at-present it is certainly not worth it, as the system is flawed, participants recognize that the system is flawed, and do not think the system to be worth the incomplete safety benefits that it *might* confer. With a perfect facial recognition system, this question should be revisited, because we would need to look at comparative studies of behaviors and patterns within society. Even if we find a marked drop upon usage in crimes committed or perceptions of safety, that does not necessarily imply that happiness has increased, as people would be confronted with the 'panopticon' effect.

Social Contract Theory in Regards to Facial Recognition

The social contract theory is a general argument for the trade-off between forgoing rights for the sake of stability and protection of its citizens. We, as people, agree to forgo certain rights for the stability and protection of the state, giving up rights for the protection of others. In the United States, this revolves around the laws, Constitution, and Bill of rights that we hold dear.

One of the major negatives, particularly in the case of society, is that facial recognition systems are knowingly making tradeoffs between privacy and security for the populace. The expectation of society lies in the Constitution, "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness." When reflecting on the usage of facial recognition technologies, are our inalienable rights broken by the usage of this technology?

With the social contract, we agree in the state's power to protect us, Hobbes' theory on the "state of nature", was to protect from chaos, seeing that cooperation was essential; government is created to enforce rules to protect safety (Quinn, pg. 81). Some freedoms are given to the state to protect us. Similarly, facial recognition can protect citizens through surveillance, and may curtail some crimes.

But because the technology is flawed, it breaks several theories of the social contract. Thomas Rawls' interpretation of the social contract, attempts at a fair social contract through his ideas of a "veil of ignorance", a starting point for deciding what is ethical in a contract. From this point, Rawls' second principle of justice stipulates that inequalities must be fair and of the greatest benefit to the least-advantaged (Quinn, 84). This principle is severely infringed upon by current biases existing in many facial recognition technologies. As was previously discussed, African Americans would be unfairly disadvantaged by the usage of facial recognition technology, as it recognizes them least-accurately; moreover, the 'least-advantaged' people in society would not benefit from the racially-biased implementation of facial recognition systems.

Society must agree that the trade-off of safety for privacy is worth it, as we must be willing participants to give privacy rights to the state. As the social contract is a shared document, the citizens of the United States need to be properly informed on the trade-off that facial recognition comes with. Citizens and representatives must be equipped to understand and speak on whether or not, or to what extent, the technology is worth using. In its current form, the Social Contract theory should not allow for the usage of facial recognition, but, if the technology is improved, it may have its use within US society.

Virtue Ethics in Regards to Facial Recognition

Virtue Ethics, the last theory discussed here, contends that ethics are rooted in the virtues of individuals in society. These are captured as moral virtues "virtues of character… are habits or dispositions formed through the repetition of the relevant virtuous actions" (Quinn, pg. 91). If everyone acted ethically and virtuously, the hope of virtue ethics, there would be little need for surveillance systems that were constantly watching. Those who practice and act virtuously. Those who do not are consumed by moral vices, shortcomings that can only be changed through much time and practice.

This does not eliminate the need for privacy within society. Even in a virtuous society, people should be granted the right to live their lives in the way they choose. Constantly watching those in society with the expectation that they will act unethically - moral virtues. Rather, if the expectation of each person is to live and act virtuously, there should be no need for surveillance. With the ethical treatment of virtues and vices, perhaps people will act as they will act regardless of surveillance.

Good people will naturally do virtuous actions. People should strive to be virtuous, which will improve their moral character. Rather than surveillance and tracking of people's faces, we should. Similarly, if the government and employees act with the expectation that most people will not be virtuous by constantly watching everyone, then they are not acting virtuously.

Regarding these points, virtue ethics, a theory that struggles with governmental policy (Quinn, pg. 93), could be argued as being against the need for facial recognition technology on the grounds that it is unnecessary. With or without it, 'good' people will do the right things; 'bad' people will not. Moreover, virtues, such as honesty, would suggest that the state would need full transparency to show that facial recognition systems protected citizens from crime. If the state wished to enact these technologies because they protected the population, they would need to prove in what way they did.

Conclusions About Facial Recognition Technology

Facial recognition has benefits, and is already making its way into the fabric of society, with even greater effect in China. For more free and open societies, our usage and implementation of them will be a challenge to the privacy we feel. Schools and private companies may support the usage of facial recognition technologies in their places of study or work, but they should understand that the full effect of the systems extends to far more than just protecting the students or employees in a building.

There will be a marked effect, upon understanding that they are being surveilled. The systems may come with inherent flaws. Moreover, complex and difficult conversations about taking actions based on the information collected from the systems will be important for future implementations. So long as we consider facial recognition through multiple ethical lenses, we can ensure that further development of facial recognition technology will consider the ethical beliefs of its participants.

Works Cited

Blad, S. D., Evie. (2019, January 25). School shootings in 2019: How many and where - education week. *Education Week*. https://www.edweek.org/ew/section/multimedia/school-shootings-in-2019-how-many-where.html

CNN, E. W. and C. W. (2019). *In 46 weeks this year, there have been 45 school shootings*. CNN. https://www.cnn.com/2019/11/15/us/2019-us-school-shootings-trnd/index.html

Facial recognition software on the rise in U. S. Schools. (n.d.). Retrieved December 5, 2020, from https://www.govtech.com/products/Facial-Recognition-Software-on-the-Rise-in-US-Schools.html

Feldstein, S. (2019). *The global expansion of ai surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

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

Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G. H., Kim, J., Wufuer, M., Jin, X., Kim, S. W., & Choi, T. H. (2019a). A facial recognition mobile app for patient safety and biometric identification: Design, development, and validation.*JMIR MHealth and UHealth*, *7*(4). https://doi.org/10.2196/11472

Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G. H., Kim, J., Wufuer, M., Jin, X., Kim, S. W., & Choi, T. H. (2019b). A facial recognition mobile app for patient safety and biometric identification: Design, development, and validation.*JMIR MHealth and UHealth*, *7*(4). https://doi.org/10.2196/11472

Nguyen, F. Q. (2018). The standard for biometric data protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Quinn, M. J. (2017). *Ethics for the information age* (7th edition). Pearson.

Silva, S., & Kenney, M. (2019). Algorithms, platforms, and ethnic bias. *Communications of the ACM*, *62*(11), 37–39. https://doi.org/10.1145/3318157

Singer, N. (2019, January 25). Amazon is pushing facial technology that a study says could be biased(Published 2019). *The New York Times*. https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

Wright, D. C. (2018). *"Eyes as bright as snow": Facial recognition technology and social control in china*. https://www.deslibris.ca/ID/10097164