Artificial Intelligence Face Recognition Technology and Ethical Gender

Run Wang[1,*]

[1]*University of California, Irvine, Irvine, California, 92697, United States*
[*]*Corresponding author. Email: Wangrunhr@gmail.com*

ABSTRACT
In the development and application of artificial intelligence, many outdated and biased data are wrongly expanded in artificial intelligence systems. Many hidden inequalities and discrimination in human society are challenging the security of society and the privacy of people. As technology continues to improve, AI is being used in a variety of fields, such as image diagnosis, prisoner tracking, cell phone screen opening and employee recruitment. In 2017, a Stanford report showed that facial recognition could become gaydar, which caused some panic at the time. Meanwhile, when face recognition started to challenge gender equity, Amazon was an example. In addition to the biases caused by the data mentioned above, the execution and design logic of AI needs to be further explored. The focus of this paper is on biases and how people can avoid them. In addition, this paper will demonstrate how AI technology and algorithms are used in human daily life, with the goal of informing people about the reasoning behind AI facial recognition.

Keywords: *Facial Recognition, Discrimination, Gaydar, Algorithm*

1. INTRODUCTION

Science and technology always come from human nature, and technical issues cannot but involve value judgment and morality, especially artificial intelligence. In the development and application of AI, many outdated, biased data are wrongly augmented in AI systems [1]. At this moment, many hidden inequalities and discrimination in human society are quietly shaping artificial intelligence. In 2006, machine learning algorithms broke through the bottleneck, allowing artificial intelligence to simulate human judgment in certain situations, such as image diagnosis; provide information interpretation - using algorithms to handle tasks such as sorting, selecting content, filtering information; speeding up operational processes, such as keywords Interpretation, foreign language translation, etc.; participate in people's decision-making and information flow. However, just as code and culture play an “agent” role in how AI understands the world and acts on it, so do the laws that compile them. Amazon's case is the best proof.

In recent years, with the attention of many people of insight, the sensitivity of ethical issues in technical design has gradually increased. In the new 2020 version of the Google Cloud Vision API, Google will de-tag gender in photo recognition to avoid gender bias instilling gender bias in AI. Google's image recognition system is often controversial. As early as 2015, it was pointed out that black people were identified as gorillas, and in 2018, there were still people who found problems. After that, Google formulated the "Artificial Intelligence Principles" to manage the development of artificial intelligence, hoping to effectively avoid the occurrence of bias and other situations [2].

In 2018, Amazon announced that it would stop using AI (artificial intelligence) to screen job resumes. Its AI recruiting engine is sexist and "female-biased" in hiring results. In 2015, a study of online advertising found that Google's artificial intelligence system advertised less high-paying jobs to women than men. The way these systems are built often inadvertently reflects greater societal biases [3]. Going back to the Amazon example, Amazon had to deprecate it due to the difficulty of ensuring gender fairness in the algorithm. In addition to the aforementioned data-induced biases, the execution and design logic of AI also requires further exploration. The main focus of this paper is on biases and how they might be avoided. What’s more, this paper will demonstrate how AI technology is used in human daily life, with the goal of educating people about the rationale behind AI facial recognition.

2. FACE RECOGNITION SYSTEM EXECUTION AND DESIGN LOGIC

Face use is a simple matter of seeing your face on the corner across the street without noticing. Facial recognition cases that have recently come to light have raised eyebrows. According to reports, some brands are using a camera, which has the function of collecting facial information.

2.1. India uses facial recognition to track sexual harassment

The most recent controversial case took place in Lucknow, the capital of the Indian state of Uttar Pradesh [4]. The local government plans to set up surveillance cameras in 200 places where sexual harassment and sexual assault are most likely to occur in 2021, and deploy artificial intelligence face recognition systems for monitoring. Once a woman is assaulted, her facial expression changes and she is sent to the police station. By detecting female facial expressions, police will use facial recognition devices to block inappropriate physical contact in real time. The focus is on ethical privacy disputes and the recognition accuracy of artificial intelligence, including the parties' inability to grasp the flow of data, and how to recognize expressions of discomfort or fear after being sexually harassed. Improper execution and design logic behind AI could lead to greater "surveillance."

India's priority in adopting artificial intelligence in sexual harassment incidents is closely related to the development of its artificial intelligence technology and talents. A successful precedent was the use of facial recognition systems by Indian police in April 2018.

India's use of artificial intelligence technology has grown exponentially over the past two years, with the world's largest system of facial recognition technology on the way. The NGO Internet Freedom Foundation has pointed out that monitoring facial expressions is inappropriate. In addition to the possibility of misjudgment, it is also like monitoring every move of passing women. Currently, a growing problem affecting the data security and privacy of domestic citizens is the unregulated and illegal use of facial recognition technology [1]. However, screening threatened female expressions through official algorithms amounts to recognizing that there are fixed images of victims in such incidents, while ignoring protections for less typical victims.

2.2. Facial recognization on LGBT group

The controversy surrounding human identification has also raised concerns among LGBT people. In the era of artificial intelligence, how to judge the sexual orientation of a stranger? One can only guess. However, AI might be able to tell you the answer just by looking at a photo [5]. Recently, a study from Stanford University has drawn attention. Using deep neural networks, researchers Miachal Kosinski and Yilun Wang used deep neural networks to extract features from more than 35,000 photos posted publicly on American dating sites [6]. Based on big data and visual analysis, their artificial intelligence algorithms can now identify a person's identity based on photos. Through preliminary tests, the algorithm was 81% accurate in judging the sexual orientation of men, while it was lower at 74% for women. However, if you can provide 5 different avatars of a person, the accuracy rate will be greatly improved, and the accuracy rate of judging male and female sexuality will reach 91% and 83%.

According to the different facial features expressed by different gender groups, gay men have softer, more energetic, cleaner facial expressions than heterosexual men, with feminine features, narrower chins, longer noses, and larger foreheads [7]. For gay women, the characteristics are reversed, they tend to be more masculine. However, the research has also raised concerns among LGBT people who fear the technology could be abused by anti-gay activists to invade privacy and combat homosexuality.

In fact, treating the results obtained by such an algorithm as "evidence" can lead to a vicious cycle of implicitly discriminatory views at the beginning and reinforced at the end. The reasons for these biases are related to the sampling bias of the initial data. How to detect the failure of the algorithm before introducing it into the application and avoid possible injustice will be an important topic for the future development of science and technology society. People tend to put too much faith in algorithms because they are mathematical, i.e. accurate. Harmful big data algorithms increasingly control society without legal and ethical scrutiny. Algorithmic auditing is still a very young field, and academic research is exploring various approaches, which may require government regulation of the industry.

3. ETHICS OF DATA: SEPARATION OF ALGORITHMS AND TECHNOLOGY

First, how do we detect and avoid these biased algorithms? Healthy algorithms are based on transparent models, use data directly relevant to the problem, and regularly compare with the real world to learn from mistakes. In contrast, algorithm-based models tend to be opaque "black boxes" and often involve harmful feedback loops. In this way, a crime prediction algorithm does not just model or mathematically represent the real world, it implements its model assumptions in the predictor's behavior. When crime is regulated, they generate more data, and more data means more accurate

predictions, which means more accurate regulation of crime.

From a research ethics standpoint, this feedback loop that transforms algorithms from modeling to instantiation is a key difference between algorithms and more common techniques. There are many separations between existing research ethics norms and regulations and the methods and outcomes behind data analysis.

Research ethics is more than just the ethics of what should be done in scientific research, it is an institutionalized set of norms and practices, involving law, that establish our shared expectations about how science can or should be managed. Most of the activities we call data science fall outside these regulations, and data science is hardly affected by previous ethics reviews. This poses a challenging problem for data engineers, ethicists, and developers: not only is most data science disconnected from the foundations of research ethics, but we also lack norms and habits of mind for how to review these techniques and expectations in order to Rules to mitigate its harm. Besides, once the loop is identified, what happens when it closes? For example, if some companies use this technology to hire people, what would the result be like? If no limitations are established on commercial companies, they will be able to gather vast amounts of face data for commercial purposes and sell and misuse that data without the consent of the consumers. Many individuals feel that among personal information, face data is the most sensitive biometric data, with the most catastrophic repercussions if misused, and that it should be secured to the greatest extent possible. Such a finding is not surprising. Researchers utilized mostly white male photographs to train the robots when creating facial recognition technology, therefore the machines were better at recognizing white males.

3.1. Facial recognization has racism

Due to a lack of experience identifying blacks and females, the machines were also more likely to make mistakes when identifying minorities and females. This prejudice develops as a result of pre-existing inequities in society, and it exacerbates those inequalities by increasing the likelihood of false convictions for disadvantaged people if police deploy this technology on a big scale. Technology is created by people who live in specific social environments, and technology can be severely biased. If we put everything in the hands of ostensibly unbiased computers and assume that everything will work out, people may see an increase in social inequality and a loss of justice. Face recognition technology may well hit a sensitive point in American culture, which is the value of individual liberty versus the fear of government abuse. The United States is slow to legislate digital privacy, and some Americans appear willing to sacrifice privacy for convenience (and essentially provide personal data to corporations, not the government); however, facial recognition technology may well hit a sensitive point in American culture, which is the value of individual liberty versus the fear of government abuse. As a result, the United States is much quicker to pass the legislation prohibiting facial recognition compared with other western countries. Next, we will address the particular ethical challenges these data analytics face.

3.2. Facial recognization as a gardar

Another example would be in that Stanford study, face recognition can tell a person's sexual orientation and that gay people have higher face values on average than people of normal sexual orientation. The authors underline that their goal was not to create a tool that invades people's privacy, but to see if current technology employed on a broad scale by governments and companies constitutes a threat to the privacy of specific groups of people. Regrettably, they discovered that it does. Even those who are opposed to the study should not dismiss the existence of such a threat because they disagree with the study's findings. The authors themselves were concerned about the attention this study would attract before publishing the paper, and spent a lot of time considering whether such a study would bring potential threats to the surface, but they ultimately decided that having a clear understanding of such threats would alert the LGTBQ community to them, alert the general public to them, alert digital service providers to better protect people's privacy, and alert policy policy makers to respond [6]. The authors also remind readers of the significance of the data in the paper, as the AUC does not equal with the correct rate of system identification. Therefore, readers should not be overly concerned about the direct impact of these results.

People want to use and improve these systems, but it is hard to find a way forward. Algorithmic capabilities, is private data viewed, recorded and analyzed adequately protected? Our every move is lured by invisible bait, because we are interested in A, and then algorithmically recommend BCD we might like. Sometimes the author finds that Big Data understands my needs and preferences better than me and my relatives. From search engines to social media, algorithms sift through thousands of pieces of information, creating bias but also creating a stratosphere [8]. For designers and users, any future technological solutions involving a wide range of technologies are issues that require careful consideration. In their book Data Feminism, Catherine D'Ignazio and Lauren Klein argue that today's data science has become a force. On one hand, it has benefits to expose injustice and improve health; on the other hand, there is a danger of harm, and it is also used for discrimination and surveillance. It is therefore necessary to ask the following questions: Who does data science? Who does data science serve? Whose interests are data science relevant

to? For example, the Sex Robots controversy clearly reflects a preference for male-centric product design. Some researchers have pointed out that the prevalence of the AI sex robots poses a growing psychological and moral threat to individuals and society [9].

4. CONCLUSION

Legislation in democracies can assist in shifting the balance of good and bad results. European regulators have included a set of principles in impending data protection legislation that states that biometric data, such as "faceprints," which belongs to the person who owns it and that its use requires agreement. Employers who screen images of job candidates may be subject to anti-discrimination legislation. Commercial facial recognition system vendors may be subjected to audits to demonstrate that their technologies are not unwittingly propagating bias. Companies who utilize this technology should face consequences. These regulations, however, cannot alter the course of events. As wearable devices become more popular, cameras will become more common. For fear of exploitation by autocratic regimes, Google has specifically declined to link faces to identities. However, there are still many companies using. Face recognition is provided by Amazon and Apple utilizing their own cloud services. Although the government will not willingly give up its interests, people's privacy must be better protected.

There are only 1 and 0 in AI's world, however, this judgment might cause discrimination in real world. In the process of technical design and application, many power relations and value judgments are implied, which are not universally applicable. So, what kind of information will be investigated statistically and what information will be collected and incorporated into the algorithm. These are important questions that we need to consider and study. The example of the robot Actroid and the genderless voice assistant Q, designed with a sample of typical Japanese women, reminds us, is data a mirror or a filter of society? The development of technology should introduce more elements of critical thinking so that AI can no longer reproduce the old prejudices and inequalities of society.

Therefore, it is particularly important to pay attention to the fairness of the data and to identify systematic biases. For data, in addition to the quantity of data, more attention should be paid to the quality, especially to check whether there are specific "data flaws" which is refer to"black box" in the sample, which make it impossible for artificial intelligence to interpret specific groups of people due to lack of data. Not only average the amount of gender data, but also data on marginalized and minority groups, use open data and logic to correct systemic biases, expand information transparency, develop relevant codes, and open up communication and monitoring for other groups. "A public right to privacy has never been legally recognized by the Supreme Court" [10]. Most police departments have not taken appropriate precautions to govern this monitoring equipment due to a lack of guidance. Technology often outpaces privacy laws in today's fast-paced society. Special attention should be paid to privacy laws. To achieve this purpose, privacy safeguards must be implemented with the collaboration of all law enforcement, facial recognition professionals, and community leaders; otherwise, privacy protections will fail. The prejudice that technology needs to overcome goes far beyond gender. Exploring how technology is affected by human strength and values is arguably the best touchstone, allowing us to glimpse the interaction of human nature, context, and technology in various decision-making.

AUTHORS' CONTRIBUTIONS

This paper is independently completed by Run Wang.

ACKNOLEDGMENTS

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Soina Katyal. From my first exposure to the work underlying artificial intelligence and the problems that drove me to think about it, her excitement, knowledge, and meticulous attention to detail inspired me and greatly aided my work. I'm also grateful for Ulric Dai, my assistant professor, for his informative comments.

REFERENCES

[1] Daugherty, R. Paul, H. James Wilson, and Rumman Chowdhury. Using artificial intelligence to promote diversity. MIT Sloan Management Review 60.2, 2019.

[2] Zou, James, and Londa Schiebinger. AI can be sexist and racist—it's time to make it fair, 2018, pp.324-326.

[3] Cirillo, Davide, et al. Sex and gender differences and biases in artificial intelligence for biomedicine and healthcare. NPJ digital medicine 3.1, 2020, pp.1-11.

[4] Parsheera, Smriti. Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not? 2019.

[5] Leuner, John. A replication study: Machine learning models are capable of predicting sexual orientation from facial images. arXiv preprint arXiv:1902.10739, 2019.

[6] Wang, Yilun, Michal Kosinski. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of

personality and social psychology, 114.2, 2018, pp. 246.

[7] Miller, Arianne E. Searching for gaydar: Blind spots in the study of sexual orientation perception. Psychology & Sexuality 9.3, 2018, pp.188-203.

[8] Kovacova, Maria, et al. Automating gender roles at work: How digital disruption and artificial intelligence alter industry structures and sex-based divisions of labor. Journal of Research in Gender Studies 9.1, 2019, pp.153-159.

[9] J. Z. Ma, Dewi Tojib, and Yelena Tsarenko. Sex Robots: Are We Ready for Them? An Exploration of the Psychological Mechanisms Underlying People's Receptiveness of Sex Robots. Journal of Business Ethics, 2022, pp.1-17.

[10] Clare Garvie. The perpetual line-up: Unregulated police face recognition in america. Georgetown Law, Center on Privacy & Technology, 2016.