VICTORIA UNIVERSITY OF WELLINGTON TE HERENGA WAKA | Wellington Faculty of Engineering Te Wāhanga Ahunui Pūkaha | Ethics and Sustainability Symposium

Code of Ethics for Facial Recognition

Caitlin Fisher

Abstract
Facial Recognition is a big part of surveillance and security in recent years. Along with any technology there are ethical issues that need to be considered when designing, creating, and using the system. This paper reviews the literature and their codes of ethics and ethical issues surrounding facial recognition to draw conclusions about the most important principles. Issues discussed include bias, collection of data, transparency, vulnerable population, security, and accountability. With these conclusions a code of ethics is introduced to improve or justify the current literature. Elaborations are made on each principle to justify the issue and inform specific ways to make the system ethical. This new code of ethics is then used to analyse the ethics around facial recognition in schools.

Keywords: Ethics; Facial recognition; Principle; system; Schools.

1. Introduction
Ethics is an important aspect to consider when creating a system, as it allows organisations to be concerned about the moral principles and applications of the system. Systems should always make sure that they are morally good and right for society and/or public use. Codes of ethics can help guide organisations to ensure their systems follow moral principles.

Due to facial recognition seeing wider use in recent years, many organisations and entities created codes of ethics to provide principles to ensure facial recognition systems are morally good and right. These principles include, security, accountability, the collection of data, transparency of the use and purpose and ensuring that the bias is kept to a minimum within the system, as these principles ensure the best outcome for the public.

1.1. Background
The protection of data is the one of the main aims for security systems, there are many different forms of security system one being Facial recognition [1]. Facial recognition is a form of security technology developed using biometric applications. These biometric features allow systems to identify people based upon an individual's physical characteristics, such as fingerprints and irises. Facial recognition uses the face as it contains "different structures and characteristics" that could identify an individual [1]. This could be applied to images, videos, and real-time clips.

The advantage of facial recognition is that there is no need to remember specific information, such as passwords, to access information. Individuals use their face to easily access this instead. However, the disadvantages are the "robustness, accuracy, complexity, and discrimination" [1].

Due to facial recognition providing an efficient form of security and surveillance, organisations recently started to use the systems for many different applications, within multiple fields. This includes border control, phone access and surveillance of public areas.

1.2. Objective

The objective of this paper is to gather important ethical principles and current issues within facial recognition technology, to help construct a new code of ethics for facial recognition. The aim of the new code of ethics is to highlight the most important ethical principles and provide informative information about each principle, to ensure organisations/entities are building an ethical facial recognition system. Finally, the new code of ethics is tested through a case study on facial recognition technology within schools. The case study covers Chinese schools that have implement these systems. It will show any unethical properties of using facial recognition in schools, and how we may make it more ethical using the code of ethics created in the report.

2. Literature review

There are many facial recognition codes of ethics that organisations follow to help them produce ethical systems. In this literature review four codes of ethics will be analysed to find common and related ethical issues within facial recognition systems. Common issues will be found by reviewing the principles in the literature and finding similar issues within them. Whereas related issues may not be found in all the literature, but they present a strong case for the ethical issue. These issues will be used to construct a new facial recognition code of ethics.

The literature used in the review are codes of ethics or papers discussing ethical issues surrounding facial recognition. The codes of ethics were found through organisations that commonly use facial recognition or provide a code for other entities to follow such as the American Civil Liberties Union (ACLU) [2].

2.1. Ethics/Sustainability issues

Bias is a key concern within facial recognition systems and should be developed and tested in a way that "prevents, or at least minimises, bias against any person or group" [3]. The types of bias that affects facial recognition are visual biases that include racial, gender, ethnicity and age bias which occurs when a system has a preference towards a race, gender, ethnicity, or age over others. Clothing bias is when a system is influenced by an individual's appearance. Religious bias can be seen in this clothing bias as some groups express their religion through specific clothing. Lastly, disability or appearance bias is where a system may present a negative bias towards individuals with facial disability or facial markings. A facial recognition system that contains these biases is error-prone and can lead to penalties to people and groups found in these biases and unfair opportunities for those not affected by bias [4].

Many facial recognition codes of ethics bring up the principle of the collection of data [2, 5, 6]. The collection of data is extremely important as the facial recognition algorithm must be trained and tested on large amounts of data to work effectively. It is easy to find faces for the dataset through webcam live-streams, footage of crowded places and public websites [6]. However, this can be highly unethical if there was a lack of consent and transparency. An organisation/entity should always receive an informed consent from an individual before adding one's face into a facial recognition database and be transparent about the purpose of this consent and use of the data [5].

Consent amongst the vulnerable is another ethical concern seen in a code of ethics [5]. A different form of consent should be considered for individuals such as, teenagers, children and the mentally disabled. This is because they may not understand the full purpose of the system and the consequences of providing certain information. Therefore, if an organisation/entity is receiving information from the vulnerable population they should

provide a form that contains the same level of understanding and take into consideration the individual's age or vulnerability or receive parental/guardian permission.

The security and privacy of the data stored in the facial recognition systems is a principle seen in many codes of ethics [5, 4]. This principle is important as the data stored in the system holds individuals' private information and can be used for criminal acts such as facial identity theft [3]. Consequently, facial recognition systems should use "encryption and other cybersecurity and privacy best practices" [4] to ensure the security and privacy of the systems data.

Accountability is an important principle for all facial recognition systems to ensure that organisations are always following ethical principles [2, 5]. Without accountability organisation/entity cannot be held responsible for any unethical activities and may start using facial recognition poorly.

3. Code of ethics/sustainability

- **Bias:** A facial recognition system should not show any bias towards an individual's race, ethnicity, sex, disability, religion, or age.
- **Collections:** An organisation/entity must receive informed, written consent from an individual before adding their face into a facial recognition database.
- **Vulnerability Population:** An organisation/entity must take extra provisions when using facial recognition from the vulnerable population. They should consider age and vulnerabilities of any individual when asking for consent. When asking for consent the organisation/entity must consider the level of understanding and age/vulnerability of the individual.
- **Transparency:** An organisation/entity must inform individuals of all ethical concerns and purposes of the collection of their information and what it will be used for before they ask for the individuals consent.
- **Security:** An organisation/entity should protect all personal data collected.
- **Accountability:** An organisation/entity must maintain an audit trail of the collection, use and other information.

3.1. Principle Bias

To ensure the bias principle is being considered within your facial recognition system, an organisation/entity should spend time testing and eliminating as much bias as possible [3]. It should be acknowledged that a facial recognition system will never be 100% bias free [7]. However, what needs to be considered is what is the acceptable level of bias and which biases should be prioritised for elimination.

The main source of bias is found in the dataset used in the training of a facial recognition system [8]. Therefore, a simple way to start solving this ethical issue would be to use datasets that contain a variety of known biases, datasets like these can be found online. There are also specific algorithms to measure the amount of bias within a system [8]. Tests can be completed before the release of a facial recognition system to find the amount of bias within it. This provides accountability to all organisations/entity.

3.2. Principle Collections

During the process of collecting images of individual faces, it is vital for a form of consent to be received for a facial recognition system to be ethical. Before consent is given, an individual must be informed of the purposes and consequences of giving their personal information [9]. Even after an individual gives their consent, they may withdraw it at any point and ask for their information to be deleted from the system. If an organisation/entity were to use the system for a secondary purpose not yet covered by consent, they must request further consent for that purpose.

There are multiple forms of consent that are both oral and written, that can be used to gather data [10]. The most ethical and lawful forms include informed consent which is the process of discussing and informing an individual to receive an individual's permission. Another is explicit consent which clearly presents individuals with the decision to agree or disagree with the "collection, use, and/or disclosure of their personal information" [10].

3.3. Principle Vulnerability Populations

Ethical consent is showing that the individual was informed on the purpose of the situation. If an individual does not contain the knowledge or capability to be fully informed on the subject, informed consent cannot be received from that individual. When an entity/organisation uses facial recognition within a vulnerable population, extra precautions should be made to ensure an ethical system. The vulnerable population may include an individual's age and/or mental disability.

These groups of people should be provided with extra precautions as they may not have the same knowledge and understanding on the purpose and consequences on giving consent. Therefore, these precautions are in place to ensure that no matter the age or level of knowledge of an individual, they can understand the purpose and consequences before giving consent. Children under the age of 16 should receive parental/guardian consent before child's data is used.

Precautions may include, writing consent at a more appropriate level for a certain age to understand, provide a space for discussion on any parts individuals may not understand or ask for parental/guardian consent.

3.4. Principle Transparency

Transparency is about the entities facial recognition system promoting ethical integrity of the system. Transparency should be shown throughout the process of the system such as collection of the data, use and security practices.

Firstly, by providing information on the purpose of collecting data, how the data will be used and the consequences of providing data before asking for an individual's consent. This makes the collection process more ethical as it ensures the individual fully understands what and why they are providing this specific information. Also being clear on the duration of time you will keep the data and being transparent on how their personal information will be stored and managed. This will ensure that the entity/organisation are putting their efforts into ensuring that security around the public's information is safe and will help individual's feel more secure.

3.5. Principle Security

Security is a big issue within many different technologies and can be overlooked as unnecessary. However, having weak security can be extremely unethical as individuals are trusting organisations/entities to protect their private information. Without these security measures, you are at risk of leaking information.

Consequently, facial recognition systems should use "encryption and other cybersecurity and privacy best practices" [4] to ensure the security and privacy of the system's data. If an organisation does not have any specialties in security, they should obtain this security service outside of their organisation.

3.6. Principle Accountability

Accountability ensures that all organisations/entities are maintaining an audit trail of the collection of data, use of the system and any other details, such as sharing information. This trail should include all information to help identify what the information is and who may be accessing the data. Some of these include time, date, location, and name of user.

This principle also covers how the facial recognition system makes its decisions. This helps identify if the system is producing ethical outcomes. A way of achieving this is to allow an assessment of the algorithms accuracy and decision making.

4. Case Study

This case study discusses the use and implementation of facial recognition in schools. Many schools in China are implementing systems in classrooms, social areas, and entrances for surveillance of students. While this sounds like an effective use of these systems, using this technology in school can lead to ethical issues that need to be considered.

These Chinese schools will be used in this case study [11], as well as a study done by researcher that gathered his data from 18–22-year-olds at a Chinese university [6, 12]. These Chinese schools show how facial recognition may be used in other schools across the world.

4.1. Principle Bias

This principle was not covered by my case study. However, within schools there can be a lot of diversity amongst the students. This makes bias a big ethical concern when facial recognition is used in schools. A study done within schools in 2021 [13], shows facial recognition systems are inaccurate with age, race, and ethnicity biases. Systems also show more errors amongst children compared to adults, as they go through puberty and facial changes throughout their schooling experience.

For this issue to be solved the system needs to prioritise eliminating the main bias affected in schools which are gender, age, ethnicity, and race. While also training and testing the system on diverse datasets. To help mitigate children's facial changes, schools can update the dataset with new images of students every year.

4.2. Principle Collection and Vulnerability Population

For facial recognition systems to be correctly used in schools, data will need to be collected from the students. It is vital that the students give informed consent. A study conducted in 2019, gathered pictures from 18–22-year-olds from a university in China [6, 12]. Even though they did receive consent from everyone, the "researchers' assertions don't assuage ethical concerns" [6]. This means that they did not simplify the ethical concerns and purpose into a form that individuals would understand. Therefore, it was unlikely that the student gave informed consent. They ended up retracting the work because of this issue.

Schools can gather informed consent by having discussions and assemblies with students to inform them at a proper level of understanding. Also, through a form that parents/guardians sign for informed consent.

4.3. Principle Transparency

Transparency is a big issue within schools as it should be a place for learning and freedom for children. However, a researcher discussed that the extra surveillance in these Chinese classrooms may make it harder for children to focus and may create a "school-to-prison" environment [11]. These issues can be fixed with Transparency. However, this can be an easy principle to overlook, as children often experience a power imbalance over adults, where they receive "less power and control over their lives" as adults may make decisions for them without children having any knowledge of this [11]. This lack of transparency can be seen in this study that was discussed above, where it was considered unlikely that the 18–22-year-old students were given enough information to make informed consent.

This is highly unethical, and schools should always be transparent with the student about the use of the system by making sure the children know what the systems are being used for and when and where they are being used.

4.4. Principle Security

Security is an important ethical principle for all facial recognition systems, which all schools should consider when using facial recognition. However, schools in China were called into question about "the school's ability to keep the students' facial data secure and isolate from possible abuse" [11]. This identifies an issue around whether schools have the proper capabilities to keep the student's data safe and secure.

If schools do struggle with these security aspects, they could outsource their security to an organisation that specialises in this field. However, this can be expensive, and some schools are not provided the budget for this expense. Therefore, if schools do not have the budget for these security measures it is unethical to gather and store this information and it should not be done.

4.5. Principle Accountability

Schools in China, such as Hangzhou high school, were criticised for how they used their system on the students. While it was stated that they installed the systems for surveillance and easy sign-in. They were found using the system to analyse if students were "dozing off in class" [14]. Due to the criticism that is seen in this report, it is likely they were using facial recognition for a purpose not covered by the consent. However, this school was not found accountable for this ethical system. While the researcher in the study above, who gathered images from 18–22-year-olds, was held accountable for his unethical processes. These schools should create an audit trial of information to ensure situations like these do not repeat themself. Schools should be held accountable for all unethical decisions made, as they oversee the next generation.

5. Conclusion and recommendations

Conclusions drawn from the case study show that facial recognition used in schools currently is not ethical. However, this can easily be improved upon by following a code of ethics. A code will help schools make ethical decisions so that systems can be used to make a positive impact within schools.

Engineers that plan to build and/or use facial recognition should always refer to a code of ethics to help identify ethical issues they may not considered. This ensures facial recognition systems will be producing effective and safe outcomes.

It is important to note that ethics can change over time, as new information is discovered, and new technology is created. Therefore, codes of ethics should be reviewed constantly to ensure that it still fits within our society.

References

[1] Y. Korti, M. Jridi, A.A. Falou and M. Atri. "Face Recognition System: A Survey". PubMed Central. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7013584/ (accessed Mar. 23, 2022).
[2] K.R. Gangarapu. "Ethics of Facial Recognition: Key Issues and Solutions." Learn.g2.com 2022 https://learn.g2.com/ethics-of-facial-recognition (accessed Mar. 10, 2022).
[3] N. Joshi. "Ethics and Errors of Facial Recognition Technology." Allerin.comhttps://www.allerin.com/blog/ethics-and-errors-of-facial-recognition-technology (accessed Mar. 22, 2022).

[4] SIA, Security Industry Association. “SIA Principles for the Responsible and Effective Use of Facial Recognition Technology.” Securityindustry.org. https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/#core (accessed Mar. 22, 2022).
[5] ACLU, American Civil Liberties Union. “An Ethical Framework for Facial Recognition.” Ntia.gov. https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf (accessed Mar. 10, 2022).
[6] R.V. Noorden. “The ethical questions that haunt facial-recognition research.” Nature.com. https://www.nature.com/articles/d41586-020-03187-3 (accessed Mar. 10, 2022).
[7] The Conversation. “Why facial recognition algorithms can’t be perfectly fair.” Theconversation.com. https://theconversation.com/why-facial-recognition-algorithms-cant-be-perfectly-fair-142608 (accessed Mar. 15, 2022).
[8] S. Glge, M. Amirian, D. Flumini and T. Stadelmann. “How (Not) to Measure Bias in Face Recognition Networks” in *Artificial Neural Networks in Pattern Recognition.* Springer, 2020, pp. 125-137. https://link.springer.com/chapter/10.1007/978-3-030-58309-5_10 (accessed Mar. 17, 2022).
[9] Privacy Commissioner, pricay.org.nz. “Click to consent? Not good enough anymore” https://www.privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/#:~:text=Unlike%20other%20parts%20of%20the,the%20holder%20of%20the%20information (accessed Mar. 12, 2022).
[10] Privacy Research Team, securiti. “What are the Different Types of Consent?” security.ai. https://securiti.ai/blog/types-of-consent/#informed-consent (accessed Mar. 12, 2022).
[11] J. Michelle. “The Danger of Facial Recognition in Our Children’s Classroom”. Heinonline.org, 2020, pp. 249-267. https://heinonline.org/HOL/PrintRequest?collection=journals&handle=hein.journals/dltr18&id=1&print=section&div=2&ext=.pdf&format=PDFsearchable&submit=Print%2FDownload (accessed Mar. 18, 2022).
[12] C. Wang, G. Zhang, W. Liu, Y. Liu and L. Miao. “Expression of Concern: Facial feature discovery for ethnicity recognition.” https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1278 (accessed Mar. 10, 2022).
[13] J.S. Cusick and C. Okoh. “Why schools need to abandon facial recognition, not double down on it”. Fastcompany.com. https://www.fastcompany.com/90657769/schools-facial-recognition (accessed May 2, 2022).
[14] X. Shen. “China is putting surveillance cameras in plenty of schools”. Techasia.com. https://www.techinasia.com/china-putting-surveillance-cameras-plenty-schools (accessed May 2, 2022).