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 Systems: A Case Study

Jaya Narayan

Abstract
The integration of Facial Recognition Systems (FRS) in society is increasing. A key factor in adequate performance for FRS is the reliance on user data. Hence it is important not only to understand the ethical issues surrounding FRS but also to ensure that a proper code of ethics is established. This paper analyses and discusses the ethical issues with existing FRS as well as ethical conducts that are already put in place. Additionally, a new code of ethics will be created for FRS. Furthermore, a case study of a specific project involving FRS is conducted. Each principle listed in the newly created code of ethics is applied to the selected project.

Keywords: Ethics; Facial Recognition Systems; Case Study.

1. Introduction
The use of Facial Recognition Systems (FRS) has been increasing. The estimated market value of FRS is "USD 3.86 billion dollars in 2020" [1] and "an expected growth rate of 15.4% from 2021 to 2028" [1]. However, with the exponential growth of FRS comes the danger and risk of flaws as well as gaps in a system going unnoticed.

FRS are a "quick, simple, easy and for the most part, is accurate" [2], it provides a faster and quicker method of identification and authentication [2]. Hence the popularity of FRS has been increasing. Many companies such as Samsung, Apple, Amazon, Microsoft, and Google have developed and implemented FRS into their products [3]. A recent survey found that 109 countries (nearly 80% of the countries in the world) have been given approval by the government approval to use FRS for surveillance [4].

1.1. Background
Facial Recognition (FR) is a Biometric and one of the many ways individuals can provide authentication to identify themselves [2]. Due to its speed and convenience, FR is becoming more popular compared to other biometrics such as identification by fingerprint, iris, and speech [5]. However, it is the reliability and high levels of security [6] that FRS provides which is gaining the attention of many corporate and government organisations [6]. There are three stages involved for FR [2,5]. The first stage is the detection stage, here an image is captured then the face in the image is located [2,5]. The second stage is extraction this is where particular features of the selected face are identified [2,5]. The next step is comparison, here extracted features of the identified face are compared against a database of preselected templates of facial features [2,5]. A successful comparison indicates a match.

For FRS there are three steps involved which are capturing/detection, extraction, and comparisons. The most crucial step to successful FR is the process of comparisons. For FRS to conduct comparisons a large data set of human faces is required [2]. These databases require images of human faces from multiple angles as well as lighting but also factors such as age, gender and race must be considered [5,7]. A lack of variety in data sets has become a concern for companies using FRS. The reason is that a study identified that individuals with fairer and lighter skin "had a 99% success rate" [7]. However,

"individuals with darker skin tones observed a 35% increase in errors arising" [7]. Another study further pointed out the increase in inaccuracy due to the rapid rise of surgical variations of the face for beauty [5]. This highlights the ethical issues encountered with FRS.

1.2. Objective

The objective of this paper is to examine ethical issues that are currently surrounding FRS and the current code of ethics that exists. This helps create an FRS Code of Ethics which is used against the case study of Clearview.

2. Literature review

The literature review is based broadly on FRS. The literature review has a deeper investigation into the frameworks that are used to deal with the ethical issues that are surrounding facial recognition systems.

2.1. Engineering NZ Code of Ethical Conduct

The Engineering NZ Code of Ethics is essentially a list of standards [8]. These standards are rules that are put in place and should be put into practice and followed by the engineers of New Zealand [8]. The profession of Engineering is broad as career paths for industry professionals in the engineering field vary from hardware engineers to software engineering. Thus, as the engineering profession is very vast it has meant that the Engineering NZ Code of Ethical Conduct is broad in terms of ethical principles. This ensures that all areas of the engineering profession are covered. The Engineering NZ Code of Ethics has 8 principles and whilst all principles are important there are a few that are of particular interest, especially for the felid of FRS. For example, the fifth principle "Behave appropriately" [8] might relate to the data collection process involved with many programs that require a database. This principle could mean that appropriate steps must be taken when collecting data. For example, entities collecting data for their systems must be given consent by the individual whose data is being obtained before proceeding. Preventing entities from violating the rights and freedom of individuals. The seventh principle "Maintaining confidentiality" [8] could relate to the accessibility of stored data a system has in its database. For example, entities selling or sharing individuals' data without consent is a loss of confidentiality. This principle would prevent loss of confidentiality because data would be consented to before being shared or sold.

2.2. IT Professions Code of Ethics

The Information Technology (IT) Professionals Code of Ethics is the code of ethics for IT Professionals in New Zealand [9]. Similar to the Engineering NZ Code of Ethics the IT Professionals Code of Ethics has eight principles that act as a guide on how industry professionals in the IT field should act and behave [9]. There are several principles in the IT Professions Code of Conduct that mirror principles found in the Engineering Code of Ethics where industry professionals should work in a manner that looks out for the well-being of others. As the IT field deals with information such as data of clients, they are likely to face more ethical issues. Thus, the code of conduct covers more areas that surround the handling of data and how interactions with clients should be conducted. There is a principle that is "good faith" [9]. It states that "*…treat people without discrimination…and have consideration for values and cultural sensitives of all groups in the community*" [9]. Hence when IT Professionals work with clients they should treat clients equally regardless of their cultural beliefs and values. Another principle is "Continuous Development" [9], which states Professionals "*develop their knowledge, skills, and expertise through their career*" [9]. Therefore, IT professionals can provide high-quality service to clients as they are up to date with the knowledge required for the field.

2.3. New Zealand Office of the Privacy Commissioner

"The Office of the Privacy Commissioner seeks to develop and promote a culture in which personal information is protected and respected in New Zealand" [10]. The main roles of the Privacy Commissioner are to examine breaches of privacy and to monitor the impact of technology on privacy [10].

2.3.1. Privacy Commissioner's regulation of biometrics

The integration of biometrics in technologies is increasing at a rapid rate hence why the privacy commission has set out regulations [11]. The privacy commission deems that "*biometric information is in fact personal information and thus is regulated by the Privacy Act 2020*" [11]. This means that entities must oblige to the 13 information privacy principles (IPP) that the Privacy Act is based upon [11]. For example, IPP2 states that "*Agencies must collect biometric information directly from the individual concern*" [11]. Having IPP2 in place ensures that an individual has knowledge of the information that is collected by agencies and how that information will be used.

As biometrics is information regarding an individual's behaviours it means that data must be collected to obtain this information however this leads to concern about Te Ao Māori perspectives [11]. The reason is that as part of the Crown there are obligations under the Te Tiriti o Waitangi to "partner with Māori and take Māori perspectives into consideration" [11]. Thus, the Privacy Commission states that the Treaty of Waitangi is a key factor when handling biometrics.

2.3.2. Privacy Commissioner Principles for safe and effective use of data and analytics

The Privacy Commissioner has an outlined list of principles "for safe and effective use of data and analytics" [12]. In this list, 6 principles are put in place for entities that wish to conduct "data analytics activities including algorithmic decision making" [12]. These principles ensure that entities that use algorithmic systems that collect and use data such as FRS, act in a manner that respects the privacy of individuals whose data is collected [12]. Firstly, there is the principle of "Deliver clear public benefit" [12]. This means that the data must be used in a way that is beneficial for New Zealanders and it prevents entities from misusing the data for purposes that are damaging and degrading. The principle of "Maintaining Transparency" [12] is key when the data of citizens has been used in systems. This principle prevents entities from not taking accountability as being transparent means admitting and taking responsibility when a breach or error/mistake occurs [12]. Having transparency put in place makes sure that individuals whose data is collected have full knowledge of where their data is, who is using it, what is it being used for, what data about themselves is being stored, how is it being used, and if is it kept safe and secure [12]. To make sure that entities collect data in a manner that is ethical these are just a few of the principles that the Privacy Commissioner has put in place.

3. Code of ethics

Essentially ethics are a set of practical rules that are imposed to identify whether actions conducted are deemed as right or wrong [13,14]. Thus, a code is ethics is a set of principles that are used to help guide industry professionals to act in a manner that is professional and is beneficial to all stakeholders of a system [13]. The code of ethics ensures that industry professionals carry out work with integrity and honesty [13]. Having all relevant and important information as principles in a code of ethics makes sure that industry professionals understand the standards that are put in place [14]. After extensive research was gathered a Facial Recognition Code of Ethics has been designed and created. For this code of ethics, the purpose is to make sure that the correct actions are maintained to ensure that professionalism with FRS is sustained.

Below is the Code of Ethics containing eight Principles:

1. Maintain transparency
2. The purpose of surveillance should be lawful
3. Take full accountability
4. Data collection consent
5. Respect Privacy
6. Avoid Biases
7. Have regard for children and teenagers
8. Report breaches of code

3.1. Principle One: Maintain Transparency

The principle of maintaining transparency ensures that companies dealing with FRS are open and honest with the limitations, gaps, and capabilities of the system. Entities involved in FRS must be transparent about how data is used and collected. It is an indication that a company is willing to share information and admit to errors occurring. Transparency ensures an individual has a clear understanding of how the system operates and is kept up to date should an unfortunate event occur.

3.2. Principle Two: The purpose of surveillance should be lawful

The principle of lawful surveillance means that unless authorised by the government FRS should only be used for lawful purposes such as being used to solve crimes. This principle also means that other than for security and safety purposes FRS should not be used to track the private details of individuals without their consent as this is a violation of their human rights and freedom.

3.3. Principle Three: Take full accountability

The principle of taking accountability means that if a breach were to occur the companies/entities involved should take full responsibility, ownership, and accountability. Thus, entities should be aware of the impact actions cause. The weight of having to take full accountability enforces the entities involved to have security as their top priority.

3.4. Principle Four: Data collection consent

The principle of data collection dictates that all entities of FRS must receive consent from an individual before proceeding to store the individual's face in a database. Furthermore, individuals consenting to data collection for FRS must be given the choice to opt-out if they wish to do so. In the case that an individual has opted out then all data of the said individual must be promptly deleted.

3.5. Principle Five: Respect Privacy

The principle of respecting privacy means that should the FRS store user data it should not contain identifiers. Data of individuals stored in the FRS database must not be sold or shared with individuals who do not have authorisation without the consent of the individual whose information is being sold or shared.

3.6. Principle Six: Avoid Biases

The principle of avoiding biases means that for FRS biases should be taken into consideration when the outcome is designed. Datasets should avoid presenting bias by ensuring to use a large database that contains data from a broad range. This means that data from different ages, races, and genders should be collected and stored.

3.7. Principle Seven: Have regard for children and teenagers

The principle of having regard for children and teenagers means that entities dealing with FRS must take extra precautions when dealing with children and teenagers. This means

due to their age entities must consider the age but also the level of competency when asking for their consent to proceed with data collection. For children under the age of 13, it is vital for entities using FRS that parental consent is taken before data is collected. In the case that parental consent is not given or received access to children's data under the age of 13 must be restricted if not prohibited.

3.8. Principle Eight: Report breaches of code

The principle of reporting breaches of code means if a breach of the Facial Recognition Code of Ethics occurs it must be immediately reported. The reporting of breaches is of utmost importance as it helps contain the damage of the breach. Additionally, it prevents further sharing, loss, or exposure of confidential personal information.

4. Case study

The case study of this paper is based on the use of FRS for policing. The case study evaluates and analyses each principle stated in the Facial Recognition Code of Ethics against the FRS that is used for policing. Biometrics such as FRS are becoming increasingly popular amongst government departments including the New Zealand Police [15]. The reason is that FRS provides increased reliability and high levels of security [6]. FRS helps police departments to conduct investigations faster by identifying suspects quicker and thus resolving crimes at an increased speed [15]. A popular FR tool that is targeted toward agencies such as the police department is Clearview [16]. The FR tool Clearview allows an "end-user to upload an image of an individual" [16] which will then enable to "end-user to see if there are any images of the selected individual that are publicly available" [16]. It allows the end-user to "identify any links as to where certain images may have appeared" [16]. The use of Clearview by the police comes with ethical issues which will be discussed here.

4.1. Principle One: Maintain Transparency

Principle one states that transparency must be maintained, which was not met. Clearview conducts automatic image scraping on platforms such as YouTube, Facebook, Instagram, and LinkedIn for public images [16,17]. Although these images are public, individuals whose images have been collected for Clearview's database do not have any knowledge of this. These individuals do not have any idea as to how their data is used, limiting their understanding of how the system is functioning. As transparency is not maintained Principle 3 of the Privacy Act 2020 is violated as individuals are not aware of why their images are being collected and who has received them. The New Zealand Police also failed to maintain transparency as they did not seek permission or approval from the Privacy Commission before conducting a trial of Clearview [16], thus they also violated principle 3.

4.2. Principle Two: The purpose of surveillance should be lawful

This principle has not been violated as the New Zealand Police stated that their intentions for Clearview were to directly relate to their line of work which is to search for persons of interest [15]. Furthermore, Clearview states its purpose is to help support law enforcement in the work they do. However, there is a serious concern that if not regulated adequately Clearview might sell its database to entities and individuals who could use the data for unlawful surveillance i.e., to blackmail or stalk individuals.

4.3. Principle Three: Take full accountability

The principle of accountability is most likely to fail. Firstly, New Zealand's Privacy Laws do not offer any legal protections to individuals whose data is held and used by Clearview [18]. Furthermore, many articles by Australian media state that there is not enough knowledge or understanding of Clearview's accountability should a breach occur [19].

4.4. Principle Four: Data collection consent

Since images for Clearview are collected via automatic image scrapping from platforms such as YouTube, Facebook, Instagram, and LinkedIn as soon as they become public [17], no consent is taken before collection. However, not requesting consent before collection breaks several Information Privacy Principles (IPP) [11]. IPP 2 is violated as it states that agencies must collect biometric information directly from the individual concerned [11]. Furthermore, IPP 3 states that if agencies collect individuals' biometric information, they need to ensure that they have informed the said individual that their information has been collected and what the purpose of collection is [11].

4.5. Principle Five: Respect Privacy

From research conducted it has been deemed that Clearview does not respect the privacy of clients. The reason for this is that individuals' data can only be sold and shared if the said individual provides consent however Clearview sells and shares individuals' images to agencies without their knowledge and consent. Thus, a violation of privacy.

4.6. Principle Six: Avoid Biases

Clearview collects data from platforms such as YouTube, Facebook, Instagram, and LinkedIn [17]. To use these platforms individuals must have access to the internet. A 2021 United Nations report states that "*3 billion (37%) individuals in the world do not have access to the internet*" [20]. As a result, data in the Clearview database is biased. This is because there is over and under-representation of ethnic groups. Furthermore, Clearview is that it is an American company and in America data is collected from felon records [21]. This results in a bias formed as there is a high number of African Americans in the felony system thus there is an over-representation of one ethnic group in the database. This means that when the police used Clearview as a trial, they would have encountered bias against citizens with darker skin.

The privacy commission report stated that the dataset of Clearview is too small to be useful in New Zealand and it had difficulty identifying people of Māori and Pacific Island descent [16].

4.7. Principle Seven: Have regard for children and teenagers

As mentioned previously the method Clearview uses to collect data is through automatic image scaping of platforms such as YouTube, Facebook, Instagram, and LinkedIn [17]. This means that when images are collected, the age of individuals is not being considered. When dealing with children and teenagers, their age, as well as their level of understanding, must be considered. Therefore, before an image of a child below 13 is collected, parental consent must be given first. Thus, Clearview violates this principle as they do to take into consideration children and teenagers.

5. Conclusion and recommendations

To be able to examine, and view weaknesses, limitations, and gaps in a system, a code of ethics is vital. Therefore, for FRS a code of ethics must take into consideration the challenges as well as any obstacles that come to light. This paper highlights the ethical issues that arise if the Facial Recognition Code of Ethics is not adequately used as well as the serious consequences that would arise, such as the violation of human rights. Hence having a list of principles in the code of ethics such as transparency, fairness, non-bias, respecting privacy, and lawful surveillance is very important. These principles are of the utmost importance as it offers industry professionals as well as entities of FRS guidance to ensure that they maintain their ethical conduct.

By using the code of ethics professionals as well as entities can determine whether they are ethical. A clear example of this was highlighted in the case study of the FRS Clearview. Clearview failed to meet the majority of the principles that were outlined in the Facial

Recognition Code of Ethics. The failure to meet these principles meant that the outcome of the case study was that Clearview is not an appropriate software as it is not ethical. Thus, the key recommendation for professionals is to use the Facial Recognition Code of Ethics to ensure that their actions and behaviours remain acceptable and ethical.

References

[1] Grand View Research, 'Facial Recognition Market Size & Trend Report', 2021. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market . [Accessed: 20-Apr-2022].

[2] J.D. Woodward, C. Horn, J. Gatune, 'Biometrics', 2003. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA414520.pdf . [Accessed: 20-Apr-2022].

[3] Thales, 'Facial Recognition: top 7 trends', 2021. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition . [Accessed: 20-Apr-2022].

[4] Source Security, 'Usage of Facial Recognition around the world', 2021. [Online]. Available: https://www.sourcesecurity.com/insights/map-illustrates-usage-facial-recognition-world-sb.1591782979.html . [Accessed: 20-Apr-2022].

[5] S. Singh and S.V.A.V. Prasad, "Techniques and Challenges of Face Recognition: A Critical Review," Procedia Computer Science, vol. 143, no. 20, pp. 536-543, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918321252. [Accessed: 01-Jun-2022].

[6] A.M. Almansori, M. Taha and E. Badr, "Facial Recognition Systems using Computational Algorithms", Journal Pone, vol. 137, no. 10, pp. 201-211, 2020. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0242269. [Accessed: 01-Jun-2022].

[7] S. Lohr, 'Facial Recognition is Accurate, if You're White', 2018. [Online]. Available: http://www.cs.toronto.edu/~bor/196f21/facial-recognition-nytimes.pdf . [Accessed: 20-Apr-2022].

[8] Engineering NZ, 'Code of Ethical Conduct', 2022. [Online]. Available: https://www.engineeringnz.org/engineer-tools/ethics-rules-standards/code-ethical-conduct/ . [Accessed: 20-Apr-2022].

[9] IT Professionals NZ, 'The ITP Code of Ethics', 2022. [Online]. Available: https://itp.nz/Members/Code-of-Ethics. [Accessed: 23-Apr-2022].

[10] Privacy Commissioner, 'Home', 2022. [Online]. Available: https://www.privacy.org.nz . [Accessed: 23-Apr-2022].

[11] Privacy Commissioner, 'Office of the Privacy Commissioner position in the regulation of biometrics', 2021. [Online]. Available: https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/2021-10-07-OPC-position-on-biometrics.pdf . [Accessed: 23-Apr-2022].

[12] Privacy Commissioner, 'Principles for the safe and effective use of data and analytics', 2018. [Online]. Available: https://www.privacy.org.nz/assets/New-

order/Resources-/Publications/Guidance-resources/Principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance3.pdf . [Accessed: 24-Apr-2022].

[13] Investopedia, 'Code of Ethics', 2021. [Online]. Available: https://www.investopedia.com/terms/c/code-of-ethics.asp . [Accessed 24-Apr-2022].

[14] BBC, 'Ethics: A General Introduction', 2014. [Online]. Available: https://www.bbc.co.uk/ethics/introduction/intro_1.shtml . [Accessed 24-Apr-2022].

[15] RNZ, 'Review prompts police to halt plan', 2021. [Online]. Available: https://www.rnz.co.nz/news/national/457588/review-prompts-police-to-halt-plans-to-use-facial-recognition-technology . [Accessed 28-Apr-2022].

[16] Privacy Commissioner, 'Controversial AI software raises privacy concerns', 2020. [Online]. Available: https://www.privacy.org.nz/blog/controversial-ai-software-raises-privacy-concerns/. [Accessed 28-Apr-2022].

[17] The Verge, 'Clearview AI hit with sweeping legal complaints', 2021. [Online]. Available: https://www.theverge.com/2021/5/27/22455446/clearview-ai-legal-privacy-complaint-privacy-international-facial-recognition-eu . [Accessed 28-Apr-2022].

[18] RNZ, 'Police trailed facial recognition tech without clearance', 2020. [Online]. Available: https://www.rnz.co.nz/news/national/416483/police-trialled-facial-recognition-tech-without-clearance . [Accessed 28-Apr-2022].

[19] The Conversation, 'Australian police are using the Clearview AI facial recognition system with no accountability', 2021. [Online]. Available: https://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667 . [Accessed 28-Apr-2022].

[20] The Guardian, 'More than a third of the world's population have never used internet, says UN', 2021. [Online]. Available: https://www.theguardian.com/technology/2021/nov/30/more-than-a-third-of-worlds-population-has-never-used-the-internet-says-un . [Accessed 28-Apr-2022].

[21] How Stuff Works, 'How US Criminal Records Work', 2021. [Online]. Available: https://people.howstuffworks.com/criminal-record.htm . [Accessed 28-Apr-2022].