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

An Ethical Framework for Facial Recognition Use in New Zealand

Emma Taumoepeau

Abstract

Facial recognition technology is an increasingly growing, constantly adapting technology. It can serve many benefits for legal entities in many ways. Examples of this would be biometric recognition or border control at an airport. Because of its power and efficiency, many legal entities are looking to utilise this technology. With this continued growth comes ethical concerns about ensuring data privacy for individuals whose data is collected, used, and stored to power this technology. Currently, there is a lack of an ethical framework for legal entities to adopt, follow and utilise within New Zealand. This makes it an ethical grey area for the businesses and individuals looking to utilise this technology. This document aims to review existing frameworks about facial recognition technology, finally concluding a code of ethics for facial recognition use in New Zealand for the engineering profession.

Keywords: Facial Recognition; Code of Ethics.

1. Introduction

The Fourth Industrial Revolution is bringing technological breakthroughs such as facial recognition technology (FRT) that transform the way we design new systems and technologies. The facial recognition (FR) market is estimated to grow from USD 3.8 billion in 2020 to USD 8.5 billion by 2025 [1][2].

FR algorithms are known to be inconsistent since the early 1990s [3]. FR algorithms were found to be biased by race, gender, and age in a study by Klare et al. [4]. The study concluded that young, Black, and female faces performed worse than their counterparts from other demographic groups. Further, studies suggest that machine learning algorithms can discriminate based on racial and gender groups [5].

The National Institute of Standards and Technology (NIST) published a report on demographic influences on FR algorithms [6] in 2019. In tests conducted by NIST, 189 algorithms were compared across vendors. This report shows that FR algorithms are becoming more accurate, and this trend will continue.

Several recommendations in a report published by Lynch et al. [7] in 2020 point to the lack of regulation for FRT in New Zealand [7]. This paper aims to establish an ethical framework for using FRT in New Zealand for the engineering profession, further complementing the Lynch et al. report [7].

1.1. Background

FRT refers to a technology that can assess the similarities between a human face and an image or video frame of a face in a database to conclude a claim. However, this identification only works if the face of the individual already exists in the database.

FRT is classified as a form of biometric security, evaluating the geometric facial features of a subject. Biometric security uses measurable characteristics from a person's body that can be used in algorithms to identify a particular individual based on the unique attributes

that distinguish them from other humans. Systems for measuring biometric security include finger reader recognition systems, fingerprint readers, iris recognition systems, and vein recognition systems. Features analysis, neural networks, eigenfaces, and automatic face recognition are the most common methods of FR. Biometric characteristics and personally identifiable information of a subject added to the database is called an enrolment. FRT then creates a unique encrypted biometric template from the enrolment, along with the raw biometric characteristics, consisting of specific features on the face, such as the spacing of the eyes, the bridge of the nose, the base of the ear, and the space between the mouth and chin. The encrypted template data that is collected during enrolment of the individual is then stored in a reference or database file. An algorithm checks whether the newly generated biometric template matches a stored biometric template in the database to authenticate or identify an unknown individual [8].

1.1.1. Types of Facial Recognition Technology

The three categories of FR are authentication, identification, and categorisation.

- Authentication is the process of verifying a person's identity [9]. Authentication consists of performing a one-to-one comparison of the newly presented image of an individual against their biometric template in the database. This requires prior enrolment and consent from the person who is to be verified.

- Identification is the process of determining the identity of an unknown individual [10] by comparing their newly presented image against the same type of biometric templates in the system of many individuals. This process is a one-to-many comparison.

- Categorisation involves using biometric characteristics to build profiles of people [11].

1.1.2. Use cases

FRT can be applied to many industries and application use cases. These solutions include:

- Apples Face ID for authentication [12];
- e-gates for automated border checks [13]; and
- online authentication systems such as RealMe [14].

1.2. Objectives

This paper aims to develop an ethical framework to assist engineers in making ethical decisions when using FRT applications in New Zealand. This framework was developed based on a literature analysis presented in section 2 and discussed in section 3.

2. Literature review

This section reviews several existing ethical frameworks and data and privacy legislation. The intent and key principles of the literature reviewed in Sections 2.1, 2.2, 2.3 and 2.4 build a base for a code of ethics framework for the use of FRT in the engineering profession, discussed in section 3.

2.1. ACM

The Association for Computing Machinery (ACM) defines their Code of Ethics as a guide for computer professionals to use computing technology impactful and inspire their ethical conduct [15]. The Code is built upon eight principles, with the principle of public interest at the centre of the Code. Moreover, the Code serves as a guide for resolving

violations and facilitating ethical decision making [15]. A summary of some key principles outlined in the ACM codes of ethics that can be applied to developing ethical frameworks for engineering professionals are as follows:

2.1.1. Principle 1.3 - Be honest and trustworthy

Transparency and disclosure of system capabilities, limitations, and potential problems by professionals are critical [15].

2.1.2. Principle 1.4 - Be fair and take action not to discriminate.

The professional's responsibilities are to promote equal participation for all, including underrepresented groups [15].

2.1.3. Principle 1.6 - Respect privacy

To protect the privacy rights of individuals and the public, personal information should only be used by professionals for legitimate purposes [15].

2.1.4. Principle 1.7 - Honour confidentiality.

Information should be kept confidential unless it provides evidence of a violation of law, organisational policy, or the Code [15].

2.1.5. Principle 2.5 - Give comprehensive and thorough evaluations of computer systems and their impacts, including an analysis of possible risks.

It is important for system descriptions and alternatives to be thoroughly evaluated, recommended, and presented objectively [15].

2.1.6. Principle 2.7 - Foster public awareness and understanding of computing, related technologies, and their consequences.

Inaccurate or misleading information must be corrected by professionals [15].

2.1.7. Principle 2.8 - Access computing and communication resources only when authorised or when compelled by the public good.

Accessing unauthorised systems and data is not in the public's interest without a compelling reason to believe it is necessary [15].

2.1.8. Principle 2.9 - Design and implement systems that are robustly and useably secure.

Professionals must take measures to prevent resources from being misused or modified [15].

2.1.9. Principle 3.1 - Ensure that the public good is the central concern during all professional computing work.

Professionals must remain focused regardless of the methodologies or techniques [15].

2.2. General Data Protection Regulations

In 2018, General Data Protection Regulations (GDPR) [16] came into effect and created obligations for organisations in terms of the personal data collected, stored, and processed by them. As biometric data is deemed sensitive personal information, it should be appropriately protected [16]. Seven principles govern the processing of data under GDPR [16].

A summary of the key principles outlined in the GDPR are as follows:

2.2.1. Principle 1 - Lawfulness, fairness and transparency.
Data should be "*processed lawfully, fairly and in a transparent manner in relation to the*" [17] individual.

2.2.2. Principle 2 - Purpose limitation.
The intention, collection and purpose of data obtained from an individual must be explicitly made [17].

2.2.3. Principle 3 - Data minimisation
Data should be collected and processed for the specified purposes only [17].

2.2.4. Principle 4 - Accuracy
Data should be kept in an accurate, up to date state, where necessary [17].

2.2.5. Principle 5 - storage limitation
Data should be stored for the specified purpose for as long as necessary [17]

2.2.6. Principle 6 - integrity and confidentiality
Data should be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*" [17].

2.2.7. Principle 7 - accountability
"*The controller shall be responsible for and be able to demonstrate compliance with*" [17] all principles.

2.3. Privacy Act 2020
New Zealand's Privacy Act 2020 [18] governs how businesses and organisations are permitted to collect, store, use and share personal information. Based on 13 principles, these rules apply to general technology.

2.4. Māori Data Sovereignty
Featuring six principles, the Māori data sovereignty [19] framework protects information about Māori people, their languages, cultures, and resources.

2.5. Ethics/Sustainability issues
By analysing the literature in section 2.1, it is evident that the ACM's code is specific to practitioners in their respective fields. Frameworks such as these are useful for specific industries whose practices are mostly contained within specific fields. Although FR is a service that can be used across a wide variety of industries and fields, it requires centralised governance, creating a single source of truth. By doing so, all stakeholders involved in planning, implementing, and adopting the technology will be held accountable.

As discussed in section 2.4, the GDPR states that explicit consent must be obtained from the data subject prior to any collection or processing of personal data. Further, the regulation offers no detailed information about consent. As a result of ambiguous language in the GDPR regarding issues such as FR, existing privacy rulings may not easily apply to FR applications [20].

Through analysis of sections 2.3 and 2.4, a lack of specific rules and regulations specific to FRT in New Zealand currently exist.

3. Code of ethics/sustainability

A framework for protecting the privacy of individuals and a guide for ethical decision making, based on existing literature reviewed in section 2, follows. This section provides six core principles to help the engineering profession make ethical decisions when using FRT.

3.1. Principle 1 – Accuracy, Integrity, and Non-discrimination

3.1.1. Principle 1.1

An entity should determine the implications and magnitude of FRT before implementing it. It is imperative that biases and inaccuracies in the system are addressed both before and after deployment. Moreover, the accuracy of the system needs to be continually audited, and third parties and government officials need to be involved in monitoring.

3.1.2. Principle 1.2

Any FR system that needs to be trained on image data sets must comply with all rules and obligations under the Privacy Act 2020 [18]. Data sets containing images that are taken from the internet for training purposes are subject to consent requirements as outlined in principle 6.1.

3.1.3. Principle 1.3

An entity should take special precautions when using an FR system with individuals under the age of 18. In providing notice to and gaining informed consent from the individual, the entity must consider the age and comprehension level of said individual.

3.1.4. Principle 1.4

An entity should take appropriate measures to consult with Te Ao Māori to identify and respond to impacts and concerns Māori may have as a result of an FR system.

3.2. Principle 2 – Transparency

3.2.1. Principle 2.1

A public announcement of the use of an FR system should be released prior to its deployment. To maintain the public's confidence in the FR system, an entity should be as transparent as possible concerning the collection, use, and disclosure of biometric data as well as security measures. The entity should be transparent with respect to the algorithms used and how these are tested and audited.

3.3. Principle 3 – Governance

3.3.1. Principle 3.1

Before deploying a system, an entity should establish policies that govern how the system will be used and how data will be managed. All such policies should be open to public input, scrutiny, and oversight whenever possible. The needs of vulnerable individuals and populations should be addressed as outlined in principle 1.4 by FR system governance mechanisms before the establishment of said systems.

3.4. Principle 4 – Accountability

3.4.1. Principle 4.1

An entity should be held accountable for the consequences and/or harm of any FR system use and misuse. This includes any action resulting in a breach under any New Zealand law.

3.4.2. Principle 4.2

An entity should offer long-term sustainable technical solutions.

3.5. Principle 5 – Security

3.5.1. Principle 5.1

An entity should ensure the FR system provides and maintains the security of all data collected and stored.

3.6. Principle 6 – Collection and Use

3.6.1. Principle 6.1

An entity should obtain informed, written consent from an individual before enrolling the individual in an FR system. The entity should make the individual aware of the type of biometric data collected, the purpose of the collection, how the data processing is conducted, how the data is protected, and the ability to withdraw consent. An entity must provide an individual with the ability to easily withdraw their data consent from the FR system at any time. Individuals are given the right to object, erase, and obtain any information collected by the entity. An entity may not use a face recognition system to determine an individual's race, colour, religion, sex, national origin, disability or age.

3.6.2. Principle 6.2

Under no circumstances should an entity collect, use, or disclose any biometric data without explicit consent from the individual, even if required by law. An entity should protect all data.

4. ClearView AI

In 2020, it was reported that the New Zealand Police had tested FR software provided by the American FR company Clearview AI [21]. This prompted an audit by Police Commissioner Andrew Coster, which revealed the FR software was used without contacting the Privacy Commissioner or the Police Commissioner or notifying the public.

"*Police national manager of criminal investigations Tom Fitzgerald said its use was limited to about 150 searches of police volunteers and roughly 30 searches of persons of interest. This involved about five suspects, but each generated several searches. Fitzgerald said police only had one successful match for a person whose photo was already in the media and that the dataset is too small to be useful in a New Zealand context, and it had difficulty identifying people of Māori and Pacific Island descent*" [22].

In future, the New Zealand Police plan to establish new consultation processes to include the Police Commissioner and the Office of the Privacy Commissioner [22].

4.1. Principle 1

Principle 1.1 stipulates that an entity must conduct a comprehensive analysis of the magnitude and potential consequences of deploying an FR system. Consultation from third parties and government officials, as well as monitoring and auditing, are necessary for this principle to be met. A violation of this principle occurred when the Police Commissioner and Privacy Commissioner were not consulted, nor were the public. As a result of this violation, Police Commissioner Andrew Coster ordered an audit.

The dataset used, according to the national manager of criminal investigations at the New Zealand Police, involved five suspects. However, it's unclear whether or not those suspects consented to have their biometric data used. Unless consent was obtained, principle 1.2 would be directly violated.

Additionally, the suspects' ages are unknown. In the event that any of these suspects were under 18, this could violate principle 1.3 if informed consent wasn't obtained and the use of the data collected wasn't made clear to them.

Consultations with Te Ao Māori are required pursuant to principle 1.4 to understand the impacts and concerns of Māori. The absence of a proper consultation outside of the New Zealand Police indicates a violation of principle 1.4. Furthermore, the FR system had difficulty identifying people of Māori and Pacific Island descent.

4.2. Principle 2

There is an apparent lack of transparency in the use of Clearview AI FR by the New Zealand Police. As stated above, there was no notification from any government agencies. This is clearly against principle 2.1.

4.3. Principle 3

By failing to notify the public of the use of the FR system, principle 3.1 was violated. It is not clear whether appropriate policies were established. In any case, the public was not aware of its deployment.

4.4. Principle 4

As a result of not consulting the Office of the Privacy Commissioner, the Police Commissioner, or the public, harm and negatively views will have affected the public's view on FRT, not only in this instance but also for future use, breaching principles 4.1 and 4.2. The lack of transparency around these events about any future planning and consultation for any entity deploying FRT in New Zealand.

4.5. Principle 5

It is not publicly known if the security of the data used in the FR system by the New Zealand Police was breached. Based on the information gathered, it can be assumed that principle 5 was upheld.

4.6. Principle 6

As previously stated above, it is unclear if the New Zealand Police obtained informed consent from the five suspects to be used in the FR system. If consent was not obtained prior to use, this would be a direct violation of principles 6.1 and 6.2

5. Conclusion and recommendations

FRT uses sensitive data unique to an individual, and specific, ethical, well formulated frameworks and regulations should be implemented by a legal entity to protect an individual's privacy. Using FRT in New Zealand requires special attention for any legal entity interested in using such a system due to the lack of regulatory framework applicable there.

Due to the sensitivity of the data, there should be a common standard that is followed to ensure New Zealand's global accountability, regulation, and control of these systems. This would be controlled with the principles and framework outlined above, which cover the accuracy of the systems, integrity of data and values, ethnic recognition, transparency with the public and users, governance and control of systems and data, accountability of the legal entities and engineers, security of the data and systems and policies for collection and use of this data.

To conclude, the proposed ethical framework containing six core principles will guide and facilitate the engineering profession in making ethical decisions when using FRT applications in New Zealand.

References

[1] “Facial Recognition Market Size, Share and Global Market Forecast to 2025”, MarketsandMarkets, 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html. [Accessed: 07- May- 2022].

[2] "Facial Recognition Market Size & Trends Report, 2021-2028", Grandviewresearch.com, 2021. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/facial-recognition-market#:~:text=Key%20factors%20that%20are%20driving,face%20recognition%20in%20different%20verticals. [Accessed: 07- May- 2022].

[3] J. G. Cavazos, P. J. Phillips, C. D. Castillo and A. J. O’Toole, "Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 1, pp. 101-111, Jan. 2021, doi: 10.1109/TBIOM.2020.3027269.

[4] B. F. Klare, M. J. Burge, J. C. Klontz, R. W. V. Bruegge, and A. K. Jain, “Face recognition performance: Role of demographic information,” in *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 1789–1801, 2012.

[5] J. Buolamwini and T. Gebru, “Gender shades: Intersectional accuracy disparities in commercial gender classification” In *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, volume 81 of Proceedings of Machine Learning Research, pages 77–91, 2018.

[6] P. Grother, M. Ngan, and K. Hanaoka, “Face Recognition Vendor Test Part 3: Demographic Effects”, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2019. [Online]. Available: https://doi.org/10.6028/NIST.IR.8280. [Accessed: 07- May- 2022].

[7] N. Lynch, L. Campbell, J. Purshouseand M. Betkier, “Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework”, The Law Foundation, 2020. [Online]. Available: https://openaccess.wgtn.ac.nz/articles/report/Facial_Recognition_Technology_in_New_Zealand_Towards_a_Legal_and_Ethical_Framework/17204078/1. [Accessed:06-May-2022]

[8] “Designing an ethical, socially accountable facial recognition system”, Thales Group, 2021. [Online]. Available: https://www.thalesgroup.com/sites/default/files/database/document/2021-11/gov-wp-facial-recognition-2021.pdf. [Accessed: 08- May- 2022].

[9] “authentication - Glossary | CSRC", NIST | Computer Security Resource Center, 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/authentication. [Accessed: 08-May- 2022].

[10]"identification - Glossary | CSRC", NIST | Computer Security Resource Center, 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/identification. [Accessed: 08-May- 2022].

[11] “Office of the Privacy Commissioner position on the regulation of biometrics,” 2021, Accessed: May 08, 2022. [Online]. Available: https://privacy.org.nz/assets/New-

order/Resources-/Publications/Guidance-resources/2021-10-07-OPC-position-on-biometrics.pdf

[12] "About Face ID advanced technology", Apple Support, 2022. [Online]. Available: https://support.apple.com/en-nz/HT208108. [Accessed: 08- May- 2022].

[13] J. Sanchez del Rio, D. Moctezuma, C. Conde, I. Martin de Diego and E. Cabello, "Automated border control e-gates and facial recognition systems", *Computers & Security*, vol. 62, pp. 49-72, 2016. Available: 10.1016/j.cose.2016.07.001.

[14] "RealMe brings biometric security within arms-reach", RealMe.govt.nz, 2015. [Online]. Available: https://www.realme.govt.nz/news/realme-brings-biometric-security-within-arms-reach/. [Accessed: 08- May- 2022].

[15] "ACM Code of Ethics and Professional Conduct", Acm.org, 2018. [Online]. Available: http://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct. [Accessed: 07- May- 2022].

[16] "6 guidelines for facial recognition to build trust", Thales Group, 2022. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/facial-recognition-regulation. [Accessed: 07- May- 2022].

[17] “Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation),” *Official Journal of the European Union*, vol. L119, pp. 1-88.

[18] "Privacy Act 2020", Office of the Privacy Commissioner, 2020. [Online]. Available: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html [Accessed: 12- Oct- 2021].

[19] “Principles of Māori Data Sovereignty” Te Mana Raraunga, 2018. [Online]. Available: https://cdn.auckland.ac.nz/assets/psych/about/our-research/documents/TMR%2BM%C4%81ori%2BData%2BSovereignty%2BPrinciples%2BOct%2B2018.pdf. [Accessed: 08- May- 2022].

[20] C. Kroet, "Facial recognition probed across Europe under GDPR ahead of new AI rules", Mlexmarketinsight.com, 2021. [Online]. Available: https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/facial-recognition-probed-across-europe-under-gdpr-ahead-of-new-ai-rules. [Accessed: 08- May- 2022].

[21] M. Smith, "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI", RNZ, 2020. [Online]. Available: https://www.rnz.co.nz/news/national/416697/police-searched-for-suspects-in-unapproved-trial-of-facial-recognition-tech-clearview-ai. [Accessed: 08- May- 2022].

[22] J. Broughton, "Controversial AI software raises privacy concerns", Privacy.org.nz, 2020. [Online]. Available: https://www.privacy.org.nz/blog/controversial-ai-software-raises-privacy-concerns/. [Accessed: 08- May- 2022].