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

Facial Recognition Technology and Ethical Issues

Jason Chan

Abstract
Facial recognition technology (FRT) is being adopted across the world with little thought given to the ethical and sustainability issues it faces. FRT must address these challenges as soon as possible to avoid repercussions. The issues of data privacy, security controls, and accuracy are discussed in this paper. To address the issues, a code of ethics is created and applied to Apple's Face ID. It is found that Apple has made much progress, but still needs further improvement in its transparency of AI training.

Keywords: Facial recognition technology; Privacy; Security; Accuracy.

1. Introduction
Technology is growing and advancing at a breakneck pace, with all sorts of technology used to improve today's society. With the recent developments in FRT, concerns are raised whether this technology is an ethical one. Today, FRT is an effective biometric identification tool for advanced surveillance and real-time face scanning [1]. Facial recognition software is used for a myriad of purposes in numerous fields. In law enforcement, it is employed to find missing individuals and to verify the identity of criminals to combat human trafficking [2]. Applications of FRT have also recently appeared at schools in the form of surveillance and monitoring cheating during exams [3] [4]. Such situations raise concerns regarding privacy, security, and accuracy considering the increasing usage of FRT for law enforcement and public sectors.

The implementation of FRT applies complex algorithms to convert photographs into a "face template" based on distinct facial features of a person such as eye position, jawline length and the shape of the cheekbone [1] [2]. FRT uses a form of artificial intelligence training called Deep Learning to train from datasets to become more accurate [5]. The template is checked against pre-existing images and returns a score of a probability match.

1.1 Objective
The objective of this paper is to create a code of ethics for FRT. A literature review is conducted on FRT to collate the issues that were common among its applications. These issues are evaluated to produce a code of ethics, outlining the ethical guidelines that should be upheld for FRT. The code of ethics is applied to Apple's Face ID technology and discussed in section 4.

2. Literature review
The explosive growth of FRT is alarming as it is easy to stray from the ethical and legal standards engineers uphold without regulation. The objective of this section is to discuss the risks and concerns in FRT, and to design a code of ethics to combat these issues.

2.1. Ethics issues
According to the NZ Engineering Code of Ethics, high standards of ethical behaviour is expected from New Zealand engineers [6]. Notably, maintaining confidentiality, acting

competently and reporting adverse consequences are in line with the problems of privacy, security and accuracy that FRT faces.

Privacy – The Collection and Storage of Facial Data

Privacy is a human right. With an invasive technology like facial recognition appearing all over the world, consideration must be acknowledged in how data is overseen and stored to avoid its misuse. In 2021, a facial recognition firm named Clearview AI, was discovered harvesting 10 billion images from the internet without consent [7] [8]. Clearview AI sells their "identity matching" service to law enforcement agencies all around the world [7]. The United Kingdoms' Information Commissioner's Office, in cooperation with Australia's privacy commissioner. They found that Clearview AI's mass collection of images did not have "lawful reason to collect the information" nor did it have controls to erase information after a certain amount of time, resulting in a £17 million fine [7] [8]. Not only is the breach of privacy a grave concern, but Clearview AI's database contained billions of previously collected, potentially sensitive images, signifying a "radical erosion of privacy" [9].

In 2019, schools in China reported installing FRT to monitor attentiveness in classrooms and to perform contactless payments [10] [11] [4]. Schools like Hangzhou No.11 High School and Jingxin Youyi Middle School monitor expressions and record transactions with facial recognition, such as borrowing books at the library and paying for lunch [4]. Adopting FRT is attractive to schools because it centralises management and "improves classroom productivity," but without privacy regulations put in place, it can be exploited by those in authoritative positions [11]. Bala [10] described that "laws need to regulate the collection and storage of biometric information at schools", and further elaborated that schools were not equipped with enough technology expertise to protect against harms to privacy. Bala implies that the risks to privacy outweigh any benefits because the regulations are immature. Another study by Yu-Li Liu et al. supports this and proposes that inadequate privacy control of FRT can encourage opportunistic behaviour by those that offer it [11].

These instances illustrate cases of breaches of privacy and unethical conduct of FRT. Liu et al. stated that establishing privacy control for FRT, such as permission requests and privacy notices, can decrease the privacy concerns among people and implies a sense of control over personal information [11]. Their findings show that this freedom can lower resistance to FRT as the risk to privacy is lower [11]. If FRT continues to expand, its applications must conform to privacy regulations and establish controls to alleviate privacy concerns by ensuring the confidentiality of personal information.

Security – Security Controls and Regulation

With applications of FRT like payment transaction and identity matching for criminal tracking, appropriate security measures need to be taken. If there are inadequate security controls, facial recognition data, such as photographs, can be used for impersonation and other malicious harm [12]. In August 2019, security researchers discovered an unencrypted database, containing facial recognition data for over 1 million people [13] [14]. The database was owned by Suprema, a security company in charge of BioStar 2, a biometric lock system for access control on facilities [13]. Accessing an unencrypted database can cause severe impacts and can be adversely leveraged for financial gain [13]. Security researchers found that they could use the unencrypted data to modify existing users and create users for impersonation [14]. A method proposed by Andy Adler could reconstruct faces to bypass security systems using facial templates [15]. Adler proposed an algorithm that could generate an image and refine it until it matches its target [15]. With unencrypted databases like the BioStar 2 database, Adler's attack can be executed.

Encrypting facial templates so that its information cannot be extracted can prevent this [15].

Research shows that it is not complicated to attack commercialised facial recognition software. Lisa Thalheim et al. [16] tested how well biometric access controls prevent unauthorised access by conducting tests with commercial FRT products. Thalheim et al. found that the facial recognition products could be bypassed by displaying an image of an authorised individual [16]. They commented that "if businesses do not want to gamble away the trust in biometric technology, it should not treat the security needs of its customers so thoughtlessly" [16]. This raises questions whether FRT should even be commercialised if it can be bypassed with little effort. Nevertheless, it is vital that adequate cybersecurity laws are created.

Accuracy – Artificial Intelligence Training and Technical Challenges

The effectiveness of FRT is dependent on its accuracy, and its capability is reliant on fair training. However, in recent years, this has not been the case. In 2011, a research study conducted by the National Institute of Technologies, discovered that algorithms developed in countries like the United States and France could better identify Caucasian faces [17]. On the other hand, East Asian countries had a far greater accuracy rate for their own demographic [17]. It was inferred that the algorithm's implementation can be influenced by its weighted dataset and the development team's ethic group [17]. The implications for biased FRT are troubling considering the racial prejudice in some nations and could lead to negative ramifications.

The limitations of FRT's accuracy stem mostly from its inability to detect the same face influenced by several factors. These factors include changes in expression, camera angles, ageing and accessories [18]. Using FRT, law enforcement in South Wales misidentified 2,297 people as potential offenders during a football match in 2017 [19]. The police officers defended that it was due to the low-resolution images. Critics find the case startling, and that it is "a threat to civil liberties and a dangerously inaccurate policing tool" [19]. In Maine, the state has already banned FRT [20]. If such challenges are not addressed, cases like these will continue to arise.

Another aspect of accuracy is its capacity to provide assurance in improved security. While the efficacy of FRT is unproven in some countries, others have shown approval. Genia Kostka conducted a study to determine the acceptance levels of FRT in China, Germany, United Kingdom and United States using online surveys [3]. They found that China was among the highest in acceptance level of FRT at 67%, almost twice as much as Germany's level at 38% [3]. Participants from China and Germany had differing definitions of privacy, but both agreed that improved security was important [3]. Given the different levels of FRT adoption and country variances in FRT, they concluded that establishing a global regulatory response would be challenging [3]. Given that each country has its own notion of privacy, creating country specific FRT legislation may be a better option. Accuracy is important not only for the advancement of FRT in society, but also for public perception.

3. Code of ethics

The proposed code of ethics comprises of the following principles:

- Ensure that privacy is preserved in all stages of information processing and storage with appropriate security controls
- For commercial use, the collection of information must not be collected unless consent is provided by the user
- For law enforcement, surveillance must be limited to only targeted individuals

- Facial recognition technology must always strive in improving its accuracy to remain fair and unbiased
- Organisations must establish compliance procedures that describe how data is utilised and a means to validate the accountability

3.1. Principle – Ensure that privacy is preserved in all stages of information processing and storage with appropriate security controls

Organisations must ensure that the privacy of facial recognition data is persevered in all phases of data collection and storage as well as to adopt adequate cyber security controls. For example, an organisation from Europe must comply with the General Data Protection Regulations. Other organisations must comply with data protection privacy laws from their own country. If data protection and privacy laws are absent, FRT should not be adopted at all. Any facial recognition product must comply with regulations to avoid unethical conduct and breaches of privacy.

3.2. Principle – For commercial use, the collection and use of information must not be collected unless consent is provided by the user

Any commercialised FRT products must explicitly prompt the user to consent for the collection of facial recognition data. If the user provides consent, the use of information is strictly limited to what the user determines. If the user does not consent to the collection of their information, they may not have access to the full functionality of the product.

3.3. Principle – For law enforcement, surveillance must be limited to only targeted individuals

Facial recognition surveillance is exclusively confined to matching certain persons. This means that surveillance in public places to detect potential offenders is prohibited in order to protect human rights. For example, utilising face recognition to hunt for missing people in known areas is permitted, while identification matching for potential offenders in a crowd is not. If surveillance is carried out, it must be done in a legal and ethical manner.

3.4. Principle – Facial recognition technology must always strive in improving its accuracy to remain fair and unbiased

Developers of FRT must always continually improve its accuracy. This necessitates overcoming technological obstacles such as recognising faces at different angles, changes in expression, ageing and identifying faces with accessories. To reduce image quality variance, FRT should use standardised cameras. Facial recognition AI must only be trained with unbiased datasets so that there is no discrimination to any demographic. The datasets must include an equal number of faces from different genders, ethnic groups, religions, sexuality, and disability. Furthermore, the development teams of FRT should be made up of people from a variety of ethnic backgrounds to ensure that any bias is avoided.

3.5. Principle – Organisations must establish compliance procedures that describe how data is utilised and a means to validate accountability

Organisations must establish clear compliance procedures that outline how data is used and maintained. These procedures should be explicit in their description of all FRT-related processes. All data processing and storage practices must be justified and lawful. If a policy changes, users should be notified and have access to their data. Organisations should also be held accountable for breaches of privacy or misconduct. A qualified entity or individual should regularly evaluate compliance procedures and modify accordingly.

4. Case study: Apple

Apple, one of the largest technology companies that specialises in consumer devices, has recently made efforts towards replacing their fingerprint scanners with Face ID. Face ID is a biometric authentication system that uses facial recognition [1] [21]. Face ID allows the user to unlock their Apple device, verify payments as well as sign into apps [21]. In this section, each principle will be applied to this case study and will be discussed.

4.1. Principle – Ensure that privacy is preserved in all stages of information processing and storage with appropriate security controls

While there are worries that Face ID is insecure and that data collected through face recognition may be exploited, Apple prioritises privacy [22] [21]. Apple complies with several information security standards like FIPS 140-2/-3, ISO-27001 and ISO/IEC 27018 for data encryption, information security management and best practices with sensitive information in the cloud, respectively [23].

Additionally, Apple has also implemented many security safeguards to protect information. Face ID, for example, assesses probability matches based on depth information not available in photographs. [21]. Nevertheless, the chance of unlocking a phone with Face ID with someone else's face is less than 1 out of 1,000,000 [21]. If there is a high probability, but not complete match, Face ID prompts the user to input their pin code [21].

4.2. Principle – For commercial use, the collection and use of information must not be collected unless consent is provided by the user

Apple does not collect personal information from its users. While the facial template of the user is stored in the device for Face ID to function, it is not sent to the cloud [1] [21]. This is a great security measure for lessening the impact of data breaches. For Face ID to operate, the user must scan their face to create the facial template [21]. Face ID is an optional feature and can be disabled. Users can also delete all their data from their device or other services like Find My iPhone [21].

4.3. Principle – For law enforcement, surveillance must be limited to only targeted individuals

Apple does not provide personal information to law enforcement. This is because personal data is only stored locally on the device, as mentioned previously [21]. Apple does not have access to the personal data collected by Face ID and hence is unable to assist law enforcement [24].

4.4. Principle – Facial recognition technology must always strive in improving its accuracy to remain fair and unbiased

Apple has made significant improvements on the technical challenges of FRT. Face ID has the capability to recognize whether someone is looking at the camera, faces in total darkness and people wearing glasses and hats [21]. Faces can even be identified with face masks in more recent iterations. Because Face ID is featured on specific Apple products, the variance in image quality in hardware is minimalized [21].

Although Apple has stated that they trained Face ID with a billion samples of different faces but could not specify exact details on ensuring equal representation [24]. In 2018, Apple's Face ID could not recognize two Chinese women apart [25]. This suggests that there may be some bias to other demographics, leading to inaccuracies in the technology. While Apple still needs to refine their face recognition training to ensure that their technology is fair.

4.5. Principle – Organisations must establish compliance procedures that describe how data is utilised and a means to validate accountability.

Apple has established compliance procedures and complies with the international standards, ISO:27001 and ISO:27018 [23] [26]. This implies that Apple has performed the due diligence in maintaining and adjusting their policies. Users have access to their personal information and can delete it, giving users control of their privacy [21]. Face ID is an optional feature and can be disabled [21].

Apple also undertakes third-party and internal assessments on a regular basis and adjusts their training and policies accordingly [26]. The results are reported to the Audit and Finance Committee of the Board of Directors [26].

5. Conclusion and recommendations

Without effective oversight, FRT is being rapidly adopted around the world. This case study explores the ethical and sustainability issues that FRT faces and proposes a code of ethics to address these issues. The current progress against ethical issues can be evaluated by applying the proposed code of ethics to a specific case. Ensuring that FRT takes appropriate security measures, prioritises data privacy and strives to improve will help in standardisation of regulations and the improvement of public perception.

While the current ethical issues are alarming, there are encouraging signs of progress. Corporations such as Apple have made substantial progress in these areas, but more needs to be done if humanity is to fully embrace FRT.

References

[1] Kaspersky, "What is Facial Recognition – Definition and Explanation," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition. [Accessed 20 April 2022].

[2] J. Lynch, Face Off: Law Enforcement use of Facial Recognition Technology, 2020.

[3] G. Kostka, L. Steinacker and M. Meckel, "Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States," vol. 30, no. 6, 2021.

[4] T. F. Chan, "A school in China is monitoring students with facial-recognition technology that scans the classroom every 30 seconds," [Online]. Available: https://www.businessinsider.com/china-school-facial-recognition-technology-2018-5. [Accessed 25 April 2022].

[5] BUSINESS CASES, "What Is AI Facial Recognition Tech and How does It Work?," REC FACES, 30 January 2021. [Online]. Available: https://recfaces.com/articles/ai-facial-recognition#:~:text=Recognition%20AI%20FAQ-,What%20is%20AI%20facial%20recognition%3F,are%20detected%20in%20a%20scene.. [Accessed 2 May 2022].

[6] Engineering New Zealand, "CODE OF ETHICAL CONDUCT," [Online]. Available: https://www.engineeringnz.org/engineer-tools/ethics-rules-standards/code-ethical-conduct/. [Accessed 22 April 2022].

[7] R. Davies, "US facial recognition firm faces £17m UK fine for 'serious breaches'," The Guardian, 29 November 2021. [Online]. Available: https://www.theguardian.com/technology/2021/nov/29/us-facial-recognition-firm-faces-17m-uk-fine-for-serious-breaches-clearview-ai. [Accessed 20 April 2022].

[8] N. Lomas, “Clearview AI told it broke Australia’s privacy law, ordered to delete data,” 4 November 2021. [Online]. Available: https://techcrunch.com/2021/11/03/clearview-ai-australia-privacy-breach/#:~:text=After%20Canada%2C%20now%20Australia%20has,law%20enforcement%20agencies%20and%20others.. [Accessed 22 April 2022].

[9] K. Hill, “The Secretive Company That Might End Privacy as We Know It,” The New York Times, 18 January 2020. [Online]. Available: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. [Accessed 27 April 2022].

[10] N. Bala, “The Danger of Facial Recognition in Our Children's Classrooms.,” no. 18, p. 249.

[11] Y.-l. Liu, W. Yan and B. Hu, “Resistance to facial recognition payment in China: The influence of privacy-related factors,” *Telecommunications Policy,* vol. 45, no. 5, 2021.

[12] M. Faundez-Zanuy, “Biometric security technology.,” *IEEE Aerospace and Electronic Systems Magazine,* vol. 21, no. 6, pp. 15-26, 2006.

[13] J. Taylor, “Major breach found in biometrics system used by banks, UK police and defence firms,” The Guardian, 14 August 2019. [Online]. Available: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms. [Accessed 22 April 2022].

[14] G. Fawkes, “Report: Data Breach in Biometric Security Platform Affecting Millions of Users,” 22 August 2019. [Online]. Available: https://www.vpnmentor.com/blog/report-biostar2-leak/. [Accessed 22 April 2022].

[15] A. Adler, “Sample Images can be Independently Restored from Face Recognition Templates,” [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1226104. [Accessed 29 April 2022].

[16] L. Thalheim, J. Krissler and P.-M. Ziegler, “Body Check,” *Biometric Access Protection Devices and their Programs Put to the Test,* p. 114, 2009.

[17] C. GARVIE and J. FRANKLE, “Facial-Recognition Software Might Have a Racial Bias Problem,” 7 April 2016. [Online]. Available: https://apexart.org/images/breiner/articles/FacialRecognitionSoftwareMight.pdf. [Accessed 27 April 2022].

[18] T. Horiuchi and T. Hada, “A Complementary Study for the Evaluation of Face Recognition Technology,” 2013. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6922048. [Accessed 27 April 2022].

[19] P. Association, “Welsh police wrongly identify thousands as potential criminals,” 5 May 2018. [Online]. Available: https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals. [Accessed 27 April 2022].

[20] J. Bryant, “Maine passes statewide facial recognition ban,” iapp, 1 July 2021. [Online]. Available: https://iapp.org/news/a/maine-passes-statewide-facial-recognition-ban/#:~:text=Maine%20passed%20a%20law%20banning,The%20bill's%20sponsor%2C%20State%20Rep.. [Accessed 29 April 2022].

[21] Apple, “About Face ID advanced technology,” 27 April 2022. [Online]. Available: Sig. [Accessed 1 May 2022].

[22] R. Jennings, “Apple's FaceID falls foul of privacy farce, security pros just say no,” [Online]. Available: https://techbeacon.com/security/apples-faceid-falls-foul-privacy-farce-security-pros-just-say-no. [Accessed 1 May 2022].

[23] Apple, “Security Certifications and Compliance Center,” December 2021. [Online]. Available: https://help.apple.com/pdf/sccc/en_US/security-certifications-compliance-center.pdf. [Accessed 1 May 2022].

[24] N. Lomas, “Apple responds to Senator Franken’s Face ID privacy concerns,” 17 October 2017. [Online]. Available: https://techcrunch.com/2017/10/17/apple-responds-to-senator-frankens-face-id-privacy-concerns/. [Accessed 1 May 2022].

[25] THEWEEK, “Is facial recognition technology racist?,” July 28 2018. [Online]. Available: https://www.theweek.co.uk/95383/is-facial-recognition-racist. [Accessed 1 May 2022].

[26] T. Cook, “Ethics and Compliance,” [Online]. Available: https://www.apple.com/compliance/. [Accessed 1 May 2022].