FACIAL RECOGNITION TECHNOLOGY: CONSIDERATIONS FOR USE IN POLICING

Nessa Lynch & Andrew Chen

An independent report commissioned by New Zealand Police examining the current use and potential use of facial recognition technology in policing in Aotearoa New Zealand.

TABLE OF CONTENTS

Part 1. Executive Summary 3

Part 2. Introduction and Methodology 7

Part 3. Introduction to Facial Recognition Technology 11

Part 4. Collection and Retention of Facial Images 22

Part 5. Uses and Potential Uses of FRT in Policing 29

Part 6. Considerations in a New Zealand Context 41

Part 7. Lessons from Comparable Jurisdictions 60

Part 8. Recommendations 73

Appendix. Summary Charts: Considerations and Risk Framework 84

PART 1. EXECUTIVE SUMMARY

An Introduction to FRT

- Facial recognition technology (FRT) is a term used to describe a range of technologies involving processing of a person's facial image. Live automated FRT is just one aspect.
- FRT's main usages are verification, identification and categorisation & counting.
- A facial image is a biometric. Although it may be collected from a distance, without the person's knowledge, and in public, it involves an intrusion on the individual's privacy.
- FRT may augment and speed up existing human capabilities (finding a person in CCTV footage) or create new capabilities (detecting emotional states of people in crowds).
- The use of FRT is increasing in the public and private sectors in Aotearoa New Zealand.
- Accuracy and bias are key concerns. There are no studies specifically on the accuracy rates of the population of Aotearoa New Zealand.

Collection and Retention of Facial Images

- Police collect and retain facial images in a wide variety of contexts, under different legislative requirements and for a range of purposes.
- A full review of Police's collection, retention, storage and use of facial images was not part of our terms of reference, but we make some comments relating to how these images could form part of the source database or 'watchlists' for future expanded use of FRT.
- Our conclusion is that facial images collected by Police appear to be held in separate systems or 'buckets', and the images were of vastly varying age and quality.
- There is no or little current capability for combining image databases for wider facial comparison and recognition mechanisms, but this is a risk to be managed.

Current and Potential Uses of FRT in Policing

- There are a range of current and potential future uses of FRT, and a blanket ban on FRT is likely to capture systems that are low risk.
- Current or imminent planned use of FRT is limited and relatively low risk including:
    - Authentication for access to devices such as iPhones,
    - Identity matching in the IMS system (which will soon be implemented),
    - Retrospective analysis of lawfully acquired footage in limited situations.
- A range of potential uses for FRT in policing are explored in this report, but there is no inference that Police are planning or considering these

uses. We found no evidence that Police are using or formally planning the use of live automated FRT.

- Police should consider the spectrum of use and spectrum of impact when assessing the use of FRT and avoid high-risk use cases. Police did undertake a limited trial of a high-risk usage (Clearview) but are not currently trialling or considering other high-risk usages.
- There are challenges with the use of third-party camera networks and OSINT data sources that need to be carefully considered.

Considerations in a New Zealand Context

- We endorse the approach in Police's draft New Technologies Framework to consider the legal, ethical and other impacts of new technologies before commissioning and implementation. The analysis of considerations in this report should assist in any consideration of expansion or new uses cases for FRT applications specifically.
- Police have a duty to consider, review and implement new technologies which would advance a function of the Police, in particular to prevent and detect crime, to improve public safety and reduce harm to communities.
- Warrantless use of a FR equipped camera in a public place could be considered a 'search' because of the increased technical capabilities of FR as opposed to regular CCTV or recording. This would attract the legislative processes and protections offered in the *Search and Surveillance Act 2012*. The issue of reasonable expectation of privacy in a public place is an evolving legal issue. A legal opinion should be sought before any decision to use live automated FRT.
- FRT, particularly live automated FRT, has a significant potential impact on individual and societal privacy interests. Privacy risks can be ameliorated through a quality and comprehensive Privacy Impact Assessment with appropriate oversight and governance mechanisms which monitor the implementation of the risk assurance conditions. Consultation with diverse communities is also important.
- Privacy impact assessments are an embedded process within Police, but commissioning and use of any FRT system, particularly live automated FRT, should also consider impacts on other rights and interests and the proportionality of those impacts. For example, monitoring of protests or community events with live automated FRT could have a chilling effect on rights to freedom of expression and peaceful assembly. An expansion of facial comparison systems to include large scale collection from those who have not been convicted or charged could impact on a person's right to be presumed innocent until proven guilty.
- Policies for retention and facial comparison of facial images from children and young persons should align with the established youth justice principles premised on reintegration and align with the principles and rules relating to other biometrics such as DNA and fingerprints.

- Technical standards for accuracy and facial comparison should consider any evidence on how children's faces develop and the particular issues relating to accuracy.
- Decision-making around application of FRT to situations and locations where children and young people are likely to be present should specifically consider the rights and interests of children and young persons and consultation with the Office of the Children's Commissioner should be undertaken.
- Māori are likely to be most impacted by any expanded use of FRT or implementation of live automated FRT. Police should also undertake further consultation to further explore any cultural considerations around collection and retention of facial images. This should be conducted early in the exploration process when considering adoption of a new FRT tool.
- Government standards set principles for the safe use of algorithms and data analytics. Of particular relevance to FRT is the human oversight element.
- Police have received independent advice on the commissioning, risk categorization and governance standards around algorithms, including those related to current FRT use. We generally agree with the independent advice that has been shared with us.
- There is very limited current evidence base for the efficacy and cost benefit of live automated FRT in policing. Any proposal for broadening of the use of FRT or implementation of live automated FRT must identify a clear problem to be solved that the proportionality and appropriateness of the technology use can be assessed against.
- Inappropriate or unjustified expansion of FRT, particularly live automated FRT, may have a negative effect on police-community relations. There are few specific studies of public opinion on FRT in the context of Aotearoa New Zealand. Studies from other jurisdictions indicate greater public acceptance of law enforcement use of FRT when compared to other use-cases. Social licence would have to be carefully gauged, including genuine engagement with diverse communities.

Lessons from Comparable Jurisdictions

- Other comparable jurisdictions are further ahead in deploying live automated FRT, but there are issues where deployment has preceded clear and transparent principles and rules.
- The impact of FRT has led to public concern, and in some cases backlash.
- Comparable jurisdictions are now looking to establish regulations and guidelines, and in some cases have banned or restricted certain high-risk applications of FRT.
- Action against FRT has come from a combination of individuals and activists, legislatures, courts, and self-regulation by tech companies.
- Police should continue to monitor comparable jurisdictions closely, and use the valuable opportunity to avoid errors made elsewhere.

Recommendations:

- Recommendation 1 – Continue to pause any consideration of live automated FRT
- Recommendation 2 – Review of collection and retention of facial images
- Recommendation 3 - Continue to strengthen processes for ethical commissioning of technology
- Recommendation 4 - Ensure continuous governance and oversight of deployment
- Recommendation 5 – Upholding Te Tiriti in partnership with Māori
- Recommendation 6 – Transparency
- Recommendation 7– Policy statement on surveillance in public places
- Recommendation 8 – Implement guidelines for access to third party systems
- Recommendation 9 - Embed a culture of ethical use of data in the organisation
- Recommendation 10 – Implement a system for ongoing horizon scanning

PART 2. INTRODUCTION & METHODOLOGY

2.1. Terms of Reference

The terms of reference for this work is to produce a written report on the following topics:

- *Definitions:*
    - *What is facial recognition technology (and what is it not),*
    - *Categorising the spectrum of usage in a policing context - from automatic 'live' FRT to 'almost' real time data matching to one to one matching,*
    - *The spectrum of effect on individual and collective rights and interests.*
- *Police's current and planned operational activity:*
    - *What Police currently does and does not do in the FRT space,*
    - *What is planned and what unused capability there is within in the organisation*
    - *Discussing and dispelling myths around nationwide live surveillance.*
- *Insights and evidence:*
    - *Insights from local and international contexts on broader/other uses of FRT in the policing context,*
    - *How those uses are (or could be) perceived in New Zealand,*
    - *Operational advantages of FRT for public safety, crime control etc*
    - *Effect on human rights, privacy, ethical frameworks, Te Tiriti implications, indigenous data sovereignty etc. For research relating to Te Tiriti implications and indigenous data sovereignty, relevant indigenous experts may be spoken with and the researchers will discuss this in advance with Police.*
- *Advice and recommendations:*
    - *Point-in-time advice and recommendations on what uses of FRT are safe and appropriate in a New Zealand policing context [particularly considering matters of bias/technology limitations, Police's need to maintain a social licence to operate, privacy rights, the Crown-Māori partnership, and Police's mandate to enforce the law and keep New Zealanders safe, etc.]*
    - *Advice around appropriate Police policy, operational, and audit safeguards for current use and any recommendations to broaden, or narrow, use (if applicable, following the in-depth analysis).*
- *A visual summary of Police's FRT use and future opportunities, which may be used for external communication purposes.*

2.2. The Researchers

Dr Nessa Lynch – Associate Professor at the Faculty of Law, Te Herenga Waka - Victoria University of Wellington. Expertise in criminal law, biometrics, data ethics and youth justice and children's rights.

I note the following relevant conflicts of interest: Interim Chair of the Data Ethics Advisory Group (convened by the Government Chief Data Steward); Observer for the Cross- Government Biometrics Group; Chair of Advisory Group on Queue-Counting Trial at Wellington Airport for AvSec/Civil Aviation Authority.

Dr Andrew Chen – Research Fellow with Koi Tū: The Centre for Informed Futures at Waipapa Taumata Rau - The University of Auckland. Expertise in AI/Machine Learning, computer vision, and digital technology ethics.

I note the following relevant conflicts of interest: Member of the Privacy Foundation; Independent Member of the Immigration NZ Data Science Review Board.

All views expressed here are our own views and not those of our employers or of New Zealand Police.

2.3. Methodology

The methodology for this project used a combination of literature review, legal reasoning, analysis of theoretical frameworks and stakeholder consultation and interviews.

Nessa Lynch would like to acknowledge her co-authors on the Law Foundation funded project – Professor Liz Campbell, Dr Joe Purshouse and Dr Marcin Betkier as aspects of this report draw on the source material and the final published report from that project.[1]

We also had access to draft material from two internally developed frameworks for Police use of emergent/new technology. In the latter stages of our work, there was the public release of the Taylor Fry *Safe and ethical use of algorithms* report from June 2021.[2] We also draw from Police documents such as Privacy Impact Assessments, previously released under Official Information Act requests to the researchers and journalists, and some proactively released on the Police website.

[1] Lynch N, Campbell L, Purshouse J, Betkier M. Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework Dec 2020 (Report) https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf

[2] Taylor Fry – *NZ Police Safe and Ethical Use of Algorithms* https://www.police.govt.nz/sites/default/files/publications/safe-ethical-use-algorithms-report.pdf

We were provided with unfettered access to all relevant Police staff, documents and business units. Scoping interviews were held with the following business areas:

- Criminal Investigations
- Auckland District
- Mobility and Digital
- Chief Information Officer
- High Tech Crime Group
- Wellington District Intelligence
- Legal Services
- Privacy Team
- Forensics (biometrics)
- ANPR/Auror portfolio
- National Biometric Information Office
- DCE Insights and Deployment

We also met with Auror and Safer Cities separately as they provide connections for Police to community and private CCTV cameras and ANPR (Automatic Number Plate Recognition) systems.

A structured interview model was used for the interviews with stakeholders. We asked a standard set of questions of all interviewees including:

- What is your role?
- What do you understand by 'facial recognition technology?' What does FRT enable you to do?
- What ways are facial recognition being used in your work area?
- What are the names of the technologies being used / vendors who provide technologies?
- How is the technology commissioned?
- What ethical/legal/privacy processes are followed in commissioning the technology?
- What is the role of consulting with the community when deploying these technologies? Which communities, and through what mechanisms?
- What governance arrangements are in place?
- What decisions are made as a consequence of outputs of FRT systems? Are any automated?
- How accurate does a FRT system need to be to give you confidence that it is working and that the outputs are reliable?
- Who has access to FRT systems and their outputs?
- What are the key risks that worry you in terms of the use of FRT?

We then had specific questions for the person or group depending on what their workgroup and area of expertise was, and interviewees were given the opportunity to give further information or views further to the structured questions.

All interviewees were provided with a draft of the report so that they could check that the information reported relating their work area was accurate, and all interviewees were invited to the internal briefing session on the draft report and findings and had an opportunity to give further feedback directly to the authors if desired.

The report benefitted from feedback from those who were interviewed, from an internal Police group that participated in a briefing, and from an external stakeholder group who participated in a briefing. We also received advice and feedback from Police's independent advisory panel on emergent technologies.

2.4. Other Contextual Comments

Facial recognition technology is a rapidly evolving field with reports and literature being published regularly. This is a point in time analysis as of November 2021.

It is difficult to predict how the technology may develop, how it may be used in other jurisdictions, or how regulations may evolve, all of which may influence how Police use (or not use) the technology into the future.

PART 3. INTRODUCTION TO FRT

This section defines facial recognition technology and discusses its principal use-cases and parameters of use.

3.1. Definition of Facial Recognition Technology

Facial recognition technology (FRT) involves identification of an individual based on an analysis of their geometric facial features, and a comparison by an algorithm between the features extracted from the captured image and one already stored. Identification/recognition is just one element because images (or recordings) need to be first collected in the form of data, and those data are stored in the computer system until they are deleted.

The software takes digital images (e.g. those collected from a camera or stored in an image database) and performs mathematical operations to detect faces of individuals. Data describing faces are normalised (e.g. scaled, rotated, aligned, etc.) to the form in which the facial features can be recognised. The FRT algorithm extracts features that individually describe a particular person. Sometimes these features may correspond to features describable by human language (e.g. "distance between eyes") but they are generally too complex for non-mathematical description. Those features are stored and compared (or matched) with features that had been previously collected and are on a list (or in a database) available to the algorithm.[3] The outcome of the comparison depends on the use case scenario. If a match is found, the computer may, for example, signal that match to the human operator or perform other (or additional) automated tasks.

3.2. Principal Uses

3.2.1. *Verification*

Verification involves the comparison of two biometric templates to verify a person's identity. This is a "one on one" comparison.

Examples of usage include access control, such as the SmartGate system at the border, using Face ID to unlock an iPhone, or other security access systems.

3.2.2. *Identification*

This involves the comparison of an individual's biometric template to a database of images to find the matching identity. This is typically a "one to many" and could be a "many to many" comparison in a surveillance scenario where multiple faces are found in an input image.

Examples of usage include scanning a crowd for people on a 'watchlist' of images, or attempting to identify a person whose identity is currently unknown by matching their image against a database of faces. A distinction may be drawn between inputting a static image versus using video footage where

[3] See also *R. (On Application of Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019)* [23] ff.

having a sequence of images gives the algorithm more chances to make a correct match, and a further distinction between 'offline' or retrospective analysis of images versus 'online' or live analysis of footage in real-time.

3.2.3. *Analytics and Trends*

FRT may also be used to extract demographic information about a person such as gender, age, and ethnicity. This is also known as 'face analysis'[4] and often informs 'video analytics'. It does not specifically identify a person, but if characteristics are inferred from a facial image and potentially linked to other data (e.g. location data), it could enable the de facto identification of an individual.[5]

Technology for emotion recognition is also being developed, which analyses the structure of the face to determine if someone is happy, sad, excited, etc. Although the academic literature shows that this is a relatively nascent technology that is generally not reliable enough for use in real-world scenarios[6], there are vendors who have incorporated these capabilities into their products.[7]

Captured images may also be subject to other forms of detection and recognition, such as counting the number of people seen, or classifying the model and make of a car that is next to a person. For example, commercial systems are available for crowd counting from CCTV video feeds at large-scale events (although the accuracy is questionable in comparison to manual counts). The Civil Aviation Authority (CAA) is currently running a trial at Wellington Airport to count the number of people that pass through airport security, using facial recognition to distinguish between passengers and known staff members so that the CAA can establish its performance against KPIs.[8]

3.3. Speed and Scale versus New Capabilities

Some functions of FRT increase the speed and scale of activities currently performed by humans, such as identity matching against a database, and the retrospective processing of large amounts of CCTV footage to identify particular persons. The time saving on human effort can be significant, and computers may be less likely to make mistakes when processing data at large scales. It can be argued that in these scenarios, the FR process is still auditable

[4] Michal Kawulok, Emre M Celebi and Bogdam Smolka (eds) *Advances in Face Detection and Facial Image Analysis* (Springer International Publishing, Switzerland, 2016).

[5] European Union Agency for Fundamental Rights *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Publications Office of the European Union, 21 November 2019) at 8.

[6] Khanal et al. report 60% true positive accuracy in "Performance analysis of Microsoft's and Google's Emotion Recognition API using pose-invariant faces", *Proceedings of the 8th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion*.

[7] See for example, NEC and Realeye's partnership: https://findbiometrics.com/nec-realeyes-unveil-biometric-emotion-analytics-service-102303/.

[8] See information and Privacy Impact Assessment here: https://www.aviation.govt.nz/assets/passenger/PIA-AVSEC-Queue-Counting-Trial-25-May-21-Final-TRZNB_Redacted.pdf

by humans (i.e. the task could be checked and repeated by humans if necessary), and that humans would be in the loop to make decisions based on the outputs, so therefore the risk of errors leading to negative impacts may be relatively low. However, auditing FR systems may still carry ethical concerns.[9]

Using FRT to improve existing capabilities should be distinguished from enabling new capabilities, such as using emotion recognition to monitor the mood of a crowd in real-time. It could be argued that some of these tasks are also simply speed and scale improvements of human processes, but the important distinction is that in these scenarios it has been previously considered impractical for humans to achieve these tasks. For example, it is theoretically possible for humans to watch CCTV footage and record the movements of every person in the city, but it is impossibly resource-intensive. Using FRT to automate this would therefore provide new capabilities, producing data and information that previously could not be produced by humans.

As we discuss further below, most of the applications that we found being used by Police fall in the first category, where the use cases were previously existing and achieved by humans. This distinction is important as the technology improves, and Police should be aware of the differing implications of new applications that previously may not have been achievable.

3.4. Facial Images as a Biometric

A biometric is a measurement or physical characteristic that may be used to identify an individual.[10] FRT differs from other biometrics (DNA, iris scan, fingerprint)[11] in that a person's face is generally public and its image can be collected from a distance, and without the knowledge of the person. It does involve intrusion on privacy:[12]

> FRT is a formidable technological innovation that allows us to connect a part of us that is inherently private, our identity, with a part of us that is inherently public, our face. Relative to other biometric technologies, FRT stands out because our face is one of our most immutable features and one of the parts of our body that we most identify with. Moreover, in most cultural contexts, our face is always exposed to the public, making it difficult to participate in societal life without revealing one's face.

[9] Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee, Emily Denton *Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing* (Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, February 2020).

[10] Cross Government Biometrics Group (2009), Guiding Principles for the Use of Biometric Technologies.

[11] Nessa Lynch, Liz Campbell, Alexandra Flaus and Elena Mok *The Collection and Retention of DNA from Suspects in New Zealand* (Victoria University Press, Wellington, 2016).

[12] Henriette Ruhrmann *Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement* (Goldman School of Public Policy, May 2019) at 73.

As England and Wales' former Biometrics Commissioner has noted:[13]

> …unlike existing police biometrics whose acquisition is quite complicated, digital facial image capture is easy and the subject may not even be aware that it has happened. For the same reason, faces in public places can be easily scanned and matched. In other words, this is potentially much more intrusive of an individual's privacy than existing police biometric use. That is not to say that there may not be a public interest case that justifies such intrusion when balanced against the public benefits derived.

Discussion in case law has also made this distinction: in the High Court decision *R. (Bridges) v Chief Constable of South Wales Police*[14] – where a campaigner from Cardiff failed to convince the High Court of Justice for England and Wales that his human rights had been violated after his face was scanned on two occasions by the South Wales Police - the Court viewed this distinction as significant. Haddon-Cave LJ and Swift J observed that there is an important distinction between 'intrusive' and 'non-intrusive' methods of gathering personal information. Live automated FRT was the latter and only the former fell outside the general common law powers of the police. The High Court ruled that the distinction turned on whether there was a physical intrusion with a person's rights vis-à-vis his or her home or interference with his or her bodily integrity.[15] It held that only these forms of 'physical' intrusion require a statutory legal basis. Whilst there are significant differences between different forms of biometric data processing technology, we submit that the physical/informational intrusion distinction drawn by the Court is too blunt to serve as a useful gauge for the extent to which a technology such as FRT should be regulated.

Adjacent to other biometric technologies are proxy biometrics such as Automated Number Plate Recognition (ANPR), which strictly speaking are not biometrics as they are not based on a biological identifier but can be used to achieve similar purposes. ANPR uses Optical Character Recognition (OCR) to read number plates, which can then be tied to owner records to identify people related to the vehicle. Tracking the movement of a vehicle in real-time may also be used as a proxy for tracking an individual inside the vehicle, for example to follow a person fleeing the scene in a stolen car. It is an interesting technology because it is highly accurate – often over 99% – and provides examples of how FRT may be used if/when it achieves similar accuracy rates.

3.5. Accuracy and Bias in FRT

Discrimination and bias have been a key criticism of FRT. This stems from academic research that has shown that FRT is less accurate on faces of certain

[13] Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020) at [37].
[14] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin).
[15] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at [74].

ethnicities and genders.[16] There are multiple potential causes, but it is primarily attributed to a lack of representation in the training datasets that are used to teach FRT systems how to distinguish between faces. Some researchers have gone as far as to claim that FRT is inherently biased and that this is an irresolvable problem, while most agree that larger datasets with better training methodologies should lead to better accuracy.[17] This is likely because commercial products trained on different datasets (particularly where those datasets have been derived from different countries) have demonstrated different biases against different ethnicities.[18] More recent studies conducted by the National Institute of Standards and Technology (NIST) suggest that ethnic and gender bias is disappearing in commercial FRT systems, although some researchers are still sceptical about the validity of the results[19]. However, with the use of FRT by police forces in the real world, this issue has now moved beyond academic debate.

Cases in the United States have demonstrated the problems when action is taken based on a flawed match. A man in Michigan was arrested for a crime he did not commit due to faulty facial recognition match. He was detained overnight, had mugshot and fingerprints taken. "[H]is case may be the first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm, according to experts on technology and the law."[20] Protesters in Detroit demanded the police stop using FRT due to its difficulties identifying the faces of black citizens accurately.[21] Police in the US used FRT to track and find a prominent Black Lives Matter protestor in relation to an assault on an officer, [22] while there have also been reports that FRT was used to identify individuals who attacked the US Capitol in 2021.[23]

NIST, a subgroup of the US Federal Department of Commerce, has provided technical evaluation of over 100 commercially available facial recognition algorithms as part of its 'Facial Recognition Vendor Tests' (FRVT). They measure the accuracy of facial recognition software algorithms in 'one-to one' (image verification) and 'one-to-many' (database search) contexts. Its FRVTs have shown that the technology is far more accurate than it was a decade ago,

[16] Joy Buolamwini, Timnit Gebru *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018).

[17] Michele Merler, Nalini Ratha, Rogerio S. Feris, John R. Smith *Diversity in Faces* (arXiv:1901.10436, April 2019).

[18] Patrick Gother, Megan Ngan, Kayee Hanaoka *Face Recognition Vendor Test Part 3: Demographic Effects* (NISTIR 8280, December 2019), and Paul Marks "Can the Biases in Facial Recognition Be Fixed; Also, Should They?" *Communications of the ACM* (64(3) p20-22, March 2021).

[19] Kate Kaye "This little-known facial-recognition accuracy test has big influence" *International Association of Privacy Professionals* (online, 7 January 2019).

[20] Kashmir Hill "Wrongfully Accused by an Algorithm" *The New York Times* (online ed, New York, 24 June 2020).

[21] M L Elrick "Detroit protesters take fight against facial recognition tech to city leaders' homes" *Detroit Free Press* (online ed, United States, 15 June 2020).

[22] Aristos Geogiou "Black Lives Matter Activist Hunted by NYPD Facial Recognition Technology" *Newsweek* (online ed, United States, 15 August 2020).

[23] James Vincent "FBI used facial recognition to identify a Capitol rioter from his girlfriend's Instagram posts" *The Verge* (online ed, 21 April 2021).

and these gains have been attributed to the confluence of growing computational power, increases in image data volume, and improvements in machine learning algorithms.[24] FRT is only likely to improve in future. However, recognition error rates remain significantly above zero, particularly where photography of faces is difficult or when confidence thresholds are adjusted to reduce false positives.[25] The performance of FRT systems and algorithms vary depending on the task they are performing, and how 'success' is defined.[26] An FRT system may be set at a particularly high sensitivity level to maximise the number of identifications (with full awareness that this will also increase the number of false positive matches). Conversely, a low sensitivity level might be used, so that matches are only returned by the system where there is a particularly strong match between the scanned image and a watchlist image.

The performance of FRT systems can vary relative to the gender, ethnicity and age of the individuals targeted.[27] NIST's FRVT Part 3 report focused specifically on demographic effects on the performance of 189 commercially available facial recognition algorithms. It found that many of the algorithms varied in performance across different demographic groups, and that the part of the world in which the algorithm was developed could have a significant impact on its performance.[28] For example, algorithms developed in the United States tend to have the high false positive rates for West and East African and East Asian people in one-to-one matching, whereas for a number of algorithms developed in China this effect is reversed, with low false positive rates on East Asian faces.[29]

For 'one-to-many' matching, the tests found that African-American females were subject to high rates of false positives. This is significant because a false positive match on a 'one-to-many' search could put an individual at risk of being subject to scrutiny by authorities as a result of an incorrect match against a database. FRVT Part 3 noted that some algorithms performed much better than others in mitigating demographic effects. Thus, in order to assess and manage the risk of adverse demographic effects, it is important to understand the performance of the algorithm being used, and the particular task it is performing.

In the specific context of Aotearoa New Zealand, the implementation of algorithms trained on overseas data sets of faces raises concern about lack of accuracy for the population, particularly for Māori. For example, a study has found that facial tattoos may disrupt face recognition.[30] One commentator

[24] Patrick Grother, Mei Ngan and Kayee Hanaoka *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* (NISTIR 8238, November 2018).
[25] "FRVT Quality Assessment" NIST <pages.nist.gov/frvt/html/frvt-quality.html>.
[26] See footnote 24.
[27] See footnote 16 and Joy Buolamwini "Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces" (25 January 2019) Medium <www.medium.com>.
[28] See footnote 11.
[29] See footnote 11 at 2.
[30] Heather Buttle and Julie East "Traditional facial tattoos disrupt face recognition processes" (2010) 39 Perception 1672.

cautions that "my concern is we're going to see an increase in false arrests with Māori ... I'm also concerned the system wouldn't have been trained on tā moko, moko kauae so we have no idea how the system will react to that."[31]

A literature search found no studies on the accuracy of facial recognition systems on Māori and Pasifika faces. This has likely been limited by the lack of datasets collected in a New Zealand or Pacific Islands context. The Privacy Impact Assessment for the One Time Identity (OTI) service run by the Department of Internal Affairs (DIA) mentions testing of "mid-tone faces" or "medium skin tone users" in 2019, noting a higher false negative rate[32]. Given the challenges that FRT has faced with "darker skin tones" globally, it is logical that these systems may produce more errors for Māori and Pasifika faces too. It may be helpful for academic research to be conducted in the New Zealand context to gather more data and understanding around these issues. If a decision is made to test or improve the performance of Police systems specifically on ethnicity – it would be important to have clear communication to the public on this and involve the necessary expertise (for example Māori data sovereignty experts) to ensure that the research is conducted in a culturally safe manner.

Assessments of FRT accuracy are heavily context dependent and challenging. It should be noted that accuracy claims can vary significantly on the context in which images have been captured. For example, accuracy rates tend to be higher where the individual is facing the camera front-on with consistent lighting conditions, in comparison to scenarios where cameras are pointing down towards individuals with variable lighting. The presence of glasses, face masks, and hats can also have an impact on the accuracy of FRT, although there is ongoing research to mitigate these effects and various vendor claims. Some people also have changing skin tones over time (e.g. lighter in winter, darker in summer) which could influence the accuracy of FRT systems.

They require consideration of the interplay between technical particulars (software accuracy; image resolution; sensitivity thresholds) and the task for which FRT is being deployed (e.g. one-to-one person verification, or one-to-many identification); and the contextual particulars of the deployment (e.g. the scale of a deployment; the location in which it is being used). Thus, when considering whether it is appropriate to use FRT, and the kind of management and decision-making procedures that should be in place prior to deployment, a case by case assessment is required.

Even where concerns about the accuracy of a system can be sufficiently mitigated, a broader assessment of its efficacy in a particular context may be needed. For example, when assessing the utility of FRT, consideration of the

[31] Karaitiana Taiuru quoted in Meriana Johnsen "Police facial recognition discrimination against Māori a matter of time – expert" *RNZ* (online ed, New Zealand, 2 September 2020).
[32] Department of Internal Affairs, "Privacy Impact Assessment: Full Report | One Time Identity" (15 August 2020), released under OIA on FYI.co.nz < https://fyi.org.nz/request/13970/response/54477/attach/5/Appendix%20A%20for%20release.pdf>

risk that a FRT system can be 'spoofed'[33] or avoided through the use of masks, baseball caps or other face coverings may be needed.[34]

There is also growing concern around the development of deepfakes and the increasing realism of generated images. These are typically generated "adversarially", with a system that produces facial images (A) connected to a system that detects and verifies faces (B) in a feedback loop, so that the system A learns how to fool the system B. As the technology becomes more widespread, there is the potential for FRT systems to suffer accuracy challenges when dealing with images that have been produced by deepfake systems, as deepfakes are, by design, difficult to detect automatically. A report by UCL ranked deepfakes as the "most serious AI crime threat."[35]

Any policy for facial recognition at the current point-in-time must consider these accuracy issues that lead to bias. However, policies should also be prepared for a future where that technology improves. Assuming that existing bias challenges can be technically ameliorated, the negative consequences of FRT may shift from bias and inequity towards oversurveillance. Improving FRT will also widen the gap between human and computer identification, as it should be noted that average humans perform very poorly relative to FRT, with forensic examiners and 'super-recognisers' achieving a draw against FRT[36].

3.6. Use of FRT in Public and Private Sectors in New Zealand

Here, we briefly outline current uses of FRT in New Zealand – this is important to show how embedded various usages are and the level of public acceptance/social licence of different types of usage. A fuller consideration of the various use cases is contained in the Lynch et al report.

3.6.1. Public Sector

FRT is used and is likely to be used more extensively, in identity verification services across a range of government services, particularly at border control. Most of this usage naturally falls into the 'verification' category – involving the comparison of one biometric template with another, though there may be 'identification' (one to many) usage also, particularly in the fraud detection procedure around passports. Biometric information such as facial images may

[33] This is where an FRT system is tricked by the use of an image of a face. For example, an individual could use the image of the face of a smartphone owner to trick the FRT software on the phone into unlocking the device. See Aleksandr Parkin and Oleg Grinchuk *Recognizing Multi-Modal Face Spoofing with Face Recognition Networks* (CVPR Workshop Paper, 2019). This challenge is further exacerbated with the development of deepfakes that are designed to fool FRT systems.

[34] An independent report into South Wales Police's use of FRT found that when targeted individuals wore baseball caps and other face coverings, this significantly affected the performance of the system deployed by the force, which was operating a one-to-many algorithm to identify individuals on a watchlist as they traversed public spaces. See Bethan Davies, Martin Innes and Andrew Dawson *An Evaluation of South Wales Police's Use of Automated Facial Recognition* (CUPSI, September 2018).

[35] M. Caldwell et al. *AI-enabled future crime* (*Crime Science* 9(1), 2020).

[36] P. Jonathon Phillips et al. *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms* (PNAS 115(24) 6171-6176, June 2018).

be used in decision-making.[37] Fraud prevention through detection of identity fraud is the principal reason why FRT is used.

DIA signed a ten-year agreement in 2018 which many public and private organisations will be able to join.[38] The deal was signed with Enterprise Services New Zealand, the New Zealand subsidiary of DXC Technology, a United States company. The system is now operational, with the aim of preventing fraud. The FRT system compares passport photos with a database to identify those with multiple identities. DXC uses software from the Japanese firm NEC.[39]

Many public agencies will have automatic access to the product and others can ask to join. Local councils can opt in and any private organisation can seek approval to join from DIA and MBIE. Other agencies must pay DXC for the service, but DXC provides the system and upgrades it. This saves these companies the cost of securing similar services and avoids the visibility of running a public tender. The intent to expand the use of biometrics among Crown agencies is apparent.[40]

3.6.2. Private Sector

Banking - Most or all New Zealand banks report using FRT technology in identity verification procedures. ASB bank has previously announced a pilot scheme for using FRT as a means of identifying customers,[41] and Westpac has implemented image matching for setting up an account.[42] Heartland Bank uses FRT to maintain compliance with anti-money laundering laws,[43] and the company OriginID is marketing a FR tool to accountants and lawyers for anti-money laundering compliance.[44] Paymark is considering the use of FRT as a means to create a seamless experience for customers when paying for products.[45] "By implementing face recognition as the key step in multi-factor authentication, banks are able to mitigate their exposure to risk and fraud, saving themselves millions of dollars in the process."[46] BNZ uses FRT to allow customers to log into their mobile banking application.[47]

[37] Immigration Act 2009, s 30.

[38] Phil Pennington "Government facial recognition tech deal offers wide access" *RNZ* (online ed, New Zealand, 12 October 2020); and Chief Executive of the Department of Internal Affairs and Enterprise Services New Zealand *Master Syndicated Agreement: relating to the syndicated procurement of Facial Recognition Services* (14 December 2018), released under the Official Information Act, copies on file with the authors.

[39] Note that the authors are meeting with DIA to clarify some details around this agreement.

[40] See footnote 38.

[41] Holly Ryan "Pilot selfie ID scheme for ASB customers" *Wanganui Chronicle* (Wanganui, 24 Apr 2018).

[42] Westpac "Westpac EasyID" <westpac.co.nz>.

[43] Heartland Bank "Biometrics" <heartland.co.nz>.

[44] OriginID "APLY ID: A SaaS solution for AML compliance" <originid.co.nz/aplyid>.

[45] Anuja Nadkarni "Paymark experimenting with facial recognition at Spark's 5G innovation hub" *Stuff* (online ed, New Zealand, 2 April 2019).

[46] Harmon Leon "How AI and Facial Recognition Are Impacting the Future of Banking" *Observer* (online ed, United States, 11 December 2019).

[47] BNZ "Help & Support - Mobile Touch ID, Fingerprint Login and Face ID" <bnz.co.nz>.

Retail security - Businesses are also employing FRT for security purposes. In May 2018 a man was taken aside by staff at a New World supermarket in Dunedin after he was mistakenly identified as a shoplifter.[48] The parent company Foodstuff refused to identify which of its stores were using FRT to identify shoplifters from existing held lists of suspect individuals. Both the Prime Minister and Privacy Commissioner noted concerns around the inaccuracy of the technology based on overseas research, highlighting the need for regulation.[49] Members of the public expressed a range of views.[50]

It has been reported that the Warehouse and Mitre 10 trialling FRT for security purposes in January 2020.[51] During the August 2020, Covid-19 Alert Level 3 in the Auckland region, a New World store in Auckland was criticised for asking customers to remove their facemasks briefly when entering the store in order for the FRT to be able to scan their face properly.[52]

Casinos were one of the earliest adopters and most widespread users of FRT. They can use FRT for security purposes, identifying cheaters or advantage players when they arrive on the premises and alerting casino staff.[53] Further, FRT can help casinos to meet their obligations to minimise harm from gambling by identifying people who have opted to be placed on self-exclusion lists or individuals who are underage.[54]

Pandemic related use: FRT is being adopted globally to help prevent the spread of Covid-19.[55] During this pandemic, the public may be more accepting of the risks of FRT in exchange for the health and public safety benefits. FRT is particularly appealing during this time because it provides a non-contact way of collecting biometric data, unlike fingerprints or iris scans. [56] FRT companies are customizing their products to specifically deal with the Covid-19 pandemic. In Australia two states are trialling FRT applications to manage people in home quarantine.[57]

[48] George Block "Supermarket chain Foodstuffs admits facial recognition technology used in some stores" *New Zealand Herald* (online ed, New Zealand, 14 May 2018).

[49] Madison Reidy "PM slams in-store face-scanning tech" *Dominion Post* (Wellington, 16 May 2018).

[50] See Matthew Rilkoff "Editorial: Recognition is reasonable on the face of it" *Stuff* (online ed, New Zealand, 21 May 2018).

[51] George Block "The quiet creep of facial recognition systems into New Zealand life" *Stuff* (online ed, New Zealand, 1 January 2020).

[52] Chris Marriner "Covid 19 coronavirus: New World store with facial recognition cameras reverses mask policy" *New Zealand Herald* (online ed, New Zealand, 14 August 2020).

[53] Sam Kljajic "Ask the Expert: Casinos, Face Recognition, and COVID-19" (15 April 2020) SAFR <www.safr.com>.

[54] George Block "The quiet creep of facial recognition systems into New Zealand life" *Stuff* (online ed, New Zealand, 1 January 2020).

[55] Lindsey O'Donnell "Covid-19 Spurs Facial Recognition Tracking, Privacy Fears" *Threatpost* (online ed, United States, 20 March 2020).

[56] Meredith van Natta, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam and Niharika Vattikonda "The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic" (2020) 7 J Law Biosci 1.

[57] Byron Kaye, "Australia's two largest states trial facial recognition software to police pandemic rules"https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/

Airline security - For example, existing FRT that was planned to be used in airports to provide a touchless experience is likely to be implemented sooner. This is because the touchless technology is thought to help prevent the spread of Covid-19.[58] While some airlines have already started rolling out the technology, interest is increasing from other airlines and airports due to the pandemic.

3.7. Introduction to FRT - Key Points

- Facial recognition technology (FRT) is a term used to describe a range of technologies involving processing of a person's facial image. Live automated FRT is just one aspect.
- FRT's main usages are verification, identification and categorisation & counting.
- A facial image is a biometric. Although it may be collected from a distance, without the person's knowledge, and in public, it involves an intrusion on the individual's privacy.
- FRT may augment and speed up existing human capabilities (finding a person in CCTV footage) or create new capabilities (detecting emotional states of people in crowds).
- The use of FRT is increasing in the public and private sectors in Aotearoa New Zealand.
- Accuracy and bias are key concerns. There are no studies specifically on the accuracy rates of the population of Aotearoa New Zealand.

[58] Jackie Snow "Nano needles. Facial recognition. Air travel adapts to make travel safer" *National Geographic* (online ed, United States, 13 August 2020).

PART 4. COLLECTION AND RETENTION OF FACIAL IMAGES

Examining collection and retention of facial images by Police[59] was not a direct purpose of our work, and we note there is a joint Independent Police Conduct Authority/Privacy Commissioner enquiry ongoing on the issue of Police photography in public spaces and related issues. We are not involved in that enquiry and have not had advance access to their findings.[60]

While we did not carry out a full review of Police's collection, retention and storage of facial images, we consider that any examination of the use of FRT now and in the future depends on the appropriate parameters of Police's collection and retention of facial images – as these images are a necessary part of the operation of FRT systems and tools. Thus, it is appropriate to make some comment and recommendations.

Anecdotally, some members of the public believe that where Police collect a facial image, it is then aggregated in one database and this may give rise to concern around the scope of current or potential FRT use.

We found that Police collect and retain facial images in a wide variety of contexts and for a range of purposes.

The ABIS2 upgrade to the Image Management System (IMS) may include:[61]

- Offenders – 1.85 million from 800,000 individuals' current records. There will be an estimated 50,000 additional records per annum.
- Suspect – it is projected there will be an additional 7,500 records per annum.
- Firearms licence holders – 245,000 records at any one time, with 10,000 renewals and 9,500 new records estimated per annum.
- Child sex offender register - 1,500 current records, with an estimated 2,300 additional records per annum.
- Facial recognition, search, compare, match and report – an estimated 15,000 additional records per annum.
- Photo line-up production – 12,000 current records (20-60 minutes to prepare standard line-ups). There will be an estimated 15,000 additional records per annum (10 minutes to prepare standard line-ups).

[59] 'Police' in this report is taken to mean New Zealand Police.

[60] Joint Inquiry by the Independent Police Conduct Authority (IPCA) and the Office of the Privacy Commissioner (OPC) into New Zealand Police's conduct, practice, policies and procedures as they relate to the photographing of members of the New Zealand public who are not being detained for or suspected of committing an offence, including whether Police action, policy or procedure has resulted in the privacy of individuals being infringed. The Inquiry will incorporate the investigation of reported incidents of Police photographing Māori youth in Wairarapa in August 2020 who had not committed or been suspected of committing an offence and who had not provided informed consent. https://www.ipca.govt.nz/Site/publications-and-media/2021-media-releases/2021-mar-09-joint-enquiry-police-photographing-public.aspx

[61] This report was originally based on the *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* dated October 2020. We have since been informed of further updates and developments, which are reflected in this report. We expect the PIA to be updated soon.

- Scars, marks, and tattoos (SMT) – capture, search, match and report – 2,500 current records, with an estimated 30,000 additional records per annum.

The IMS system is managed and operated by the National Biometric Information Office (NBIO). The system is being designed in a way that parallels the fingerprint database, including similar legal protections. We will now discuss each of the principal contexts of facial image collection and retention.

4.1. Formal Images

The *Policing Act 2008* empowers Police to collect particulars (including facial images in the form of photographs) from suspects in lawful custody. The legislation requires that these are destroyed as soon as practicable after:

- A decision not to charge,
- Acquittal.

The images may be retained after the following events:[62]

- Diversion,
- Conviction,
- Section 283 orders in the Youth Court (for children/young people),
- Discharge under s. 106 of the Sentencing Act.

These images are currently being held in a legacy system while the new ABIS upgrade to the IMS system is implemented.

4.2. Firearms Licence Images

Firearms licence holder images comprise around 250,000 images, which is a significant portion of the New Zealand population.[63] These are likely to be high quality images, particularly with most images now being collected in a digital format.

Lynch et al's report in late 2020 was critical of the proposal to have this database searchable through facial comparison because the images had been collected for a regulatory purpose. It is only one step away from then ingesting driver's licence photos as well, which would capture the vast majority of the population.

We note that the application and renewal form for firearms licences (January 2021 edition) has been updated to include a privacy notice which says that the image may be used for other law enforcement purposes.[64]

[62] Policing Act, s 34A.
[63] National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020) at 4.
[64] Firearms licence application form available at https://www.police.govt.nz/advice-services/firearms-and-safety/licences-permits-and-endorsements/apply-new-zealand-firearms

4.3. Other Images

We heard that Police collect facial images in a range of 'non-formal' settings held outside of the IMS and the NBIO's control. Our view was that some or most of this material would be from the public sphere (physical or online) and the individual may not be aware that their image has been collected. There is increasing use of the OnDuty application for frontline officers to report on situations in the field, which then feeds data into the National Intelligence Application (NIA). However, because there is a limit on the number of images that can be submitted via OnDuty, we heard that officers sometimes e-mail themselves the photos so that they can attach it into the NIA when at a desktop computer later. The NIA can contain formal and non-formal images taken from the physical or online public spheres. Police may also produce reports on events (e.g. from surveillance of an organised crime group meeting) which packages photographs, CCTV, etc. together in case it might be useful in the future.

In addition to images that are attached to individual files in the NIA, are informal images that Police may hold on their devices. These are essentially unmanaged by Police centrally as they do not have access to the Camera Roll on the Police-issued smartphones. However, locally held phone images cannot be searched using any Police approved software applications.

4.4. Evidential Images/Footage

We heard that Police collect family harm videos, statements, surveillance images and footage which are to be used as evidence. Video interviews (e.g. from a family harm incident) are taken on a mobile device and stored on Axon Citizen.[65] Photographs taken by front-line staff are attached to an incident report in NIA. Axon Citizen is also used to store footage taken after deployment of Tasers.[66] It is important that images from these sources, particularly where they include victims of family harm, are not subject to FRT.

4.5. CCTV Partnerships/Other Third-Party Systems

Police claim to not own any CCTV cameras operating in public spaces,[67] but through connections to private providers they have access to many live camera feeds. Providers include Auror, Auckland Transport, and SaferCities. None of these systems currently use FR, but the underlying camera owners may do on their own systems. The systems have varying capabilities (for example, SaferCities does not provide historical footage, while Auckland Transport cameras can be remotely controlled and moved by Police). As the cameras are owned by others, they retain control over the cameras and what is ultimately available to Police.

[65] New Zealand Police: Technology Capabilities List July 2021, p. 17
[66] See footnote 65.
[67] Note that Police own security CCTV in their own premises such as police stations.

Police may also be supplied with images and footage from the public directly, from business CCTV systems, or receive offers to use or receive FRT comparison results from private sector systems. We heard mixed responses about whether or not Police should accept footage and match results when offered. However, we were also informed that a FR match request submitted to the NBIO will only be accepted from a crime scene via the normal suspect process.

4.6. Access to Government Agency Databases of Facial Images

The Privacy Act 2020 has a number of mechanisms to allow agencies to exchange information. Police have identity information sharing agreements with several agencies including DIA in its capacity as the administrator of the Citizenship and Passports Acts). This set of agreements are wider than the issue of FRT and collection of facial images.[68]

This agreement is confined to several specific circumstances, allowing verification of an identity:

- of a person in lawful custody who has been detained for committing an offence whose identifying particulars (which includes facial images) have been taken,[69] or
- of someone whose particulars have been taken to send a summons, where the constable has good cause to suspect and intends to bring proceedings,[70] or
- of a returning offender[71] whose particulars have been taken.

This appears to have been introduced in response to the Philip Smith case, where an offender managed to obtain a passport and flee the jurisdiction without triggering any alerts.[72]

Police's own press release states the broad purposes of the system:[73]

> The system allows Police 24/7 access to passport and birth information, making it easier to identify a person police are taking enforcement action against. This is particularly valuable when police have arrested a person or suspect that a person has breached a court order. "This electronic access to passport and birth information improves Police's ability to better manage the identities of people entering the criminal justice system," says National Manager Criminal Investigations Tim Anderson.

[68] For context see Treasury *Impact Summary: Improvements to the accuracy and timeliness of Police information regarding name changes, deaths and non-disclosure directions* (April 2019).
[69] Policing Act 2008, s 32.
[70] Policing Act 2008, s 33.
[71] Returning Offenders (Management and Information) Act 2015.
[72] Which initiated policy changes that were further enacted in Enhancing Identity Verification and Border Processes Legislation Act 2017.
[73] New Zealand Police "Improvements to information sharing between DIA, the Registrar-General, Births, Deaths and Marriage and Police" (press release, 3 May 2019).

> The improvements build on recent automated access for Police to driver licence images held by the NZ Transport Agency, as well as immigration data and photos from Immigration New Zealand (INZ). Police can send a subset of data back to INZ under certain conditions.

The mandatory reporting of the use of this agreement in the Police Annual Report suggests that this identity verification method was used over 250,000 times in the last 12 months reporting period.[74] The annual report show the number of queries made from Police to Immigration New Zealand: The Police on-duty mobile application was used to make 112,380 queries to the INZ system, including for suspects/offenders identity 82,078 times. 252,228 queries were made in total from the Police NIA desktop application.

While it is not possible for us to gain further information on the nature of these queries[75] and not all will involve transfers of biometric information such as facial images, it does suggest that the use of the interface has become a regular part of policing.

A similar situation exists in relation to the driving licence database. This is administered by the Transport Agency. Its privacy policy states that:

> The photo captured for your driver licence under Part 3 of the Land Transport (Driver Licensing) Rule 1999 may also be used by the Department of Internal Affairs, Department of Corrections, Ministry of Justice, Ministry of Business, Innovation and Employment (Immigration), New Zealand Customs Service, and the New Zealand Police for the purposes of identity verification and law enforcement under section 200 of the Land Transport Act, or for one of the purposes outlined in Part 10A of the Privacy Act. Your photo may therefore be disclosed to one of these agencies, for one of these purposes.

It is worth noting that both the identity information exchange (Part 10A of the former Privacy Act 1993, Part 7 subpart 2 Privacy Act 2020 and law enforcement information exchange (Part 11 of the former Privacy Act 1993 and Schedule 5, Part 7 subpart 3 Privacy Act 2020 and Schedule 4) are, unlike other sharing mechanisms, not under the statutory oversight of the Privacy Commissioner.

4.7. Horizon Scan of Possible Developments in Biometrics Regulation

At present, the regulations regarding the collection, retention, comparison and matching of facial images by Police are very complex, sitting across numerous pieces of legislation, regulation and policy. Additionally, the common law position on photography and recording in public spaces does not countenance the technological capabilities currently available.

[74] New Zealand Police *Annual Report 2019/20* (December 2020) at 145.

[75] We sought information under the Official Information Act but the queries had not been answered in time for the publication of this report. MBIE sought an extension of time, and Police did not respond within the timeframe.

We consider that it is likely that the Government will consider some form of legislation, governance, oversight or other regulation of the collection and retention of biometrics. As we discuss in the recommendations section, it would be advisable for Police to consider and review the collection and retention of facial images in contemplation of likely regulation.

There are several relevant ongoing developments in this sphere which Police should be cognisant of:

- The Law Commission's review of search and surveillance noted that "a consistent approach to all biometric information may be considered desirable" but recognised that DNA contains much more personal information than other forms of biometrics.[76]
- The Privacy Commissioner is consulting on a position paper on biometrics which is expected to be released publicly later in 2021.
- In the Facial Recognition Technology project final report published in late 2020, Lynch et al recommended that the Police establish an oversight mechanism with independent representation to ensure that image databases (and any potential FRT or other matching proposals) are ethical and sound, including independent representation and Māori representation.[77]
- The recently released Law Commission Final Report on DNA states:[78]

> We note the rapid pace of technological developments in relation to other biometric information, such as facial recognition software, remote iris recognition and other behavioural biometrics (for example, voice pattern analysis). We are also aware of concerns in relation to existing and emerging forensic science techniques other than DNA analysis. Many of these are largely unregulated in Aotearoa New Zealand. In light of such developments, and concerns that have arisen in other jurisdictions, we recommend that the Government considers the adequacy of existing oversight arrangements in the fields of biometrics and forensic science.

As an example of such a regulator in a comparable jurisdiction, the Scottish government has established the office of 'Scottish Biometrics Commissioner' and established a Code of Practice for the use of biometrics by the Police. This includes regulation of facial images.

The Scottish legislative scheme defines biometric data as "…information about an individual's physical, biological, physiological or behavioural characteristics which is capable of being used, on its own or in

[76]Law Commission *Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012* (NZLC R141, 2017), at para 2.38

[77] Recommendation 11.

[78] Law Commission *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara – Final Report (2020), recommendation 45.*

combination with other information (whether or not biometric data), to establish the identity of an individual."[79]

This Commissioner:

- keeps under review the law, policy and practice of collection, retention, use and destruction of biometric data by the Police,
- promotes public awareness and understanding of the powers and duties related to the acquisition, retention, use and destruction of biometric data, how those powers and duties are exercised, and how the exercise of those powers and duties can be monitored or challenged,
- promotes and monitors the impact of the Code of Practice for biometrics.

- We also note that the Department of Internal Affairs has re-convened the cross-government biometrics group and that will result in review and update of the guidance for collection of biometrics across government in the next 12-18 months.[80]
- The Department of Internal Affairs is also carrying out some policy work on facial recognition technology across the public sector. The potential outcomes and timeframes of this work are unknown.
- Additionally, future regulation will need to consider the role of deepfakes, which have been applied most commonly to facial images, but could be applied to other forms of biometric data as well.

4.8. Collection and Retention of Facial Images - Key Points

- Police collect and retain facial images in a wide variety of contexts, under different legislative requirements and for a range of purposes.
- A full review of Police's collection, retentionstorage, and use of facial images was not part of our terms of reference, but we could make some comments relating to how these images could form part of the source database or 'watchlists' for future expanded use of FRT
- Our conclusion is that facial images collected by Police appear to be held in separate systems or 'buckets', and the images were of vastly varying age and quality.
- There is no or little current capability for combining image databases for wider facial comparison and recognition mechanisms, but this is a risk to be managed.

[79] Scottish Biometrics Commissioner Act 2020, s 23(1) and (2).
[80] Cross Government Biometrics Group *Guiding Principles for the Use of Biometric Technologies for Government Agencies* (Department of Internal Affairs, April 2009).

PART 5. USES AND POTENTIAL USES OF FRT BY POLICE

We will now discuss the various categories of use-cases that we have identified. Under each category, we discuss past, current and potential future uses by Police.

The discussion of past and current use is drawn from documentation and interviews. Potential use is drawn from comments made during interviews and our analysis of the literature. For any discussion of potential use, there is no inference that Police are planning or considering these uses, it is simply a horizon scan of what might be possible.

Under each category we make an initial assessment of the issues which each capability may raise. These inform our analysis in the other Parts of this report.

5.1. Relevant Capabilities

A previous section identifies the many and varied use-cases for FRT.

The principal uses of FRT which are in current use or of potential interest in a policing context are:

- Verification of identity for security access/log-ins/visitor access,
- Identity matching/facial comparison of facial image to a database to verify a person's identity, or to identify an image of an unidentified person,
- Retrospective analysis of lawfully acquired footage/stills/data to identify instances where a person appears,
- Data scraping tools using publicly available facial images (i.e. non-Police data) - used to identify people in images and present images of the same person collected from other contexts,
- Live automated facial recognition technology/live biometric tracking – using real-time footage to identify whether a person from a pre-selected 'watchlist' is present,
- Counting and categorisation of people – using a system which counts facial images or categorises people's emotional states.

Much of the discussion and literature on the use of FRT in policing both globally and in New Zealand, has focussed on use of particular proprietary software or systems. In this report we have chosen to focus principally on capabilities (that is, what a system could do), though we do refer to the current Technology Capabilities List for examples of current use.

5.2. FRT in Security and Access

Like many large organisations, it is likely that Police will consider the use of FRT for security and access. We think this is very unlikely to be of concern to the public and has minimal impact as it is internal-facing, but it is important in demonstrating the many and varied uses of the technology (and by implication the consequences of calling for a complete ban on Police usage of FRT).

5.2.1. Current Usage

Police are currently issued iPhone X smartphones as standard equipment, and some staff may choose to use Face ID, a facial recognition function to unlock their phones. This is optional, and Police do not hold the reference images for identity verification.

5.2.2. Potential Usage

We heard that in the future there could be consideration of FRT for staff access to buildings and computer systems. It could also be used to automatically check visitors in and notify staff that the visitor is there to see them. This could make signing-in more efficient for frequent visitors (e.g. contractors, stakeholders, family members).

5.2.3. *Initial Assessment*

It is unlikely that internal use of FRT for Police staff access and log-ins would pose any risk to the public's rights and interests and is very unlikely to be of concern.

If FRT was considered for use as a visitor-entry system for members of the public to Police premises, this may raise some issues relating to privacy and data security. This could be ameliorated through public signage, provision of alternative means of entry control (opt-out) and transparency about storage and deletion of the facial images.

5.3. Identity Verification via FRT

5.3.1. Current Use

Identity matching/facial comparison involves the loading of a facial image to a database to verify a person's identity (one-to-one) or identify an unidentified person (one-to-many). This is also referred to as facial matching or facial comparison, but is premised on facial recognition technology. FR is not currently used for these tasks, although there was an older system that was trialled. Manual versions of this task include verifying a person's identity against their driver's licence, matching a person against a watchlist on an internal communication channel (e.g. 'National Top 5 Offender'), and the use of police line-ups. A text-based search system has been available for scars, marks and tattoos (SMTs) for two years, where an officer enters a text search of an SMT and the system returns matching images based on their categorisation.

5.3.2. Planned Imminent Use

The Automated Biometric Identification System (ABIS) 2 Project aims to upgrade Police's existing image management system (IMS Photo Manager) with an FRT algorithm. This is being provided by DataWorks Plus, using the NEC FACE Plus software. The system was planned for deployment by September 2020, but this has been delayed as the standard operating processes are further developed and implementation issues are resolved. The system will also have the capability to search across scars, marks and tattoos (SMTs).

The tool will not be available to Police staff in general, only by formal request to the National Biometric Information Office (NBIO), where trained staff will operate and manage the system under defined business processes and system rules. Strict search criteria will limit the scope of data sources used, depending on the context (e.g. firearms license images will only be used if a firearm was involved in the incident under investigation). Business rules will be established to limit the number of results that can be returned from any search (e.g. top twenty matches) to prevent 'fishing' for data and to mitigate privacy impacts for immaterial people appearing in results, with some flexibility on the thresholds depending on the severity of the crime under investigation. NBIO are currently evaluating NIST guidelines, and Forensic Face Examiners will be required to complete a three-year training course which includes the Diploma in Forensic Identification (Biometrics) from the Canberra Institute of Technology, as well as keeping up to date with new developments in FRT. There will also be a very limited number of examiners (only five at this stage). A Privacy Impact Assessment and security certification/accreditation are ongoing considerations.

Use cases include identifying an arrested person to find records of their previous interactions with Police, identifying a suspect that may be giving a fake name or identification document, identifying a suspect from an image as part of an investigation that may lead to an arrest, identifying a witness seen in an image as part of an investigation, or identifying a victim of a crime where that person is unable to identify themselves. Interviewees noted that a match in IMS would only be used as one source of information in the context of a robust forensic model, and officers would still use other information sources to verify identity such as DNA or fingerprints. It will be treated as an Intelligence product, rather than a direct source of evidence for investigations. As searches are conducted through NBIO, results will not be provided instantaneously, which may discourage unnecessary or experimental use of the tool. The primary advantage for Police is that it provides a quality-assured system of identity matching.

We queried whether images collected through OnDuty (an intelligence filing app on Police phones) could be subject to IMS searches, and were informed that OnDuty data is filed against a person's file in the NIA but is not connected to IMS, and therefore would not be subject to FRT. Police should be aware that merging image databases together in the future could expose more images to the FRT capabilities in IMS. This should also be considered if image search functionality is extended to other people (e.g. frontline officers who may want to run their own queries). It was noted that a large proportion of Police interactions with individuals is roadside, and that remote identification of individuals may be helpful in that context, although technical issues such as inconsistent lighting should be considered.

5.3.3. Potential Usage

As discussed, Police collect and retain facial images from a large range of sources. We heard varying views on whether it would be appropriate to implement a more expansive facial comparison in the future and what type of images it would be appropriate to include. Image sources that could be incorporated in the future include images currently in other Police systems (e.g. NIA), images held by other Agencies (e.g. driver's licence images, passport images), and images collected from open source intelligence (OSINT, e.g. social media). There is some ambiguity about what can or cannot be done with informal images taken by individual officers – for example, photos in the Camera Roll on the phone that have not been otherwise uploaded to a Police system are not currently monitored by Police and are not subject to any controls or audit log. Police are aware that greater clarity is need in respect of this issue.

The appropriateness of adding any of these image sources needs to be considered carefully. For the avoidance of doubt, we are not suggesting that these sources are currently being used, or that there are active proposals to incorporate them.

5.3.4. Initial Assessment

We generally view the use of FRT-enabled identity matching or verification in a forensic or investigative setting, using a limited set of formally collected images, to be low risk where there are sufficient governance safeguards and business rules in place to a high standard. As noted in the Taylor Fry report on algorithms, having a human in the loop remains best practice, with the human responsible for any decisions made based on the information produced by FR, ensuring that the sufficiently trained human understands the limitations of the tool.[81] In many of these scenarios, FR is providing a "scale and speed" improvement on existing manual processes of searching image databases. Given the types of images that are used in IMS, we note that there may be accuracy challenges with older historical reference images in the database, as aging effects can lead to poor matching (depending on the sensitivity threshold of the algorithm).

If databases are merged, or facial comparison is made available across a wider range of databases collected for different purposes, then the risk level (for Police and for the public) may increase. This is further exacerbated if other government databases or third-party databases are incorporated as well. Extending access beyond NBIO (e.g. remotely to roadside officers) would also increase risk. Further business rules would need to be added to mitigate privacy and misuse risks.

[81] See footnote 2.

5.4. Retrospective Analysis using FRT

This category refers to FRT analysis of historical information (generally video footage) that has been collected by Police (i.e. not live video feeds). The most common application is to analyse CCTV footage to find a specific face belonging to a person of interest, but could also be used to identify potential suspects or witnesses. A manual version would be for human officers to watch the footage themselves, which is typically a labour-intensive and costly process. FR can reduce hundreds of hours of footage to selected clips of interest that Police can then review.

5.4.1. Current Usage

BriefCam – a system which analyses lawfully obtained video footage from static cameras - has been adopted by the High Tech Crime Group (HTCG), which is part of the National Criminal Investigation Group.[82] The primary purpose is to reduce Police time spent on locating and analysing evidential footage. Investigators request the input of video files by HTCG. BriefCam creates a synthetic view of objects to speed up review, and makes objects contained in the footage searchable (e.g. red cap, blue t-shirt, vehicle registration plate, etc.). Face matching capabilities are available in BriefCam. The evidence is then given to a human as part of their usual investigative processes. It is important to note that this is a tool to find a known person in footage rather than to identify an unknown individual against a large database like IMS.

Interviewees noted that investigators would usually only rely on FRT as a last resort and when there was limited other information to work on. They would generally try to corroborate FR matches with other evidence sources such as fingerprints before making any decisions. It was noted that while use is low now, it may increase over time as its efficacy is proven, and it is integrated into existing business processes.

The Technology Capabilities List (July 2021) reports that other FR tools have been used in specific contexts, such as Griffeye for face analysis in child abuse material, Nuix for searching unstructured data for faces, weapons, and SMTs, and Cellebrite to search for faces in images held on smartphones (although the FR component may not have been used by Police).

5.4.2. Potential Usage

Analysis of retrospective footage will grow as it provides significant efficiencies over manual processes, especially as processing power improves and costs decrease. It is possible that faces in that footage may be matched against larger Police databases (e.g. IMS rather than a limited watchlist for a specific investigation), which would have broader reaching privacy impacts.

[82] NZ Police Technology Capabilities List, July 2021, p.18.

Other sources of video footage could also be incorporated, such as body-worn cameras.

5.4.3. Initial Assessment

For information that has been lawfully collected through warrant or consent, where human officers still retain final decision-making powers, the risks associated with FR analysis of retroactive footage are medium-low. The risks here primarily relate to accuracy concerns that could lead to false negatives (face matches that are missed by the system). It is also important to ensure that there are sufficient processes in place to mitigate any false positives (the system making an incorrect match), such as having multiple people review the outputs of the FR system. Again, where people remain in control of the final decision, they should be well-trained on the limitations of the tool. The accuracy of systems used for this capability should be closely monitored, and users regularly asked for feedback about whether they trust the outputs of the system.

It could be argued that using these tools is privacy protecting, as automated video selection avoids human officers watching excess footage about people unrelated to a case and making incidental findings. It is also in the public interest to reduce staff costs on relatively unproductive tasks and to solve crimes faster to mitigate harm. On balance, it is likely appropriate to use FR tools for these applications with appropriate safeguards, noting accuracy and broader cultural considerations.

5.5. OSINT Data Sources

While somewhat adjacent to the use of FR technologies, it is important to consider where image data and video footage may be collected from. Open Source Intelligence (OSINT) refers to information collected from publicly available sources, which tends to be on the internet and commonly on social media platforms or news websites. These may also be referred to as ‘data scraping’ or ‘web scraping’ tools, although they are generally more targeted towards specific individuals than generic ‘web crawler’ tools. Images collected by OSINT tools could then form part of a database against which FR queries can be run.

5.5.1. Past Usage

A short, non-operational test of Clearview AI was carried out in early 2020. Advice was provided that if the software was to be considered for ongoing investigatory use then a formal legal review and Privacy Impact Assessment (PIA) would be necessary. Clearview draw their images from OSINT sources scraped from millions of websites, without consent from the individuals whose images are captured, or the websites hosting those images. Users could then upload images of people and Clearview would return matching images, along with other contextual information such as the source of the image and the identities of other people in the image. The tool was ultimately considered too inaccurate and ineffective for use in a New Zealand context, likely because Clearview's dataset did not have sufficient local data. OIA requests subsequently revealed the short test/trial, leading to Police establishing an emergent technology work program, including this report.

5.5.2. Current Usage

While Clearview was ultimately not operationalised by Police, the technology assessment was part of broader searches for technology that could help identify individuals in legally obtained video footage.

OSINT tools are reported in the technology stocktake, but the specific tools and the way that they are used are withheld for operational reasons.[83] However, there appears to be a distinction between formal collection run by the OSINT team that supports intelligence and investigations groups, and less formal OSINT that may be run by individual officers. As there is a lack of legislative guidance on the boundaries of how OSINT can be collected or used, Police have had to form their own policies. We heard that it is often used to obtain a warrant or production order, but less often used as evidence in court. We heard in interviews that here is no specific FRT system used on OSINT data at this point, although there could be some interest in the future.

5.5.3. Potential Usage

The main purpose of OSINT in a FR context is surfacing additional people who may be connected to an individual of interest. For example, Police may have a photo of a known drug dealer in discussion with two other people, and want to know who those others are. An OSINT database of images would provide significant capability to identify those people using FR. Another use would be to search for images that contain a person of interest in order to identify their frequent locations, supporting investigative work.

However, Police should also be aware of technology that is developing around synthetically generated hyper-realistic facial images, otherwise known as deepfakes. Particularly in scenarios where the image source is not in the control of Police (e.g. scraped from social media vs a formal image taken during processing), there is a growing risk of those images not being genuine, either because the face is fictional, or worse, because the face has been swapped out for someone else's. There is limited technology available to detect deepfakes today, and as deepfakes continue to improve in quality it will become increasingly difficult to automatically classify them as real or fake correctly.

5.5.4. Initial Assessment

The use of OSINT information in a FR context is high risk and very problematic. Individuals generally have not given consent for their images to be captured by Police, and building an OSINT database to allow for general purpose

[83] NZ Police Technology Capabilities List, July 2021, p. 16.

identification of individuals carries significant civil liberties risk. The far-reaching scope of OSINT, and the inherent repurposing of the images (i.e. individuals share the images for a purpose different to the one that Police use the images for) are of concern from a privacy perspective. It is a very different class of data to the formal images captured in IMS, and different again to other government databases like drivers licenses or passport images. Police should avoid using FR systems that rely on OSINT information. A wider review of the role of OSINT in policing is outside the scope of this report. As we foreshadowed earlier in this report, the issue of how and when police can use images collected in the public sphere (both the physical and online public spaces) is a complex one. While the common law and the Privacy Act 2020 do not preclude police collection and analysis of publicly available images, the law lags the development of large-scale analytical tools like FR. Police should monitor this developing area of law and policy closely.

5.6. Automated Live FRT

Automated live FRT, a form of live biometric tracking involves the application of software to a live video feed. The system compares a pre-selected watchlist of images to the video feed and alerts when the person's face is detected. The system can be used from a static camera network or through mobile cameras. Live monitoring of all possible CCTV camera feeds manually is not practically achievable, although Police do monitor camera feeds in real-time for specific events (e.g. major sporting events, parades, significant traffic incidents, etc.), primarily to inform resource deployment decisions.

5.6.1. Current Usage

We did not find any current usage of live FR technology within Police. Police do not currently own CCTV cameras for use in public spaces, and rely on access to camera feeds provided by 'community owners' such as Councils, religious groups, and private businesses. We interviewed entities that provide access to CCTV camera feeds to Police, and were satisfied that Police cannot currently use FR on those connections. It is important to note that individual camera owners may have systems with FR capability, but these are not extended through to Police. Further evaluation of those camera networks is outside the scope of this report.

5.6.2. Potential Usage

We heard that this type of technology could be useful in several different situations in policing, but the general view was that the risks outweighed the benefits and that there were concerns with accuracy and bias. Our conversations yielded little interest in imminent deployment of live FRT in public spaces.

Possible use-cases mentioned were:

- ❖ A limited system could be installed where there was a particular need at a particular time, for example, to alert Police where a person who had made threats against a property or people appeared at a premises (without the need to have a police officer stationed at all times),

- ❖ Locating suspects in high risk situations at short notice – for instance where a terror suspect or armed suspect was at large,
- ❖ Use at a public event to locate people of interest e.g. those who have warrants to arrest,
- ❖ Major events -a mobile camera van could be used to quickly identify risky people in a crowd,
- ❖ Could be used for less serious offences such as volume property crime which do still cause considerable harm in the community,
- ❖ Could save Police time by monitoring public spaces for prolific offenders.

As we discuss in more detail below, comparable jurisdictions have used live FR for all of these applications to varying degrees. Several trials have shown mixed results in terms of accuracy and effectiveness.

5.6.3. Initial Assessment

Live FRT is the most high-risk usage of this technology, which engages a range of ethical and legal considerations. It is a new capability that disproportionately shifts the balance of power between individuals and Police. The use of live FRT inherently requires all people captured by a camera to be subjected to FR regardless of their relevance to Police, in a less constrained setting than use of retrospective footage for a specific case or incident. There is also uncertainty as to whether subjecting a person to a live FR comparison constitutes a search in the context of the *Search and Surveillance Act 2012* (see Part 6 for further discussion).

Due to the time-sensitive nature of live FRT, it is also more likely that errors are more impactful, as alerts generated by FRT may require fast decisions (e.g. to deploy resources immediately to intercept a person) that cannot have the same level of scrutiny as offline processing. In this context, accuracy and bias challenges are a critical consideration. Multiple interviewees noted that Police likely did not have social licence or consent to use live FRT, with some indicating concern that backlash to live FRT could lead to a loss of social licence for Police use of CCTV feeds in general.

As we discuss below, we recommend that Police should continue to pause any consideration of live FRT until several conditions are met, including identifying a clear, lawful and appropriate purpose, engaging in community consultation to confirm social licence, and evaluating the technology until there are improved accuracy rates that demonstrate the systems are not biased or discriminatory against subsets of the population. If these conditions cannot be met, Police should consider ruling out the use of live FRT permanently. We also believe that any future use should be restricted to high-impact use cases and should not be used at the lower end of the spectrum.

While an offence-based threshold (allowing use of a technology for serious offences only) has a certain logical simplicity, there certainly difficulties in establishing purely offence-related thresholds for use of FRT. Offences of terrorism are frequently used as an example to justify live automated FRT and are considered serious offences. However, planning for a terrorist attack could engage purely lower-level offence thresholds such as offences against the Arms Act. The Search and Surveillance Act permits trespass surveillance and interception for offences punishable by 7 years or more or for a variety of offences against the Arms Act and Psychoactive Substances Act. Internal guidance around use of live automated FRT (if ever implemented) would need to be nuanced enough to capture relevant high-risk situations which may not directly be categorised according to an offence threshold model.[84]

5.7. Access to Third Party Systems

During our interviews, we identified that Police have access to several third-party systems, either as part of a network with continuous access, or through ad hoc access and data being provided by private owners in response to specific incidents. Some of those private sector systems have live FRT capabilities available, even if they are not being directly controlled or used by Police. As the proliferation of FRT increases, Police are increasingly likely to be offered results of matches from FRT systems, or offered the ability to provide watchlists for ongoing monitoring. This could be 'offline' (i.e. retrospective footage or data provided after the fact) or 'online' (i.e. live feeds with FR matching run over the images). There may also be overseas transfers of images to other jurisdictions, which may have access to tools that are not available to New Zealand Police.

It is arguable whether this is any different to the common scenario today of Police being offered recorded footage from CCTV cameras, or Police asking private individuals to keep an eye out for specific individuals. We hold the position that the use of FRT in these contexts goes beyond a speed and scale improvement because it enables the automated continuous monitoring of camera systems and automated matching of faces that could not be achieved without a dedicated human resource. It would enable new types of decisions to be made, such as deploying resources to intercept a person because an alert has been generated for a match by a third-party FR system.

Regardless, ultimately the decision-making outcomes and impacts are the same whether the FR system is owned by a third-party and used by Police, or the system being owned by Police themselves. It would be problematic if third-party cameras and processing systems were used as a loophole to do things that Police cannot do with their own systems. We therefore recommend that Police use the same policies and rules for handling data derived from third-party FR systems as they would do their own. For example, if Police decide to

[84] Note Richard Wilson's work towards his thesis which contains an example of an offence-based threshold model: Wilson, R.J. (2021). *Operational use framework for emergent technologies*. Wellington: New Zealand Police. This work could provide a useful model for development of operational guidelines.

place a moratorium on the use of live FR on their own systems, then that should extend that to live FR on third-party systems and Police should refuse offers from private entities.

5.8. Counting and Categorisation by Demographics or Emotions

In some scenarios, it would be useful to use computer vision or video analytics technologies to provide data about people in a camera view, without necessarily identifying them. While this is strictly speaking not FR, it uses similar methodologies and relies on similar input sources. Individuals can be counted, could be categorised by demographics, and could be analysed for emotional state. A manual version today would involve human officers watching a live feed to estimate the size of a crowd at a large event, but it is extremely difficult to get a more granular description of the individuals.

5.8.1. Past Usage

Police trialled a system for counting people in queues at police stations, logging when they visited and the length of time spent at a counter. [85] This was primarily to analyse demand trends and therefore inform capacity planning. The system is no longer in use.

5.8.2. Future Usage

While counting and tracking could be re-introduced to police stations, it is more likely that this technology could be adopted for monitoring large events. Current methods of estimating crowd sizes (manual counting, cell phone signals, infrared) have high rates of error and typically cannot be provided in real-time. Person detection technology could help count the number of people in certain areas and therefore inform resource allocation decisions (e.g. deploy more officers to areas where there are more people and there is more risk). This could be further augmented with demographic analysis to deploy certain types of officers to certain environments. Emotion recognition could be used to measure the 'mood of the crowd' and inform the timing and type of interventions that should be taken (e.g. de-escalation at a protest before a situation gets worse).

5.8.3. Initial Assessment

The appropriateness of using these adjacent technologies varies; on the one hand, simply counting people without collecting their biometrics is obviously less privacy-infringing than FR, while on the other hand, analysing the emotional state of individuals (also without collecting their biometrics) would likely still be perceived as an infringement on privacy rights, even if it were to be aggregated at a group or crowd level. If Police do not own the cameras themselves, then this would need to be conducted in discussion and with the permission of system owners. Police should be prepared for the development of these technologies, potentially separate to policy on FR specifically. We

[85] NZ Police Technology Capabilities List, July 2021, at p.52.

believe that social licence has not yet been established for these types of applications and that this should be evaluated carefully.

5.9. Combinations of Capabilities

Thus far, we have largely considered the potential capabilities and use cases independently. However, combining different capabilities together can increase the level of risk non-linearly. For example, using OSINT tools to collect facial images, and then using that database for retrospective FRT analysis of footage presents a much higher risk than conducting retrospective analysis with a limited watchlist. In another example, connecting a visitor FR sign-in system with a front counter queue monitoring system could enable identities to be attached to visitor trends and patterns. Police should be particularly aware when capabilities from different contexts or business groups are being combined, as new risks may appear in less predictable ways that also need to be identified and mitigated.

5.10. Uses and Potential Uses of FRT by Police - Key Points

- There are a range of current and potential future uses of FRT, and a blanket ban on FRT is likely to capture systems that are low risk.
- Current or imminent planned use of FRT is limited and relatively low risk including:
    - Authentication for access to devices such as iPhones,
    - Identity matching in the IMS system (which will soon be implemented),
    - Retrospective analysis of lawfully acquired footage in limited situations,
- A range of potential uses for FRT in policing are explored in this report, but there is no inference that Police are planning or considering these uses. We found no evidence that Police are using or formally planning the use of live automated FRT.
- Police should consider the spectrum of use and spectrum of impact when assessing the use of FRT and avoid high-risk use cases. Police did undertake a limited trial of a high-risk usage (Clearview) but are not currently trialling or considering other high-risk usages.
- There are challenges with the use of third-party camera networks and OSINT data sources that need to be carefully considered.

PART 6. CONSIDERATIONS IN A NEW ZEALAND CONTEXT

In this section we discuss the relevant considerations applying to use and potential use of FRT in policing Aotearoa New Zealand. These are drawn from a review of the literature and themes which arose from interviews.

We endorse the approach in Police's draft New Technologies Framework to consider the legal, ethical and other impacts of new technologies before commissioning and implementation. The analysis of considerations in this section should assist in any consideration of expansion or new uses cases for FRT applications specifically.

6.1. Purposes of Policing

There can be tendency in analyses of Police use of technology to focus entirely on constraints and impacts, but it is important to note the legislative requirements and common law duties which Police must carry out.

Section 9 of the Policing Act 2008 describes the functions of Police as:

- keeping the peace,
- maintaining public safety,
- law enforcement,
- crime prevention,
- community support and reassurance,
- national security,
- participation in policing activities outside New Zealand,
- emergency management.

Key Point – Police have a duty to consider, review and implement new technologies which would advance a function of the Police, in particular to prevent and detect crime, to improve public safety and reduce harm to communities.

6.2. Search and Surveillance

Our comments on this topic are mostly directed at the potential use of live automated FRT in a public place. This is not a question that has been directly considered by a New Zealand court, or indeed any comparable jurisdiction's court, but there is some relevant case-law on other forms of warrant-less surveillance.

It is open to Police to seek authorisation through warrant for a surveillance device with a FR capability. We did not hear of any instance where this has been done.

Pre- *Hamed v R*[86], the law was understood as being that video surveillance by the Police was not unlawful because it was not forbidden by statutory or common law.[87] This position was confirmed in *Ngan*, *Fraser* and *Gardiner*.[88] Thus, police officers are entitled to do anything that can be lawfully done by a citizen unless there is a common law or statutory prohibition. This view was confirmed by the majority in *Hamed.* This is also the general position in the *Search and Surveillance Act 2012* – surveillance in a public place where no trespass has occurred is lawful and does not require a warrant.[89] The Court of Appeal in *Lorigan* found that covert surveillance with a night vision equipped camera was lawful as there was "no statutory or common-law prohibition and it would not have been unlawful for a citizen to do the same thing".[90]

Elias CJ in *Hamed* took the dissenting view that video surveillance in that case was unlawful, whether there was a trespass or not.[91] Elias CJ would have held that public officials are different to private citizens and cannot do something unless they have lawful authority (whereas private citizens have the freedom to do anything that they are not prohibited from doing). In our opinion, this is the preferred interpretation, but this was a minority view in this case.

Would the use of a FR equipped camera by Police in a public place constitute a 'search' in terms of s. 21 of the New Zealand Bill of Rights Act? The English Court of Appeal in *Bridges* did not engage with this point in the context of English law, merely noting that a FR enabled camera was more intrusive than regular CCTV.[92]

Several New Zealand cases have discussed whether various forms of camera surveillance constitute a 'search'. In *Lorigan v R*,[93] the appellant argued that surveillance evidence gathered by the police in a drug offending case was inadmissible. The police had set up a video camera (with the permission of the landowner) and then subsequently a second camera with night-vision capabilities. The extent of the cameras' view was that which was in plain sight of any person who walked down the street.

[86] *Hamed v R* [2011] NZSC 101, [2012] NZLR 305.

[87] See also *R v Fraser* [1997] 2 NZLR 442 (CA) and *R v Gardiner* (1997) 15 CRNZ 13. For a discussion of the English law see J Purshouse "Facial Recognition Technology, the Metropolitan Police and the Law" (19 January 2020) Policing Law Blog <policing.law.blog>. The idea that police enjoy a residual liberty to do 'that which is not forbidden' no longer applies to covert surveillance activities that would engage an individual's privacy rights under Article 8 of the European Convention on Human Rights (see *Malone v The United Kingdom* [1984] ECHR 10), and since the enactment of the Human Rights Act 1998, police have tended to rely on positive common law powers to prevent crime for overt surveillance operations.

[88] *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48; *R v Fraser* [1997] 2 NZLR 443 (CA); and *R v Gardiner* (1997) 15 CRNZ 13.

[89] Search and Surveillance Act 2012, s 46; Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016); and Law Commission *Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012* (NZLC R141, 2017).

[90] *Lorigan v R* [2012] NZCA 264 at [29].

[91] *Hamed v R* [2011] NZSC 101, [2012] NZLR 305 at [47].

[92] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [85]-[89].

[93] *Lorigan v R* [2012] NZCA 264.

As to the question of whether covert video surveillance was a search, counsel for the Crown accepted that covert video surveillance in this context was a 'search' for the purposes of s. 21 of the Bill of Rights Act. This view was supported by two out of three Supreme Court Judges from the case of *Hamed*.[94] In *Hamed,* Blanchard J did not regard surveillance in a public place as being a search because there was no state intrusion into reasonable expectations of privacy. Nonetheless, he did mention that the situation may be different where the "surveillance of the public place involved the use of equipment that captured images that were not able to be seen by the naked eye, such as the use of infra-red imaging"[95] Tipping J in *Hamed* defined "search" as being able to include watching people by technical means. This is highly relevant to the use of live FRT as the system is processing biometric data.

The Court in *Lorigan* considered that the test was "whether the surveillance by the police involves state intrusion into reasonable expectations of privacy" relying on *Ngan*[96] and *Hamed*.[97] However, the Court in *Lorigan* did not consider the "regular" video surveillance to be a search because it did not involve trespass and there was no or minimal intrusion into the privacy rights of those in the area under surveillance.[98] But, in relation to the camera with the night-vision capability – the Court found it was a search as "the images it could capture were such that they could not be seen by the naked eye."[99]

Key Point – Warrantless use of a FR equipped camera in a public place could be considered a 'search' because of the increased technical capabilities of FR as opposed to regular CCTV or recording. This would attract the legislative processes and protections offered in the *Search and Surveillance Act 2012*. The issue of reasonable expectation of privacy in a public place is an evolving legal issue. A legal opinion should be sought before any decision to use live automated FRT.

6.3. Privacy

There is no specific right to privacy in the New Zealand Bill of Rights Act but Article 17 of the International Convention on Civil and Political Rights provides for privacy rights: "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation… Everyone has the right to the protection of the law against such interference or attacks."

The Privacy Act 2020 is a flexible legislative regime that places limits on collection, processing and retention of personal information through the

[94] *Lorigan v R* [2012] NZCA 264 at [15]-[16].
[95] *Lorigan v R* [2012] NZCA 264 at [17]; and *Hamed v R* [2011] NZSC 101, [2012] NZLR 305 at [167].
[96] *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48.
[97] *Hamed v R* [2011] NZSC 101, [2012] NZLR 305.
[98] *Lorigan v R* [2012] NZCA 264 at [23].
[99] *Lorigan v R* [2012] NZCA 264 at [25].

privacy principles (Informational Privacy Principles (IPPs)). IPPs regulate collection, processing, use and disclosure of personal information either by private companies or by public authorities. Facial biometrics are personal information, so every operation on information comprising facial images such as photographs or videos requires compliance with those principles.

The IPPs do not confer on an individual any right that is enforceable in a court of law, except for the right to confirmation whether a public sector agency holds any personal information about an individual and their right to access to that information.[100] Individuals who believe that an organisation has interfered with their privacy should raise this with the organisation concerned in the first instance. If unsatisfied, the individual can make a complaint to the Privacy Commissioner, and then to the Human Rights Review Tribunal.[101]

Deploying an FRT system either by private companies or by public authorities is legal under the Privacy Act 2020, as long as it complies with IPPs.[102] Those principles require: stating a lawful purpose (IPP1), collection of information directly from individuals (IPP2), notifying individuals (IPP3),[103] collection in a manner that is not unfair or unreasonably intrusive (IPP4), ensuring security of information (IPP5), allowing individuals access and correction of information (IPP6 and IPP7), ensuring accurateness of information (IPP8), deleting it where it is no longer needed (IPP9), limiting the use and disclosure of information (IPP10 and IPP11),[104] and some special use of assigned unique identifiers (IPP13).[105] The new Privacy Act 2020 contains an additional principle related to disclosure (or transfer) of information overseas (new IPP12).

The Privacy Act 2020 does not provide for specific, sensitive categories of data, such as biometric data, that would require special protection. [106]However, the Privacy Commissioner is clearly aware about the increased sensitivity of such information, with the Commissioner's website hosting a warning as to its security and risks for individuals associated with potential

[100] Privacy Act 2020, s 31.

[101] Part 5, Privacy Act 2020.

[102] Office of the Privacy Commissioner "Can I use facial recognition technology?" <www.privacy.org.nz>.

[103] A relatively broad exceptions to this principle apply 'to avoid prejudice to the maintenance of law … including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences', when 'compliance would prejudice the purposes of the collection', or even when 'compliance is not reasonably practicable in the circumstances of the particular case', see Privacy Act 2020, s 22, IPP3, cl 4.

[104] Those principles have a very similar set of exceptions as IPP3, described above.

[105] A facial template decoded from someone's face could be considered a 'unique identifier' of the individual under the Privacy Act 2020. That would mean serious limitations to the use of FRT because according to IPP13 in the new Act no agency could assign to the individual unique identifier that has already been assigned by another agency. Such interpretation, however, seems to be unlikely because of the current understanding and use of that term (for identifying numbers, e.g. IRD, passport, or driving licence number), and because the facial template seems to not be 'assigned' by the agency, but naturally belongs to the individual (like a fingerprint).

[106] For more detail, see Office of the Privacy Commissioner 'Office of the Privacy Commissioner position on the regulation of biometrics' (October 2021) available at https://www.privacy.org.nz/assets/DOCUMENTS/2021-10-07-OPC-position-on-biometrics.pdf

data breaches.[107] However the Privacy Act does mention that biometric data (including images of people) can be used and shared in restricted conditions, notably that in the government context only named agencies can do very specific things with that type of information.[108]

In a broader sense, individual and collective conceptions of privacy depend on culture, age, history and personal experience.[109] Community perception will influence privacy expectations. Considering this, any regulation of FRT in New Zealand will have to account for the different understandings of privacy as recognised by Māori, Pākehā and other ethnic and religious minorities. Any benefits accruing from FRT may come at the cost of individual privacy, which is experienced differently depending on the person's context and heritage.[110]

Privacy is a nebulous and culturally loaded concept that is difficult to define. For our purposes, privacy is typically split into two categories:

- Informational privacy – the right to control over collection and use of personal information or data;[111] and
- Spatial privacy – the right to physical inaccessibility to the person or other designated private spaces.

Informational privacy has the potential to be impacted by FRT. Faces are inherently unique to a person and so the information relating to their structural geometry is clearly personal information. The New Zealand Supreme Court has recognised that a person should be protected from intrusion by the state into personal space that is recognised as private in accordance with human dignity.[112] FRT, in breaking the face down to an information structure for identification purposes, goes far beyond day-to-day norms of subjecting each other's faces to a passing glance.

Key Point – FRT, particularly live automated FRT, has a significant potential impact on individual and societal privacy interests. Privacy risks can be ameliorated through a quality and comprehensive Privacy Impact Assessment with appropriate oversight and governance mechanisms which monitor the implementation of the risk assurance conditions, but consultation with diverse communities is also important.

[107] Office of the Privacy Commissioner "Can we collect biometric information" <www.privacy.org.nz>.

[108] Subpart 2 of Part 7, Sharing, accessing and matching personal information, and Schedule 3 which lists the accessing agencies, purpose of access, and holding agency, Privacy Act 2020.

[109] Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [2.34].

[110] Clare Garvie and Laura M Moy "America Under Watch: Face Surveillance in the United States" (16 May 2019) America Under Watch <www.americaunderwatch.com>.

[111] That definition may be derived from works of different privacy scholars: Alan F Westin *Privacy and Freedom* (Atheneum Press, New York, 1967) at 7; Charles Fried "Privacy" (1968) 77 Yale LJ 475 at 483; and Arthur R Miller *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press, Ann Arbor, 1971) at 25.

[112] *Hamed v R* [2011] NZSC 101 at [11].

6.4. Human Rights

Human rights are the basic rights and freedoms that all people are entitled to. A person's human rights arise from a mixture of international and national sources. In New Zealand, this includes the New Zealand Bill of Rights Act, the Human Rights Act and the international human rights framework.

While our conversations with Police staff regularly traversed privacy implications, there was little mention of the potential implications on other fundamental rights and freedoms. Any consideration of the expansion of the use of FRT, particularly live FRT must consider whether the impacts of use are proportionate to the benefits.

Some of the principal areas of human rights that may be affected by the use of FRT are: [113]

- Freedom of thought, conscience and religion; Freedom of expression; Freedom of assembly and association (e.g. where FR systems are used to monitor protests);
- Freedom of movement (e.g. where FR systems are used in border control or in public spaces where a person does not want to be monitored);
- Freedom from discrimination (e.g. where FR systems run on biased algorithms which impact particular sections of society);
- Privacy/respect for private life (e.g. where FR equipped cameras are used in public spaces);
- Protection of personal information/data (e.g. where facial images are stored by the state);
- Right to be free from unreasonable search and seizure (e.g. where FR is used in surveillance by the police);
- Presumption of innocence (e.g. where a person has not been convicted or charged but their facial images form part of a database or watchlist);
- Minimum standards of criminal procedure (e.g. where evidence of identity from a facial recognition match is sought to be introduced into evidence).

A report by the European Union notes that processing of facial images may affect human dignity in the following ways: [114]

- People feeling uncomfortable going to public places because of surveillance,
- biometrics must be obtained in line with human dignity,
- and increased police interaction due to 'hits' from automated FRT.

[113] European Union Agency for Fundamental Rights *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Publications Office of the European Union, 21 November 2019). See also Surveillance Camera Commission *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 of Freedoms Act 2012* (March 2019).

[114] See first item of footnote 114.

Key Points:

- ❖ Privacy impact assessments are an embedded process within Police, but commissioning and use of any FRT system, particularly live automated FRT, should also consider impacts on other rights and interests and the proportionality of those impacts.
- ❖ For example, monitoring of protests or community events with live automated FRT could have a chilling effect on rights to freedom of expression and peaceful assembly. An expansion of facial comparison systems to include those who have not been convicted or charged could impact on a person's right to be presumed innocent until proven guilty.

6.5. Impact on Children and Young Persons

Children, as members of society, are equally affected by the threats that FRT may pose to individual and collective rights. Yet, children's particular characteristics create an additional layer of concern regarding FRT, as 'biometric information collected through cameras falls under the sensitive data category, but also because of children's heightened vulnerability'.[115] Scholars note that children's 'particular vulnerability … relative to adults might make them … natural candidates for heightened protections from facial recognition technologies.'[116]

Children and young persons, as human beings, are rights-holders, and should receive the same minimum standards of human rights protections as adults. Children and young persons have a specialized human rights treaty (the United Nations Convention on the Rights of the Child[117]) which recognises the particular vulnerabilities and characteristics of children and young persons, and emphasises the best interests principle and the principle of non-discrimination. It is appropriate to note that Māori children and young persons are over-represented and thus will bear the brunt of FRT surveillance if implemented.[118] In the context of youth justice, international standards require special consideration for children and young people, based on their vulnerability and lesser capacities.[119] The rights of the child in the digital environment is an issue of contemporary importance,[120] with human rights bodies expressing concern

[115] Human Rights Center, UC Berkeley School of Law, Memorandum on Artificial Intelligence and Child Rights, April 30, 2019

[116] Barrett, Lindsey. 'Ban Facial Recognition Technologies for Children - and for everyone else'. *B.U. J. SCI. & TECH. L.*, Vol. 26 (2020): 2

[117] Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with article 49.

[118] Ministry of Justice *Youth Justice Indicators Summary Report August 2019* (2019).

[119] UN Committee on the Rights of the Child *General Comment No. 24 (2019) Children's rights in the child justice system* CRC/C/GC/24 (18 September 2019).

[120] Caroline Keen "Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy" [2020] New Media Soc 1.

about the impact of emerging technologies and surveillance on the child's right to privacy and the right to freedom of expression.[121]

In Aotearoa New Zealand, there has been considerable concern about police practices in relation to police photographing of children in public spaces for intelligence purposes.[122] As referred to previously, this is permissible under the common law. But such photographing of children in their everyday activities in public spaces is stigmatising and labelling, particularly as the children involved were indigenous children. A review by the Privacy Commissioner and the Independent Police Complaints Authority is now in progress.

Children's particular vulnerability means that collection and retention rules for facial images should be specifically designed with children in mind. Rules should mirror principled approaches to DNA, where collection and retention should only be allowed in specified strictly necessary circumstances, and data deleted to ensure that children are not stigmatised or labelled unnecessarily.[123]

The legislation governing the youth justice system – the Oranga Tamariki Act emphasises principles such as the importance of reintegration and the vulnerability of children and youth during police investigations. There is an emphasis on avoiding the stigmatisation of children and young persons by ensuring that where the child or young person complies with their requirements, that they leave the system without a permanent record (e.g. through the use of the section 282(1) order).

There is some literature relating to the performance of FRT systems with children and young people, which suggests additional problems with accuracy.[124]

[121] Mario Viola de Azevedo Cunha *Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy* (UNICEF, DP 2017-03, December 2017).

[122] Radio New Zealand, Police photographing young Māori: IPCA, Privacy Commissioner investigating (24 December 2020) https://www.rnz.co.nz/news/national/433550/police-photographing-young-maori-ipca-privacy-commissioner-investigating

[123] Lynch N, Campbell L, Purshouse J, Betkier M. Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework Dec 2020 (Report) https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf

[124] Srinivas, Nisha, Karl Ricanek, Dana Michalski, David S. Bolme, and Michael King. "Face recognition algorithm bias: Performance differences on images of children and adults." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pp. 0-0. 2019; Michalski, Dana, Rebecca Heyer, and Carolyn Semmler. "The performance of practitioners conducting facial comparisons on images of children across age." *PloS one* 14, no. 11 (2019): e0225298; Ferguson, Eilidh Louise. "Facial identification of children: a test of automated facial recognition and manual facial comparison techniques on juvenile face images." PhD diss., University of Dundee, 2015.

Children make up approximately 20% of the population in Aotearoa New Zealand and are heavy users of physical and online public spaces. Like adults, children have the right to protest and peacefully assemble, and this typically takes place in public spaces.[125] Recent youth movements such as the School Strike for Climate have demonstrated the power of children's participation in the public space.[126] If FRT was to be used to monitor protests in public spaces may have a similar 'chilling' effect on children's freedom of expression and participation.

Key Points:

- Policies for retention and facial comparison of facial images from children and young persons should align with the established youth justice principles premised on reintegration and align with the principles and rules relating to other biometrics such as DNA and fingerprints.
- Technical standards for accuracy and facial comparison should consider any evidence on how children's faces develop and particular issues relating to accuracy.
- Decision-making around application of FRT to situations and locations where children and young people are likely to be present should specifically consider the rights and interests of children and young persons and consultation with the Office of the Children's Commissioner should be undertaken.

6.6. Impact on Māori

Building on our more general comments about discrimination and bias, specific considerations in Aotearoa must be highlighted. The principles of Te Tiriti require that the impact of decisions and policies on Māori must be considered.[127] Māori are over-represented in the New Zealand criminal justice system, and this disproportionate effect is observed at all stages from apprehension to custody. "Māori are 38% of people proceeded against by Police, 42% of people convicted, and 51% of people in prison."[128] This is despite Māori making up only approximately 16% of the New Zealand population. A range of factors influence this disproportionality from the effects of colonialism,[129] the largely mono-cultural nature of the justice system, bias in decision-making, and the higher rate of adverse life events amongst Māori.[130]

[125] Aoife Daly *A Commentary on the United Nations Convention on the Rights of the Child, Article 15: The Right to Freedom of Association and to Freedom of Peaceful Assembly* (Martinus Nijhoff Publishers, The Hague, 2016).

[126] Shelley Bouillaine ""School Strike for climate": Social Media and the International Youth Protest on Climate Change" (2020) 8 Media Commun 208.

[127] Waitangi Tribunal *Tū Mai Te Rangi! The Report on the Crown and Disproportionate Reoffending Rates* (Wai 2540, 2017).

[128] Hāpaitia te Oranga Tangata: Safe and Effective Justice "Our justice system needs to change" (14 May 2019) <safeandeffectivejustice.govt.nz>.

[129] See footnote 127.

[130] *Ināia Tonu Nei – Hui Māori Report - The time is now: We lead, you follow* (July 2019).

This disproportionate effect means that those whose images populate facial image databases created by the Police, are likely to be disproportionately of Māori ethnicity. No ethnic breakdown of the ethnicity of those images held from convicted persons and voluntary provision could be found, but since the DNA database shows considerable over-representation, it is likely that the rate would be similar. This necessarily enables more intensive policing and surveillance of Māori where FRT is to be used. The impact is further worsened if (as expected) FRT systems are less accurate on Māori faces.

We note the current ongoing project commissioned by New Zealand Police 'Understanding Policing Delivery' which is working on identifying whether, where, and to what extent, bias exists at a system level in Police's operating environment. This work programme will no doubt have relevant findings and recommendation for Police practice relating to collection of data from Māori and other aspects of Police practice and policy. [131]

One of the purported advantages of FRT surveillance is that it can bring objectivity to the exercise of identifying suspects or 'persons of interest' in real time. Unlike the human eye, the software "does not see race, sex, orientation or age."[132] However, this truism masks the danger that this technology can reflect, produce and maintain biases in policing and security outcomes. In particular, as discussed above, the limited independent testing and research into FRT technology indicates that numerous FRT systems misidentify ethnic minorities and women at higher rates than the rest of the population.[133]

As noted in the introductory section, there are particular concerns around accuracy in relation to tā moko and moko kauae.[134] For instance, we heard that a female and her sisters could all have the same moko kauae and this could lead to misidentification due to common facial features. There are also cultural issues in ownership and storage of images of tā moko and moko kauae that have both personal and familial importance. It is also inappropriate in a number of cultures to mix images of deceased persons with living persons,

[131] https://www.police.govt.nz/news/release/independent-panel-and-research-team-appointed-research-policing-our-communities, noting that this work programme has a wider focus than policing of Māori.

[132] See Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 57.

[133] These disparities of performance across different demographic groups are believed to be attributable to the way FRT algorithms are 'trained', and the inherent difficulties in accurately recognising the facial features of some demographic groups. See Brendan F Klare, Mark J Burge, Joshua C Klontz, Richard W Vorder Bruegge and Anil K Jain "Face Recognition Performance: Role of demographic information" (2012) 7 TIFS 1789 at 1797; and Patrick Grother, Mei Ngan and Kayee Hanaoka *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280, December 2019) at 2.

[134] We note that in conversation with the Department of Internal Affairs, there have been few reported issues with tā moko and moko kauae in the context of the passport image process. However, the standard image requirements for the passport situation differ markedly from some of the use-cases discussed here e.g. retrospective or live automated FRT. The risks of tā moko and moko kauae contributing to mis-identification may be higher due to lower quality images or human operator error. We expect to be able to discuss this further with the DIA team before the final publication of this report.

which is likely to occur in an image database unless there is regular data cleaning linked to the Births, Deaths, and Marriages system.[135] Death notices are currently received by the Biometrics team in Police, and the related NIA profile is marked as deceased, but not expunged.

There appears to be a credible risk that FRT technology will undermine the legitimacy of the police and other public authorities if it is targeted disproportionately towards minority groups in society. For example, the targeting of FRT towards neighbourhoods or events that are populated by groups that skew towards a particular demographic may increase the probability that members of the public from these particular backgrounds will be mistakenly identified as 'persons of interest' relative to other demographic groups.

Indigenous data sovereignty is the idea that indigenous peoples have sovereignty over their own data[136] – which would include databases of facial images. Te Mana Raraunga (the Māori data sovereignty network) have recently cautioned about the particular implications of the new all-of-government biometrics contract: "the proposed processing of large-scale biometric data by an overseas agency (DXC Technology via its subsidiary) represents clear and significant risks to Māori Data Sovereignty and the wider community in Aotearoa".[137] There may be particular issues where Police amass a collection of images of predominantly Māori faces.

Key Points – Māori are likely to be most impacted by any expanded use of FRT or implementation of live automated FRT. Police should also undertake further consultation to further explore any cultural considerations around collection and retention of facial images. This should be conducted early in the exploration process when considering adoption of a new FRT tool.

6.7. Government Standards and Policies

6.7.1. Algorithm Charter

New Zealand claims to be the first jurisdiction in the world to have a government commitment to a set of standards for the use of algorithms by the public service.[138] This Charter now sets principles for public sector agencies using algorithms for the basis of, or to guide, decision-making. Government agencies who sign up agree to several principles to guide use of algorithms. The term algorithm is not specifically defined in the Charter, noting that it is the

[135] We acknowledge and thank Karaitiana Taiuru for his time and consideration in making these points in consultation with the authors.

[136] Tahu Kukutai and John Taylor (eds) *Indigenous Data Sovereignty: Towards an Agenda* (ANU Press, Canberra, 2016). Walter, Maggie, Tahu Kukutai, Stephanie Russo Carroll, and Desi Rodriguez-Lonebear. Indigenous Data Sovereignty and Policy. (Routledge,2020).

[137] Te Mana Raraunga "Te Mana Raraunga Statement on Department of Internal Affairs facial recognition system procurement" (press release, 14 October 2020).

[138] James Shaw "New Algorithm Charter a world-first" (press release, 28 July 2020).

effect of the particular algorithm rather than the complexity that must be considered. The key principles of the Charter are:[139]

- Transparency,
- Treaty partnership,
- A focus on people,
- Data that is fit for purpose,
- Privacy, human rights and ethics are safeguarded,
- Human oversight is retained.

6.7.2. Principles for the Safe and Effective Use of Data and Analytics

The Government Chief Data Steward and the Privacy Commissioner have developed a set of principles to guide safe and effective use of data and analytics:[140]

- Deliver clear public benefit – it is essential government agencies consider, and can demonstrate, positive public benefits from collecting and using public data.
- Maintain transparency – transparency is essential for accountability. It supports collaboration, partnership, and shared responsibility.
- Understand the limitations – while data is a powerful tool, all analytical processes have inherent limitations in their ability to predict and describe outcomes.
- Retain human oversight – analytical processes are a tool to inform human decision-making and should never entirely replace human oversight.
- Ensure data is fit for purpose – using the right data in the right context can substantially improve decision-making and analytical models, and will avoid generating potentially harmful outcomes.
- Focus on people – keep in mind the people behind the data and how to protect them against misuse of information.

Applications of FRT should comply with the principles of the Algorithm Charter and the Principles for the Safe and Effective Use of Data and Analytics. It is also important to document the assessment of tools against the Algorithm Charter and the Principles to ensure that assessment processes are robust. The draft New Technology framework being developed by Police proposes an appropriate process for this.

Police have carried out a stocktake of uses of algorithms across the organisation conducted by Taylor Fry.[141] The independent panel has also reviewed the report and provided further advice.

[139] Stats NZ *Algorithm Charter for Aotearoa New Zealand* (July 2020).
[140] Privacy Commissioner and Stats NZ *Principles for the safe and effective use of data and analytics* (May 2018).
[141] See footnote 2.

We agree with the point in time risk assessments of the algorithms underpinning IMS (identity matching) as being low, but as we note in our recommendations section, if the system is expanded to include a wider set of databases, the risk assessment may change.

We note that the Taylor Fry report states that BriefCam does not have a facial recognition capability use currently in use by police, but this was not our finding or the finding in the Technologies Capabilities List. The capability may have been purchased during the time lag between reports. We believe that Police can use BriefCam to find faces in retrospective footage, but use has been limited thus far. It is possible that the Taylor Fry report was referring to facial recognition on live feeds, which is offered by BriefCam but definitely not used by Police.

As we discuss in our recommendation section, we classify retrospective FRT as medium-risk. This is in line with the draft European Union Rules and the approach of Police Scotland.

Key Points:

- Government standards set principles for the safe use of algorithms and data analytics. Of particular relevance to FRT is the human oversight element.
- Police have received independent advice on the commissioning, risk categorization and governance standards around algorithms, including those related to current FRT use. We generally agree with the independent advice that has been shared with us.

6.8. Evidence on Efficacy

We discussed the particular question of accuracy of FRT earlier in the report. Any consideration of the implementation of new capabilities, most particularly the use of live automated FRT, should have a solid evidence base for efficacy against a clear problem. This goes beyond technical accuracy of the system, and speaks to the broader processes and policies, such as what users will do with the information generated by FRT systems.

Duan (in a study based on interviews of police) suggests that that for the use of live FRT,[142] questions of effectiveness should consider the following factors:

- Technical – e.g. how accurate it is across different demographics,
- Teleological – e.g. how effective in achieving the stated purpose,
- Social – e.g. how effective it is compared to alternatives and counterfactuals.

[142] Duan, F., Governing Live Automated Facial Recognition Systems for Policing in England and Wales (December 2020): https://www.bennettinstitute.cam.ac.uk/media/uploads/files/AFR_Isabella_Duan.pdf

There is a dearth of peer-reviewed literature on whether FRT achieves objectives in a policing/law enforcement context. Opinion pieces and promotional material from suppliers identify benefits such as reductions in time spent, catching criminals, preventing crime, reuniting missing children, and removing offensive online material[143] but without much verifiable data such as statistics on outcomes.[144]

Reported cases of successful outcomes of apprehending suspects tend to be anecdotal, and unclear as to whether other leads and investigatory methods were used along with the technology.[145] Evaluations of trials of automated live FRT across the United Kingdom have found problems with inaccuracy and false positives.[146] Body worn cameras showed some positive effect on the crime rate but no evidence for FRT.[147]

We heard from our conversations with Police staff that it was important that there was a clear identification of the problem that was intended to be solved, particularly when considering any use of live automated FRT.

Key Point – there is very limited current evidence base for the efficacy and cost benefit of live automated FRT in policing. Any proposal for broadening of the use of FRT or implementation of live automated FRT must identify a clear problem to be solved that the proportionality and appropriateness of the technology use can be assessed against.

6.9. 'Policing by Consent', Trust, Legitimacy

The phrase 'policing by consent' was mentioned regularly in our interviews as being an important consideration and constraint when considering use or potential use of FRT. People appeared to have differing conceptions of the concept, mainly falling into two principal categories:

- ❖ Policing depends on the consent of the people rather than coercion,

[143] Michael Punke, Some Thoughts on Facial Recognition Legislation (7 February 2019) https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/

[144] https://www1.nyc.gov/site/nypd/news/s0610/how-facial-recognition-makes-you-safer

[145] See e.g. https://www.usatoday.com/story/tech/talkingtech/2018/06/29/capital-gazette-gunman-identified-using-facial-recognition-technology/744344002/

[146] Bethan Davies, Martin Innes and Andrew Dawson, "An Evaluation of South Wales Police's Use of Automated Facial Recognition," (September 2018).; Fussey, Peter, and Daragh Murray. "Independent report on the London Metropolitan Police Service's trial of live facial recognition technology." (2019); Metropolitan Police Service, "Metropolitan Police Service Live Facial Recognition Trials," (February 2020), 5: https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/metevaluation-report.pdf.

[147] Park, Jiyong and Pang, Min-Seok, Information Technology on the Beat: The Impacts of Body-Worn Camera and Facial Recognition Technology on Public Safety (July 24, 2019). Available at SSRN: https://ssrn.com/abstract=3426427 or http://dx.doi.org/10.2139/ssrn.3426427

- The police reflecting what the public wanted – in the sense of 'the public would expect that…' (this is more aligned with social licence, discussed in the next section)

The first concept is aligned with the classic statement of policing by consent (derived from the principles underpinning the early police force in England): [148]

- To recognise always that the power of the police to fulfil their functions and duties is dependent on public approval of their existence, actions and behaviour and on their ability to secure and maintain public respect.
- To recognise always that to secure and maintain the respect and approval of the public means also the securing of the willing co-operation of the public in the task of securing observance of laws.

In New Zealand Police's Briefing to the Incoming Minister, the Commissioner defined the concept as: [149]

> We police by consent; this means we work alongside and with the broad support of the communities we ourselves come from, in order to be effective. The way our actions are perceived impacts on the public's willingness to engage and work with us.

There are concerns that the use of FRT may damage the legitimacy of Police, particularly if its use is not transparent or consensual. Police generally depend on the voluntary support and cooperation of the public to exercise their functions effectively, and this support is often contingent upon public perceptions of the manner in which police exercise their authority.[150] The Black Lives Matter protests that have spread across the world in recent months are a potent example of how excessive or discriminatory exercise of police power can rapidly lead to a breakdown in police/community relations.

If FRT is perceived to produce unfair or discriminatory outcomes or is used excessively in the absence of a prescribed legal framework, there is a risk that this will corrode the legitimacy of the police.[151] When subject to automated surveillance, it is important that the public can assess that any intrusion occasioned is lawful and justifiable.

Key point – inappropriate or unjustified expansion of FRT, particularly live automated FRT, may have a negative effect on police-community relations.

[148] https://www.gov.uk/government/publications/policing-by-consent/definition-of-policing-by-consent

[149] New Zealand Police 'Briefing to the Incoming Minister of Police – Part A – Overview of Portfolio' November 2020

[150] See, for example, Tom R Tyler "Enhancing Police Legitimacy" (2004) 593 Ann Am Acad Pol Soc Sci 84.

[151] Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, 60(6), 1502–1522.

6.10. Social Licence/Public Opinion

Gulliver et al have defined social licence in the New Zealand data context as being:[152]

> "…societal acceptance that a practice that lies outside general norms may be performed by a certain agent, on certain terms. It is the result of a process of negotiation with a wider societal group, and means that the practice can be performed by that agent without incurring social sanction."

Social licence can never override consent, human rights or privacy protections. Social licence may be relevant in considering the shape of legislative and policy reform. A salient question is also whether social licence for privacy and liberty restrictions in pursuit of collective safety/welfare has changed in the context of the 2020 global pandemic. Social licence can change rapidly – we have seen that in relation to reactions to terrorist attacks such as the Christchurch mosque terror incident[153] but perhaps COVID-19 may shift social licence more slowly[154].

Several themes emerged from our interviews about the risks that automated live FRT or considerable expansion in facial comparison systems could pose to social licence. There was mention of the risks of losing rapport with the public, and a backlash against surveillance in public spaces which could then spread to resistance towards established tools such as CCTV.

It was also mentioned that there could be risks to public confidence if Police did not take advantage of the safe use of technology to carry out its functions more efficiently. Multiple interviewees cited the Christchurch mosque terror incident as a reason to use FRT, but acknowledged that the technology may be less appropriate for crime at the lower end of the spectrum of harm, such as shoplifting.

6.10.1. Research studies on public views of FRT in policing

Research studies in other jurisdictions give insight into people's level of comfort with the use of FRT. We qualify this discussion that there is little or no insight into indigenous peoples' or minority groups, or any studies specifically on New Zealand.

[152] Pauline Gulliver, Monique Jonas, Tracey McIntosh, Janet Fanslow and Debbie Waayer "Surveys, social licence and the Integrated Data Infrastructure" (2018) 20 ANZSW 57 at 60.

[153] Nur Diyanah Anwar and Cameron Sumpter "Societal resilience following terrorism: Community and coordination in Christchurch" [2020] Behav Sci Terrorism Polit Aggres 1; and S Every-Palmer, R Cunningham, M Jenkins and E Bell "The Christchurch mosque shooting, the media, and subsequent gun control reform in New Zealand: a descriptive analysis" [2020] Psychiatr Psychol Law 1.

[154] Leslie Lenert and Brooke Yeager McSwain "Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic" (2020) 27 J Am Med Inform Assoc 963; and Sawsan Abuhammad, Omar F Khabour and Karem H Alzoubi "COVID-19 Contact-Tracing Technology: Acceptability and Ethical Issues of Use" (2020) 14 Patient Prefer Adherence 1639.

Most people surveyed in studies in the US, UK and Australia[155] were comfortable with the police or government using FRT for law enforcement purposes. However, the surveys indicated that most people would want regulations in place to control this power. Further, in the UK study, most people believed that there should be the option to opt out of FRT (46% thought this option should be available, 28% did not and the rest were unsure).

The surveys listed common reasons behind people being uncomfortable with police use of FRT in UK and Australia. These included the infringement on privacy, normalisation of surveillance, lack of opt out or consent and lack of trust in the police to use the technology ethically.

The Australian study also gathered common reasons why people were comfortable with the government using FRT. These included the fact that they had nothing to hide, that security is very important to protect against terrorists and catch the 'bad guys,' placing a higher priority on security than privacy and loosening societal expectations around privacy.

In November 2021, it was reported that Adelaide City Council voted to block Police using FRT on the new city surveillance network, citing risks to privacy and public concern. [156]

A separate study showed that China has reasonably high levels of acceptance for FRT (67%), followed by the UK (50%) and US (48%), with the least acceptance in Germany (38%).[157] A study with mostly New Zealand-participants found that an 'intelligence agency person tracking' scenario was the second least comfortable out of ten surveillance camera scenarios, and elicited the strongest response from the privacy-conscious, although this study did not focus on FRT specifically.[158] The Office of the Privacy Commissioner reports that in their 2020 survey, 41% of respondents were 'concerned with the use of CCTV and facial recognition technology'.[159]

[155] Aaron Smith "More than half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly" (5 September 2019) Pew Research Center <pewresearch.org>; Darrell M West "Brookings survey finds 50 percent of people are unfavorable to facial recognition software in retail stores to prevent theft" (8 October 2018) Brookings <brookings.edu>; Ada Lovelace Institute *Beyond face value: public attitudes to facial recognition technology* (September 2019); and Roy Morgan "Australians not concerned about use of mass facial recognition technology" (10 October 2017) <roymorgan.com>.

[156] Malcolm Sutton, "Facial recognition technology put on hold in Adelaide amongst privacy concerns" 10 November 2021 https://www.abc.net.au/news/2021-11-10/facial-recognition-tech-on-hold-amidst-privacy-concern/100608514

[157] Genia Kostka, Léa Steinacker, Miriam Meckel "Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States" *Public Understanding of Science* 30(6) 671-690.

[158] Andrew Tzer-Yeu Chen, Morteza Biglari-Abhari, Kevin I-Kai Wang "Context is King: Privacy Perceptions of Camera-based Surveillance" *2018 IEEE International Conference on Advanced Video and Signal-based Surveillance (AVSS)*. The respondents rated the 'supermarket motion tracking' scenario (which included connecting individual tracks to loyalty cards) the least comfortable scenario.

[159] Office of the Privacy Commissioner "Survey: Two thirds of New Zealanders want more privacy regulation" < https://www.privacy.org.nz/publications/statements-media-releases/survey-two-thirds-of-new-zealanders-want-more-privacy-regulation/>

In the United Kingdom, football fans have responded to the use of live FRT at a number of matches by wearing face coverings or holding up signage to protest its use. When South Wales Police used live facial recognition at a football match between Cardiff City and Swansea City in January 2020, this prompted condemnation from football supporters' groups and civil liberties campaigners who argued that its use on football fans was unduly stigmatising.[160]

The Ada Lovelace Institute in the United Kingdom established a Citizens' Biometrics Council to engage in a deliberative democracy process involving 50 diverse community members. Participants heard from experts including police strategists, technology developers, regulators, campaigners, tech ethicists and more – and debated on the opportunities and risks posed by biometric technologies.

Some relevant themes from the findings include:[161]

- Participants accepted that "some loss of privacy through surveillance as a trade-off for living in a society which is kept safe from crime or other harms"
- "Uses of biometrics that seem more beneficial, or even benign, could act as gateways to rolling out more controversial uses with less resistance, as the 'acceptance' of biometric technologies would become normalised."
- "Where public health and safety is the goal, consent could be obtained by broad public consensus or approval"
- "Uses of biometrics must be transparent and accountable"
- "Inaccuracies and errors can cause harms and damage trust"
- "Disproportionate impacts occur when the technologies deployed reflect and amplify biases that can exist in unrepresentative datasets, be baked into poorly designed algorithms, or be prevalent in institutional and social norms."

Key Points:

- There are few specific studies of public opinion on FRT in the context of Aotearoa New Zealand.
- Studies from other jurisdictions indicate greater public acceptance of law enforcement use of FRT when compared to other use-cases.
- Social licence would have to be carefully gauged, including genuine engagement with diverse communities.

[160] Football Supporters Europe "FSE Opposes Fans Being Used as Test Subjects for Facial Recognition Technology" <www.fanseurope.org>.

[161] A full copy of the report can be accessed at https://www.adalovelaceinstitute.org/project/citizens-biometrics-council/. These quotes are drawn from the "Findings" chapter.

6.11. Counter-Surveillance Against Police

Lastly, it is worth mentioning that there have been media reports in other jurisdictions of OSINT tools being used to identify police officers.[162]

It is entirely possible that covert operations staff could be subject to counter-surveillance using OSINT tools which collect publicly available images such as public social media profiles or profiles from public websites to identify people.

We did not specifically consider whether Police had guidelines or guidance on this issue, but we recommend that Police review whether any guidance needs to be provided, updated or implemented.

[162] Activists Turn Facial Recognition Tools Against Police, New York Times, https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html

PART 7. LESSONS FROM COMPARABLE JURISDICTIONS

Comparable jurisdictions are using FRT to a greater degree, particularly in the sphere of live automated FRT. This does afford Police in Aotearoa New Zealand a valuable opportunity to consider and reflect on the use of FRT by police forces in other jurisdictions before any decisions on expansion of the use of FRT or particularly any moves to implement live automated FRT. In this section we will highlight use-cases and lessons from a selection of comparable jurisdictions.[163]

This is a rapidly moving subject and new reports and guidelines appear regularly. Only a portion of the most relevant issues are mentioned here. One of our recommendations is that Police have a structured horizon scanning process for emergent/new technologies and the situation in comparable jurisdictions will be a key part of this.

7.1. England and Wales

7.1.1. *Developments in use of FRT*

England and Wales have been the site of a number of trials of live automated FRT for law enforcement e.g. with South Wales Police,[164] the London Metropolitan Police,[165] and various quasi-private schemes[166] The Protection of Freedoms Act 2012 provides a legal framework for two types of biometrics (DNA and fingerprints) but does not apply to other biometrics such as facial images, gait, or voice. No jurisdiction in the United Kingdom has introduced any specific laws relating to FRT; this situation has prompted much commentary as well as an ongoing legal challenge. A number of academic commentators suggested that police deployment of FRT in England and Wales may be held unlawful due to the absence of domestic legal authorisation.[167] The Law Society for England and Wales suggested that it is highly unclear whether facial recognition at scale can meet a test of strict necessity as required under the Data Protection Act 2018, particularly given issues of accuracy and its “highly unproven nature”.[168] The police response to this was that the legal basis regulating its proper operational limits is adequate

[163] We note that there is considerable media and other coverage of police and security services' use of FRT in China. There is also considerable doubt as to the accuracy and verifiability of these reports. We have chosen to focus here on jurisdictions with similar legal systems and comparable protections of rights and freedoms.

[164] Big Brother Watch *Face Off: The lawless growth of facial recognition in UK policing* (May 2018).

[165] National Physical Laboratory and Metropolitan Police Service *Metropolitan Police Service Live Facial Recognition Trials* (February 2020).

[166] Dan Sabbagh “Facial recognition technology scrapped at King's Cross site” *The Guardian* (online ed, United Kingdom, 2 September 2019).

[167] Joe Purshouse and Liz Campbell “Privacy, Crime Control and Police Use of Automated Facial Recognition Technology” (2019) 3 Crim Law Rev 188 at 198; and Pete Fussey and Daragh Murray *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (Human Rights Centre, July 2019).

[168] Michael Veale *Algorithms in the Criminal Justice System* (The Law Society of England and Wales, June 2019) at 42.

and lies in the Data Protection Act 2018 (DPA 2018); the Surveillance Camera Code of Practice; and relevant common law and human rights principles.

7.1.2. *The Bridges Decision*

South Wales was the setting for the first court challenge to the use of live automated FRT in a public place. South Wales Police (SWP) had been using a mobile camera van to run a FRT equipped camera with a 'watchlist'. SWP is the national lead on FRT in England and Wales, having received a £2.6 million government grant to test the technology. Mr Bridges had challenged the legality of SWP's use pf FRT on the grounds that its use was contrary to the Human Rights Act 1998, Data Protection legislation, and that the decision to implement it had not been taken in accordance with the Equality Act 2010.

In September 2019, a Divisional Court in *R v Bridges* refused an application for judicial review challenging the legality of SWP's use of FRT.[169] The matter was appealed, and the Court of Appeal ruled that the Divisional Court erred in its finding that the measures were 'in accordance with the law'. The Court analysed whether the framework governing the use of live AFR was reasonably accessible and predictable in application, and sufficient to guard against 'overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights'.[170] While statutory authorisation was not deemed to be required, the Court of Appeal was not satisfied that the SWP's use of live automated FRT was sufficiently regulated by the combination of the DPA 2018, the Surveillance Camera Code of Practice and SWP's local policies, as this left too much discretion in terms of who was to be placed on the watchlist, and where the technology could be deployed.[171] This is a significant finding, as it means that more detailed and circumscribed polices would address these issues and thus satisfy the 'in accordance with the law' component of Article 8(2). The Court held that the SWP's use of AFR was a proportionate interference with Article 8 rights under Article 8(2). In addition, the Court held the Divisional Court erred in finding that SWP provided an adequate 'data protection impact assessment' (DPIA) as required by the DPA 2018. Finally, the Court of Appeal held that the SWP 'never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex.'[172]

7.1.3 *Guidelines*

Subsequent to *Bridges*, there has been a considerable amount of guidance and review documents forthcoming on the subject of live automated FRT in England

[169] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin).
[170] *Beghal v Director of Public Prosecutions* [2015] UKSC 49, [2016] AC 88 at [31] and [32] per Lord Hughes.
[171] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [96].
[172] *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [199].

and Wales. We summarise some main points here, but this is an area worth monitoring. We particularly note that the College of Policing is working on Authorised Professional Practice guidelines on the use of the technology, which were not yet available at the time of writing.[173]

In addition, there are several guidance documents, such as from the Home Office Biometrics and Forensics Ethics Group (2018), and the Surveillance Camera Commissioner (2019),[174] which seek to steer police practice in this area. Though these guidance documents may be cited in court, they do not provide actionable grounds for an individual to make a complaint. Moreover, non-compliance would not impact on the admissibility of any material gleaned.

The United Kingdom's Information Commissioner's Office provides guidance for police forces considering FRT:

- "Carry out a data protection impact assessment and update this for each deployment - because of the sensitive nature of the processing involved in LFR, the volume of people affected, and the intrusion that can arise. Law enforcement organisations are advised to submit data protection impact assessments to the ICO for consideration, with a view to early discussions about mitigating risk.
- Produce a bespoke 'appropriate policy document' to cover the deployments - it should set out why, where, when and how the technology is being used.
- Ensure the algorithms within the software do not treat the race or sex of individuals unfairly."[175]

In terms of any future police trials of FRT and other technologies, the London Policing Ethics Panel has proposed a framework to support analysis of the ethical issues raised field trials of policing technologies, grouping suggested inquiries into four domains: serving the public; robust trial design; respect for equality, dignity and human rights; and addressing concerns and outcomes.[176]

The House of Commons Science and Technology Committee in July 2019 reiterated its recommendation from a 2018 Report, that live automated FRT

[173] A public consultation was open until late June: https://www.college.police.uk/article/police-use-live-facial-recognition-technology-have-your-say

[174] Biometrics and Forensic Ethics Group *Ethical Issues arising from the police use of live facial recognition technology* (Facial Recognition Working Group, Interim Report, February 2019); and Surveillance Camera Commission *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 of Freedoms Act 2012* (March 2019).

[175] Suzanne Shale, Deborah Bowman, Priyah Singh and Leif Wenar *London Policing Ethic Panel: Final Report on Live Facial Recognition* (London Policing Ethics Panel, London, May 2019) at 8.

[176] See footnote 175.

should not be deployed until concerns over the technology's effectiveness and potential bias have been fully resolved.[177]

While the previous Surveillance Camera Commissioner was critical of FRT, the new merged role of Biometrics and Surveillance Camera Commissioner believes police, "will have no alternative but to use facial recognition along with any other technology that is reasonably available to them."[178] The Commissioner's views are premised on the need for Police to be able to match the technological sophistication of criminals.

These views are in opposition to previous Commissioner, Paul Wiles, who believed the significant intrusion posed by the technology meant it ought to be subject to strict regulation and oversight. In reference to the proposed AI regulations recently published by the European Commission which would allow countries to place a blanket ban on facial recognition, the current Commissioner said:[179]

> I think where the risk lies is if … you end up with complete bans, it results in the proscription of certain technologies and tools and techniques, as we have seen in some other jurisdictions. I think blanket bans … may well be premature.

He went on to say, "I think the framework, whatever we come up with in future, needs to … enable public bodies like police… to reasonably use all means available to discharge their statutory duty."[180]

The Home Office's Biometrics and Forensics Ethics Group (BFEG) was recently commissioned to investigate ethical issues relating to the use of the collaborative use of live automated FRT by police and private sector organisations, for example in airports or shopping centres.[181] There is particular thought given to the fact these situations often leave people no choice of being observed by CCTV cameras, and thus there is no genuine consent to be subject to FRT.

The group found that these situations are likely to increase and in light of this, as well as a variety of ethical concerns which the group highlighted in regard to privacy, data security and freedoms, made a number of recommendations of how best to protect the privacy of the public. The recommendations included:

[177] House of Commons Science and Technology Committee *The work of the Biometrics Commissioner and the Forensic Science Regulator: Nineteenth Report of Session 2017-19* (HC 1970, 17 July 2019) at [25].

[178] *Police Should not be Banned from Using Facial Recognition Technology, Says UK Watchdog* Financial Times (3 May 2021) at paragraph 2. <https://www.ft.com/content/79223f6e-a772-4e74-b256-88641a416f92>.

[179] At paragraph 8.

[180] At paragraph 9.

[181] *Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology* The Biometrics and Forensics Ethics Group (21 January 2021).

- The establishment of an independent ethics group to oversee the use of live FRT both by the Police and in collaborative use scenarios.
- Police should only share data with trustworthy organisations that have been vetted.
- Data should be shared with, or accessed by, the minimum number of people.
- Biometric data (including image data) must be safely and securely stored.
- Watchlists should be narrow and targeted.
- A publicly accessible record of collaborative uses of LFR should be created.
- Collaborative use of LFR should be authorised by a senior police officer.

7.2. Scotland

Scotland currently has a moratorium on law enforcement use of live FRT, in contrast to the rest of the United Kingdom. While Police Scotland's 10-year strategy, Policing 2026, included a proposal to use live FRT,[182] a parliamentary committee was highly critical of this. The Justice Sub-Committee on Policing found that live FR software is known to discriminate against women, and those from black, Asian and ethnic minority communities, that there is no justifiable basis for Police Scotland to invest in this technology; that prior to any decision to introduce automated live FRT a robust and transparent assessment of its necessity and accuracy should be undertaken, and that the potential impacts on people and communities are understood, and that the use of live facial recognition technology would be a radical departure from the fundamental principle of policing by consent.[183]

A subsequent response from Police Scotland responded that the force currently does not use live facial recognition technology, nor has plans to do so at this time, that it would ensure safeguards are in place prior to introducing the use of this technology, and agreed that the impact of its use should be understood fully before it is introduced.[184]

7.3. The European Union

The European Union (EU) is a standard setter for data protection, even outside its territorial jurisdiction. The General Data Protection Directive (GDPR) is highly influential worldwide, even where compliance is not strictly required.

[182] Police Scotland *Policing 2026: Our 10 Year Strategy for Policing in Scotland* (June 2017) at 39 and 43.

[183] Justice Sub-Committee on Policing *Facial recognition: how policing in Scotland makes use of this technology* (SP Paper 678 1st Report, 2020 (Session 5), 11 February 2020).

[184] Letter from Duncan Sloane (T/Assistant Chief Constable Major Crime and Public Protection) to Convenor of Justice Sub-Committee on Policing regarding Facial Recognition: how policing Scotland makes use of this technology (8 April 2020).

In mid-2021, the European Union (EU) promulgated a draft set of Rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach.

The EU is a major world market, and if these Rules are adopted, it will have a significant effect and influence on tech development and commercial strategies even outside the EU. We will focus here on some key aspects related to 'remote biometric ID' which would include live automated FRT.

The draft regulation would:

- Define 'public space' for the purposes of remote biometric ID systems as "any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned."
- Regard remote biometric ID in public spaces (e.g. facial recognition) as 'particularly intrusive' and should be prohibited except where it is strictly necessary to achieve substantial public interest. Examples include threats to life, terrorism, search for victims of crime, and detecting serious crime (defined as attracting a term of imprisonment of three years or more.[185]
- Live automated FRT is considered "particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities."[186]
- Impose the following safeguard – "Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should in principle be obtained prior to the use, except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In such situations of urgency, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations seek to

[185] Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN, at para 19
[186] Draft regulation, at para 18

> obtain an authorisation as soon as possible, whilst providing the reasons for not having been able to request it earlier."

The European Data Protection Board has gone further and called for a complete ban on live automated FRT:[187]

> Deploying remote biometric identification in publicly accessible spaces means the end of anonymity in those places. Applications such as live facial recognition interfere with fundamental rights and freedoms to such an extent that they may call into question the essence of these rights and freedoms. This calls for an immediate application of the precautionary approach. A general ban on the use of facial recognition in publicly accessible areas is the necessary starting point if we want to preserve our freedoms and create a human-centric legal framework for AI. The proposed regulation should also prohibit any type of use of AI for social scoring, as it is against the EU fundamental values and can lead to discrimination.

On 6 October 2021, a majority of the European Parliament voted in favour of a resolution which noted the potential discrimination and bias in AI systems, and noted that human supervision and strong legal powers are needed, particularly where such technologies are used in a law enforcement or border enforcement context.[188] The resolution called for a permanent ban on the automated recognition of individuals in public spaces, noting that individuals should only be subject to such monitoring when suspected of a crime. Private facial recognition databases (such as Clearview) and predictive policing based on behavioural data should also be forbidden.

7.4. The United States

Considerable analysis on the use of FRT systems by police in the US has been done by Clare Garvie of Georgetown University.[189] FRT is in widespread use in the US policing context. Police in multiple jurisdictions can use FRT to identify people that they encounter who refuse to be identified or cannot identify themselves. They can take the person's photo with a device, process it through software they have in their patrol car, and receive a near-instantaneous response from the system.[190]

[187] EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination (21 June 2021)
https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

[188] European Parliament, Press release: Use of artificial intelligence by the police: MEPs oppose mass surveillance (6 October 2021), https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance

[189] Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016).

[190] At 10.

When investigating a crime, they run a picture of a suspect captured from a security camera or other device through a database of mugshots or drivers licences and create a list of candidates for further investigations. This can also be used when police believe that a suspect is using a pseudonym.[191] FRT can also be used for real-time video surveillance. When the police are looking for an individual, they can upload an image of them to a 'hot list'. A FRT program compares images from real-time video surveillance to this hot list to find the individuals. When a match is found, police are alerted. Similar searches can also be run on archival footage.[192]

FRT is also used to catch those using fraudulent identification. Departments of Motor Vehicles can compare the faces of new applicants for identification against the existing faces in its database. Individuals who may be using the same person's photo and a pseudonym as fraudulent identification are flagged.[193]

However, in some jurisdictions, significant constraints have been placed on the use of FRT. For instance, Oregon and New Hampshire barred the use of facial recognition searches of police body worn camera recorded footage;[194] Maine and Vermont restricted the use of facial recognition on footage collected by police drones,[195] Massachusetts has passed a law that places comprehensive limits on law enforcement use of FRT,[196] Michigan requires the destruction of facial recognition data from people who are arrested but never charged, or are acquitted.[197]

In 2019, authorities in San Francisco banned the use of facial recognition technology, or information received from external systems that use the technology, by the police and other city agencies.[198] This was followed by the City of Oakland and the City of Berkeley.[199] Most recently, the Portland City Council banned the public and private use of facial recognition technology in September 2020.[200] A hiatus has been imposed in a number of US states: in

[191] At 11.
[192] At 12.
[193] At 12.
[194] Or Rev Stat § 133.741(1)(b)(D); and NH Rev Stat Ann § 105-D:2(XII).
[195] Me Rev Stat Ann, title 25 § 4501(5)(D); and Vt Stat Ann, title 20 § 4622(d)(2).
[196] See Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 35. This report observes that "Not a single state has passed a law that places comprehensive limits on law enforcement use of face recognition technology", though this predates the Massachusetts State Senate Bill.
[197] Mich Comp Laws Ann § 28.243(7)-(8). See Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 35.
[198] SF Admin Code § 19B.2(d); and Kate Conger, Richard Fausset and Serge F Kovaleski "San Fransisco Bans Facial Recognition Technology" *The New York Times* (online ed, New York, 14 May 2019).
[199] Oakland Mun Code § 9.64.045; Edwin Chau *Resolution opposing California State Assembly Bill No. 2261* (City and County of San Fransisco, Res No 217-20, 12 May 2020) at 1; and Berkley Mun Code § 2.99.030(5).
[200] Portland.gov "City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces" (press release, 9 September 2020)

July 2020, the New York legislature voted to pause the implementation of FRT in schools for two years, and the state's education commissioner is to issue a report on the potential impact of the technology on students and staff privacy.[201] Likewise, in June 2020, the Massachusetts state senate passed a bill that pauses law enforcement use of FRT until a special commission studies it and recommends regulation.[202]

Maine has passed the strongest anti-facial recognition laws in the country which[203] "prohibits the use of facial recognition technology in most areas of government, including in public schools and for surveillance purposes. It creates carefully carved out exceptions for law enforcement to use facial recognition, creating standards for its use and avoiding the potential for abuse." The Article goes on to say: "law enforcement must now — among other limitations — meet a probable cause standard before making a facial recognition request, and they cannot use a facial recognition match as the sole basis to arrest or search someone. Nor can local police departments buy, possess or use their own facial recognition software, ensuring shady technologies like Clearview AI will not be used by Maine's government officials behind closed doors."

Civil liberties organisations have proposed ethical frameworks for the use of FRT. One such example is in a 2016 report of the Center on Privacy & Technology at Georgetown Law by Clare Garvie. This provides a very helpful overview of recommendations for "commonsense" and "comprehensive" regulation,[204] which while created with the US context and legal framework in mind, are of comparative value.

The most salient recommendations include:

- "Law enforcement face recognition searches should be conditioned on an individualized suspicion of criminal conduct."
- "Mug shot databases used for face recognition should exclude people who were found innocent [sic] or who had charges against them dropped or dismissed."
- "Searches of driver's license and ID photos should occur only under a court order issued upon a showing of probable cause."
- "Limit searches of license photos—and after-the-fact investigative searches—to investigations of serious offenses."
- "Real-time video surveillance should only occur in life-threatening public emergencies under a court order backed by probable cause."

[201] Connor Hoffman "State Sentate to vote on facial recognition moratorium bill" *Niagra Gazette* (online ed, Niagra Falls, 21 July 2020).
[202] MA Bill S.2800 § 65(b); and Jared Council "Massachusetts Senate Passes Bill That Would Halt Police Use of Facial Recognition" (14 July 2020) WSJ Pro Artificial Intelligence <www.wsj.com>.
[203] *Maine's facial regontion law shows bipartisan support for protecting privacy Tech Crunch* (21 July 2021): https://techcrunch.com/2021/07/20/maines-facial-recognition-law-shows-bipartisan-support-for-protecting-privacy/
[204] Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 62.

- "Use of face recognition to track people on the basis of their race, ethnicity, religious, or political views should be prohibited."
- "All law enforcement use of face recognition should be subject to public reporting requirements and internal audits."
- "State … financial assistance for face recognition should be conditioned on transparency, oversight, and accountability"

State and local law enforcement should:

- "Impose a moratorium on face recognition searches of state driver's license and ID photos until state legislatures regulate that access"
- "Adopt public face recognition use policies that have received legislative review and approval."
- "Use contracts and the contracting process to maximize accuracy"
- "Implement internal audits, tests for accuracy and racial bias, and the use of trained face examiners."[205]

7.5. Australia

FRT is used by a number of police forces in Australia, though empirical evidence about the extent of use is patchy. For instance, police and city councils in Perth and Melbourne use FRT to identify individuals, but there is no indication of specific guidance or statistics linked to this.[206]

Australian Federal Police and Victoria Police have been using Clearview AI.[207] This revelation about law enforcement use was despite initial police denials. Clearview uses an FR algorithm to allow users to photo anyone in public, upload it, and access public images of that person collected by Clearview, such as on their public social media accounts.[208] As this case exemplifies, like in *Bridges* (and New Zealand), if Australian police forces are not banned from using FRT explicitly they do not need specific legislative authority to deploy it.

The Office of the Australian Information Commissioner (OAIC) subsequently found that Clearview AI's methodology of harvesting social media images was unlawful as it collected sensitive information without consent and without checking its matches were accurate[209]. The OAIC ordered the company to stop collecting images and to destroy the data collected in Australia. An investigation in the Australia Federal Police's trial of the software is being finalised at the time of writing.

[205] Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 68.

[206] City of Melbourne "Safe City cameras" <melbourne.vic.gov.au>; and Elias Visontay "Councils tracking our faces on the sly" The Australian (online ed, Canberra, 29 August 2019).

[207] Stephanie Palmer-Derrien "Aussie entrepreneur launches "disturbing and unethical" facial recognition tech in Silicon Valley" (22 January 2020) Smart Company <smartcompany.com.au>.

[208] Hannah Ryan "Australian Police Have Run Hundreds of Searches On Clearview AI's Facial Recognition Tool" (28 February 2020) Buzzfeed <buzzfeed.com>.

[209] Byron Kaye "Australia says U.S. facial recognition software firm Clearview breached privacy law" (4 November 2021) Reuters <reuters.com>.

At the federal level an Intergovernmental Agreement on Identity Matching Services was reached in 2017 between the Prime Minister and the first ministers of all states and territories.[210] This agreement hinged on retention or creation of legislation to support the sharing of facial images and related identity information, via a set of "identity-matching services", for a range of national security, law enforcement, community safety and related purposes.

The Identity Matching Services include the Document Verification Service (DVS); Face Verification Service (FVS), which involves one-to-one matching to help verify the identity of a known person; Face Identification Service (FIS), one-to-many or one-to-few matching to identify an known person or where a person may hold multiple identities; One Person One Licence Service (OPOLS), "a narrowly focused check, on a constrained one-to-many basis, of facial images within the National Driver Licence Facial Recognition Solution"; Facial Recognition Analysis Utility Service (FRAUS), enabling each state or territory Road Agency or licencing authority to conduct biometric matching using its own data; and the Identity Data Sharing Service (IDSS).[211]

Agencies with access to the Face Identification Service may use the service for a list of specified purposes only, which centring quite an expansive interpretation of safety and security.[212] Private sector access currently is not allowed for any FRT services under the National Facial Biometric Matching Capability, though there is provision to make Facial Verification Services available to the private sector for one-to-one matching in accordance with the agreement.[213] No other FRT related services will be made available to the private sector.[214]

Part 8 of the Intergovernmental Agreement suggests that legislation should be preserved or introduced to the extent necessary to support the Facial Matching Services. Part 9 discusses privacy concerns and steps to be taken to address or mitigate these concerns. Part 11 provides that "The Ministerial Council for Police and Emergency Management (MCPEM) will exercise ministerial oversight of the Identity Matching Services".

There is a memo of understanding between the Office of the Australian Information Commissioner and the Attorney General's Department on the National Facial Biometric Matching Capability,[215] setting out the role of the OAIC in relation to its role of assessing and advising the AGD in relation to FRT. While the primary focus appears to be in relation to funding the purpose of the

[210] Council of Australian Governments Intergovernmental Agreement on Identity Matching Services (Australia, 5 October 2017); Australian Government Department of Home Affairs *Privacy Impact Assessment: Law Enforcement, Crime and Anti-Corruption Agency Use of the Face Matching Services, NFBMC (v.1.0)* (Bainbridge Associates, March 2019).

[211] Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017), part 4.

[212] At [4.21].

[213] At part 5.

[214] At [5.5].

[215] Office of the Australian Information Commission *MOU in relation to National Facial Biometric Matching Capability* (15 November 2017).

MOU appears to be: "to set out the operational arrangements between AGD and the OAIC by which the OAIC will conduct privacy assessments of AGD's privacy practices in connection with the NFBMC".[216] Beyond this, each agency must enter into a separate agreement on data sharing and a separate MoU with the Attorney-General's Department, setting out the terms and safeguards.

The *Identity-matching Services Bill 2018* was introduced in 2018 to authorise the Department of Home Affairs to collect, use and disclose identification information in order to operate the systems that will support a set of new biometric face-matching services. This Bill was seeking to implement the 2017 Intergovernmental Agreement on Identity Matching Services just outlined. This lengthy and complex bill encompasses FVS (establishing someone with an identity), Facial Identification Service (for law enforcement comparative purposes), and FRAUS (looking for quality issues).

7.6. Self-Regulation by Multi-National Tech Companies

In addition to public action by states in the context of law enforcement, some corporations have taken action to restrict their own use of FRT. In June 2020, Amazon, IBM and Microsoft all stated that they would not sell any facial recognition technology to US police forces, amid increasing concerns about racial injustice in the US and the racial bias that has been found in facial recognition software. Amazon initially implemented a one-year moratorium on sales of its "Rekognition" product to police departments.[217] It announced in May 2021 that the moratorium would be extended indefinitely, although the existing platform is utilised by a number of unspecified federal agencies.[218] IBM's CEO wrote a letter to US law makers, stating that it will stop making general purpose facial recognition software altogether. The letter stressed that "now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies."[219] Similarly, Microsoft announced that it would not sell any FRT to the police until there was federal regulation around police use of the technology.[220] However, it appears this ban only applies in the US, as it is utilised by overseas, notably NSW Police.

However, it should be noted that these companies are not the top suppliers of facial recognition software to police departments in the US. Leading companies like Clearview AI, NEC, Ayonix, Cognitec and iOmnisicent all intend

[216] Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017) at [5.1].

[217] "Amazon extends moratorium on Police use of facial recognition software" *Reuters* (19 May 2021): https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

[218] *Facial Recognition Technology Report* United States Government Accountability Office (June 2021) at Page 12.

[219] IBM "IBM CEO's Letter to Congress on Racial Justice Reform" (8 June 2020) <ibm.com>.

[220] "Microsoft President Brad Smith says the company will not sell its facial recognition technology" *The Washington Post* (online ed, Washington DC, 12 June 2020).

to continue their relationships with United States police forces.[221] We note that the Draft AI rules being promulgated by the European Union are likely to be highly influential on tech company behaviour.

Notably, in November 2021, social media company Facebook announced that it would shut down its facial recognition system and delete the faceprint data of over 1 billion users. Media reports indicate that public concern (particularly after the leak of internal documents) and the settlement of an action under Illinois law relating to biometric data were relevant to the decision.[222]

7.7. Lessons from Comparable Jurisdictions – Key Points

- Other comparable jurisdictions are further ahead in deploying live automated FRT, but there are issues where deployment has preceded clear and transparent principles and rules.
- The impact of FRT has led to public concern, and in some cases backlash.
- Comparable jurisdictions are now looking to establish regulations and guidelines, and in some cases have banned or restricted certain high-risk applications of FRT.
- Action against FRT has come from a combination of individuals and activists, legislatures, courts, and self-regulation by tech companies.
- Police should continue to monitor comparable jurisdictions closely, and use the valuable opportunity to avoid errors made elsewhere.

[221] Julia Horowitz "Tech companies are still helping police scan your face" *CNN Business* (online ed, United States, 3 July 2020).

[222] ABC News 'Facebook to shut down facial recognition system and delete face print data of 1 billion users https://www.abc.net.au/news/2021-11-03/facebook-to-shut-down-facial-recognition-system/100589540

PART 8. FRAMEWORKS AND RECOMMENDATIONS

8.1. Spectrum of Use in a Policing Context

The basic operational aspects of collection, retention and comparison of facial images are used in a range of contexts. The technology patently has many uses and potential uses which, consequently, create a spectrum of risk in terms of impact on human rights.[223]

A key message is that there is a spectrum of use and impact of FRT in a policing context. Many people move immediately to thoughts of live automated FRT when the subject is mentioned, but it is important for Police to clearly distinguish the spectrum of use of the technology, both in internal and external guidance.

Through the development of the draft New Technology Framework, Police are already advancing structured decision-making and thinking around the risks of emergent/new technologies and ethical commissioning and governance processes.

Here, we categorise various aspects of FRT usage in a policing context which should be additional specific considerations layered on the draft New Technologies Framework.[224]

This risk framework is a starting point and should be read in conjunction with our analysis of the type of risk relating to each category of use case in the considerations section.

Classification of a use-case as low risk does not mean that lower levels of oversight over commissioning and governance should be exercised.

[223] Similar findings and principles have been set out in the international literature – See e.g. World Economic Forum, Interpol, UNICRI, Netherlands Police, A Policy Framework for Responsible Limits on Facial Recognition – Use Case-Law Enforcement Investigations – White Paper, October 2021 https://www3.weforum.org/docs/WEF_A_Policy_Framework_for_Responsible_Limits_on_Facial_Recognition_2021.pdf

[224] These principles are:

1. Necessity – there is a demonstrable need for Police to acquire the capability
2. Effectiveness – there is good reason to believe the technology will meet the need
3. Lawfulness – the proposed use is lawful
4. Fairness – possible data or use biases have been considered and risks mitigated
5. Privacy – impacts have been considered and risks mitigated
6. Security – data and information security risks have been considered and risks mitigated
7. Partnership – a te ao Māori perspective has been considered and affected communities consulted
8. Proportionality – individual, group and wider community impacts have been considered and any negative impacts are proportionate to the necessity and benefits
9. Oversight and accountability – policy, audit and reporting controls will assure that the technology is only used as intended
10. Transparency – appropriate information about the technology, its use, and how to challenge adverse outcomes will be publicly available

Attributes of Lower- Risk FRT Activities

- Consent-based FRT activities or services:
    - The consent should be opt-in rather than opt-out,
    - The individual clearly consents to and understands the storage and comparison of their facial image. However, we note that consent may be somewhat illusory,[225]
    - An alternative path must be provided (consent without alternative means does not make sense),
    - The use of FRT for decisions that have little gravity at an individual level (e.g. a quicker access to a service, internal security and authentication).
- One to One Verification
    - FRT used for comparing one image to another image where those images have been lawfully obtained under warrant or with consent, particularly where other factors are available to confirm the identity.
- Anonymised counting systems with data minimisation (e.g. footage is deleted immediately and only aggregated counts are displayed to users).

Attributes of Medium-Risk FRT Activities

- Staff that are making decisions based on FR output are appropriately trained and are aware of the limitations,
- Activity that involves information sharing between agencies – facial images are collected and stored by one agency, but are available for search and comparison by another agency,
- Retrospective analysis of lawfully obtained data with trained humans making final decisions based on the FR output,
- Private sector suppliers are involved, but this may be mitigated by a high degree of transparency and accountability in the contractual arrangements,
- One-to-many identity verification, particularly where the reference image databases draw from a wider variety of contexts,
- Anonymised demographic analysis of groups of people, where high-level statistics are made available to users with an understanding of the limitations of these tools,
- 'Isolated' use of live automated FRT at particular place and time ('controlled environment' where the system can be 'switched on and off') with data minimisation and privacy built into design (only the necessary amount of data collected, data deleted straight afterwards).

[225] Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880; and Nili Steinfeld "Situational user consent for access to personal information: Does purpose make any difference?" (2020) 48 Telemat Inform.

Attributes of High-Risk FRT Activities

- Decisions that have grave consequences for the individual, such as identification in criminal proceedings, requiring outputs to meet evidentiary standards,
- Particularly wide deployments that may affect people en masse, including use of OSINT data sources,
- Systems completely controlled by the private sector that provide data to Police without the same checks and balances as Police-owned and operated systems,
- Systems which transfer data overseas without necessary contractual arrangements (against losing control over data),
- Systems with low or uncertain accuracy, especially for subsets of the population,
- Systems that combine multiple technologies together,
- Activities that may affect Māori and Māori data sovereignty and require consultation
- One-to-many identification (i.e. searching for a match with an unknown person), particularly where the reference image databases draw from a wider variety of contexts,
- Making decisions in real-time based on FRT outputs (e.g. live response),
- Use of FRT on images or footage taken in public spaces,
- Systems that analyse the emotional state of people in an aggregated and anonymised way at the group or crowd level.

Attributes of Unacceptable Risk FRT Activities (at this point in time)

- Activities that could be used to track individuals, build or contribute/link to their detailed profile, discriminate against, recognise the person from the distance,
- Systems that are highly automated (human out of the loop) without the consent of individuals being subject to FRT,
- Unconstrained use of FRT by officers without appropriate governance controls or audit trails,
- Use of FRT or similar technologies to profile individuals on their mood/emotion/psychographic characteristics.

8.2. Recommendations

Recommendation 1 – Continue to pause any consideration of live automated FRT

We consider that live automated FRT/live biometric tracking is a high-risk activity which can have significant impacts on individual and societal interests. Its use is also likely to impact significantly on over-represented communities and vulnerable adults and youth.

It is significantly different to the taking of photographs or footage by Police in a public space and differs in speed and scale from an officer 'scanning' a crowd with their own human abilities.

Our review of the literature and the situation in comparable jurisdictions concludes that:

- ❖ There is no strong evidence base for effectiveness or cost benefit considerations,
- ❖ There are continuing concerns about accuracy and bias,
- ❖ Use is contrary to the principle of policing by consent and could be detrimental to community confidence and trust in Police,
- ❖ There is a strong likelihood of a backlash against surveillance which could impact public views on existing systems such as CCTV and established security partnerships.

It is important to note that we did not hear of any plans to consider or implement live automated FRT during our interviews, and there was general consensus from those with whom we spoke that the current state of the technology is not ready for use in New Zealand.

We also note that we consider retrospective FRT to be less risky as there is no element of live tracking. It may be an obvious point, but we would consider 'near real time' (within seconds or minutes) processing to be in the same category as 'live' FRT given the ability to take immediate action to apprehend the person.

We recommend that ***Police formally pause any consideration of deployment of live automated FRT*** (akin to Police Scotland's announcement) for a minimum time period and make a public statement or policy to that effect. This would reassure the community and help build trust that there are appropriate boundaries set on the use of FRT.

We do consider that Police have a duty to regularly review available technologies. However, we generally feel more comfortable with New Zealand Police remaining cautious about the adoption of this controversial technology, rather than feeling the need to be a technology leader in this space. Thus, ***Police should continue to monitor developments in the technology and use in comparable jurisdictions, but should not advance any***

consideration of deployment until at least the following conditions have been met:

- A clear purpose which is strictly necessary,
- The community has been appropriately consulted, particularly those most likely to be impacted,
- Less intrusive alternatives have been considered,
- Impacts on Māori, children and young persons have been considered and mitigated,
- Accuracy can be assured, particularly in the context of bias and discrimination,
- Oversight and governance are assured,
- Processes for redress and appeal for victims of misuse or errors have been developed.

Police should be open to the possibility that these conditions may never all be met contemporaneously.

Recommendation 2 – Review of collection and retention of facial images

Police access to databases of facial images is a necessary operation of any FRT system, including the lower risk usages of facial comparison/identity matching and retrospective analysis. Images collected now and, in the past, could form part of 'watchlists' were live automated FRT to be implemented in the future.

We acknowledge the following factors:

- The ABIS2 upgrade of the IMS is still in its implementation stage and a final set of business rules for the system have not yet been finalised,
- The IPCA and the Privacy Commissioner are conducting a joint review on police photography which is yet to report,
- Many similar organisations face similar challenges in managing large amounts of personal data of varying age and quality,
- While the law is clear on the deletion and retention conditions for formal images, there is much less regulation or guidance on the retention and storage of other types of facial images such as intelligence images,
- Merging or aggregation of Police-held repositories plus the ability to search using FRT would be a significant power, particularly as live AFR and analysis of existing CCTV footage becomes faster, cheaper and easier to implement.
- New Zealand lags other jurisdictions in having law, regulation and governance mechanisms for collection and retention of biometrics,
- We also consider that it is likely that there will be law reform and/or additional guidance in this area in the short to medium term, as the government advances issues such as the response to the Law Commission's review of the DNA legislation and work on digital identity frameworks.

In concert with these ongoing factors, ***we recommend that Police consider:***

- In parallel with the current work on business rules for the IMS system, consider the implementation of a set of rules for collection and retention of facial images across the various contexts including information/intelligence and already collected footage. We reviewed parts of Police instructions which cover some aspects of collection and retention.[226] We also sighted guidelines for collecting images at the roadside. Some of these guidelines are under review, and are likely to be updated after the Privacy Commissioner/IPCA review. We recommend that these are collated into a set of guidelines specifically on facial images,
- In developing and collating these guidelines:
  - Consider whether images of children and young persons (in categories which fall outside the formal image legislative regime in the Policing Act) should have special retention rules given the different principles applying to the youth justice system,
  - Consider whether indefinite retention of non-formal images aligns with other schemes for retention of biometrics (e.g. DNA retention periods, which are not uniformly indefinite). We heard that non-formal images do not get stored in the NBIO database. However, when the ABIS 2 upgrade to IMS is implemented, some suspect photos are proposed to be retained in a 'suspect database' where they remain 'unsolved'. This is not dissimilar to fingerprints and DNA who operate partitioned databases for crime scene samples (as these suspect images and unidentified fingerprints are). We note that the Law Commission's review of the DNA regime has made recommendations for significant reform of the rules on collection and retention of DNA, and retention rules for other biometrics should align with any new legislation in this area,
  - Consider whether retention policies align with the principles of the Clean Slate legislation, which provides for reintegrative responses for less serious offending,
  - Provide reporting on the ethnicity of those persons whose images are held (as with the DNA database) which then provides transparency for patterns in image collection practices,
  - Consider harm-based thresholds for use of facial comparison (e.g. serious crimes only),
  - Ensure that there are strong approval processes and audit trails around the collection and use of image data, with special consideration for the common use of mobile and smartphone devices,

[226] Photography (Forensic Imaging); CCTV guidelines – Crime Prevention Cameras CCTV in Public Places

- Consider ongoing education for officers to understand the principles for appropriate and inappropriate collection and use of images,
- Develop policies around the collection and use of OSINT data, and avoid connecting those sources to FRT systems.

Recommendation 3 - Continue to strengthen processes for ethical commissioning of technology

The trial of Clearview in early 2020 was a welcome catalyst for Police review of emergent/new technology. We acknowledge Police's work over the last 12-18 months in strengthening frameworks and processes for the commissioning of new technologies and the efforts to stocktake current technology uses.

The draft New Technology Framework (which we reviewed draft material from), the establishment of a New Technology Working Group and the establishment of the independent external panel on emergent technologies[227] are all important assurance mechanisms for new technology proposals. These mechanisms should make clear which individual within Police is held accountable for the use of technologies approved under these processes.

These frameworks provide a generic approach that would be applicable across multiple technologies and tools, leading to a consistent standard that can become common practice. Our considerations for FRT should inform any relevant applications or referrals to these assurance mechanisms.

Recommendation 4 – Ensure continuous governance and oversight of deployment

A robust commissioning process is an important assurance but there are also risks in the operation of a technology and scope creep or inappropriate use after commissioning. It is important that oversight processes are not only tied to procurement.

While we heard about the new and developing mechanisms for commissioning new technologies, we were less clear on the mechanisms that are in place to ensure that commissioned new technologies operate within their approved scope and adhere to any conditions around use.

For example, we heard that audit logs are used to monitor usage of community camera networks, but that these audit logs may not be regularly checked. Robust security and access controls are critical if Police are dealing with biometric information.

These governance mechanisms are essential before Police could consider any expansion of facial comparison systems or consideration of live FRT.

[227] New Zealand Police 'Advisory panel on emergent technologies' https://www.police.govt.nz/about-us/programmes-and-initiatives/police-use-emergent-technologies/advisory-panel-emergent.

Recommendation 5 – Upholding Te Tiriti in partnership with Māori

We note that neither of the researchers working on this report are Māori, and that this report is not a replacement for genuine engagement with Māori communities on the appropriateness of facial recognition in Aotearoa.

Commentators have suggested that facial image data represents individual and collective whakapapa.[228] We believe there may be an impact where a person has tā moko or moko kauae, which may make the facial image of particular importance in revealing personal information. There may also be further accuracy implications that disproportionately affect Māori.

Police data (including facial images) has been gathered through a system in which Māori are over-represented in apprehension, arrest and conviction. Independent oversight mechanisms that include Māori voices and apply appropriate ethical frameworks are essential.[229] Alongside social licence sits cultural licence, and different perspectives on rights (e.g. individual and collective) must be considered during technology assessments. Māori scholars and advocates have expressed concern over data sovereignty in the context of FRT,[230] particularly where suppliers are from other jurisdictions.

Documents on emergent technologies released under the Official Information Act 1982 show little evidence of consideration of Te Tiriti principles or potential disproportionate impact on Māori thus far, although this has been raised by the Expert Panel. We heard that Police have a range of networks and Panels for particular communities, and emergent technology issues should be canvassed broadly.

We recommend that:

- ❖ Disproportionate effect on Māori and accuracy and bias issues resulting from the over-representation of Māori in police data are considered a high risk in any considerations of use or future use of FRT.
- ❖ Invest into research alongside Māori to better understand the appropriateness and weaknesses of FRT systems, including accuracy and bias, in the Aotearoa New Zealand context.
- ❖ Conduct further and ongoing consultation with Māori scholars and community representatives to explore the cultural issues embodied in the collection, retention and comparison of facial images.

Recommendation 6- Transparency

A lack of transparency around the use of FRT or whether particular capabilities are in use or being considered is cause of public concern and speculation. We

[228] Meriana Johnsen "Police facial recognition discrimination against Māori a matter of time – expert" *RNZ* (online ed, New Zealand, 2 September 2020).

[229] See also the recommendations of the Law Commission: Law Commission *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara – Final Report (2020).*

[230] Te Mana Raraunga "Te Mana Raraunga Statement on Department of Internal Affairs facial recognition system procurement" (press release, 14 October 2020).

welcome the approach to release the stocktake of the Technology Capabilities List which is comprehensive and clear. This report and continuing proactive release of Privacy Impact Assessments and referrals to the Expert Panel is a welcome development and will help improve trust and comfort for stakeholders.

We recommend that Police consider:

- ❖ Continued proactive release of any use of FRT capabilities through the Technology List,
- ❖ Continued proactive release of Privacy Impact Assessments and broader assessments of impacts on human rights,
- ❖ Clearer public guidance on when a member of the public may be subject to FRT,
- ❖ Clearer public guidance on Police access to other databases,
- ❖ Formulation of a policy document on the use of FRT, [231]
- ❖ Transparency in releasing documentation around partnerships that Police have involving access to third party systems,
- ❖ Consider funding deliberative democracy processes around biometrics use, similar to the process run by the Ada Lovelace Institute in the UK.[232]

Recommendation 7 – Policy statement on surveillance in public places

Although our firm recommendation is that there should be a pause on any consideration of live FRT, we also consider that Police's public guidance on surveillance in public places should be more transparent. Although live FRT is not in use, Police surveillance activities in public places are the source of facial images that could later form watchlists for either retrospective analysis or use by third-party camera systems. The public need clearer guidance on the threshold between when Police are allowed to capture an image (particularly a facial image) and when a warrant is needed, to ensure confidence and trust. This is particularly important for legitimacy where Police are relying on common-law powers and 'third source authority'.

We note that the intelligence services in New Zealand have statements which discuss the impact of public surveillance (particularly camera/CCTV-based) that discuss the impact on an individual's rights and interests.[233] The

[231] See e.g. New York Police Department https://www1.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf; Detroit Police Department https://detroitmi.gov/sites/detroitmi.localhost/files/2019-07/FACIAL%20RECOGNITION%20Directive%20307.5_0.pdf; Michigan State Police https://www.michigan.gov/documents/msp/SNAP_Acceptable_Use_Policy_2016_03_07_533938_7.pdf; Indiana State Police https://secure.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf

[232] The Ada Lovelace Institute is an independent research institute investigating data and AI issues. They ran a consultative and deliberative process on biometrics during 2020: https://www.adalovelaceinstitute.org/project/citizens-biometrics-council/.

[233] Office of the Inspector-General of Intelligence and Security *Review of NZSIS use of closed circuit television (CCTV)* (June 2021) at 4-6.

development of publicly accessible policies which set out the principles which guide Police discretion in these circumstances would be an improvement.

We believe it is important to note that 'public spaces' are not limited to the physical world, but should also include online/digital open sources. Therefore, clearer policies around OSINT are necessary to give confidence that data collected in those contexts follows the same principles as data collected in physical public spaces.

Recommendation 8 – Implement guidelines for access to third party systems

As third-party camera systems become increasingly common, Police need clear rules around when it is appropriate to use them. The spectrum of potential use ranges from ad hoc requests for offline recorded footage, to ongoing agreements for access to live camera networks, to the use of third-party FRT systems to monitor for individuals on watchlists. Private sector use of FRT-enabled surveillance is likely to increase, particularly in the retail sector, especially as these services come 'baked-in' to vendor offerings.

There are considerable risks in Police accessing CCTV systems and running FRT directly, and some risk in contributing images to watchlists. Regardless, it is important that Police interactions with third-party FRT systems are well-governed and have audit logs to monitor use and to detect misuse. Collecting data on the frequency and type of use may also be helpful for understanding the effectiveness of these relationships and tools. In general, the use of a third-party system should be subject to the same guidelines and principles as Police systems.

Recommendation 9 – Embed a culture of ethical use of data in the organisation

While good governance and oversight at an organisational level is important assurance, individual staff and managers must be equipped with ethical frameworks to manage day to day issues (such where a private sector organisation offers use of a FRT system). This is particularly important where staff may be tempted to use their individual devices to take photos or videos, or to download tools onto their own devices. For example, it is currently physically possible for a Police officer to use their smartphone to take a video of a CCTV camera feed, and then run a FR check against a suspect on their own device (although this would not be considered admissible evidence). "Shadow IT" cannot be easily monitored or detected until it's too late. Police's ability to manage these devices will always be limited to devices owned by Police, and so an understanding of the underlying data ethics principles has to be instilled within all staff.

We heard that there is now an awareness of the availability of the Emergent Technologies workgroup as a point of contact for enquiries and assistance. We also heard that there is organisational culture work ongoing on the concept of ‘policing by consent’ and related legitimacy and trust frameworks. There may be ongoing training opportunities related to bias as well.

We recommend that Police consider:

- Developing ethical tools to deal with emerging situations – such as an offer of access to a third-party system or consideration of use of a system or tool where a system or tool is readily available to the public but not to Police,
- Add a module in recruit training, with key messages delivered at the time the device or access to tools are provided,
- Provide guidance on common scenarios relating to data privacy and the risks of inappropriate data usage,
- Embed messages with staff when they return for regular digital technologies and cybersecurity training.

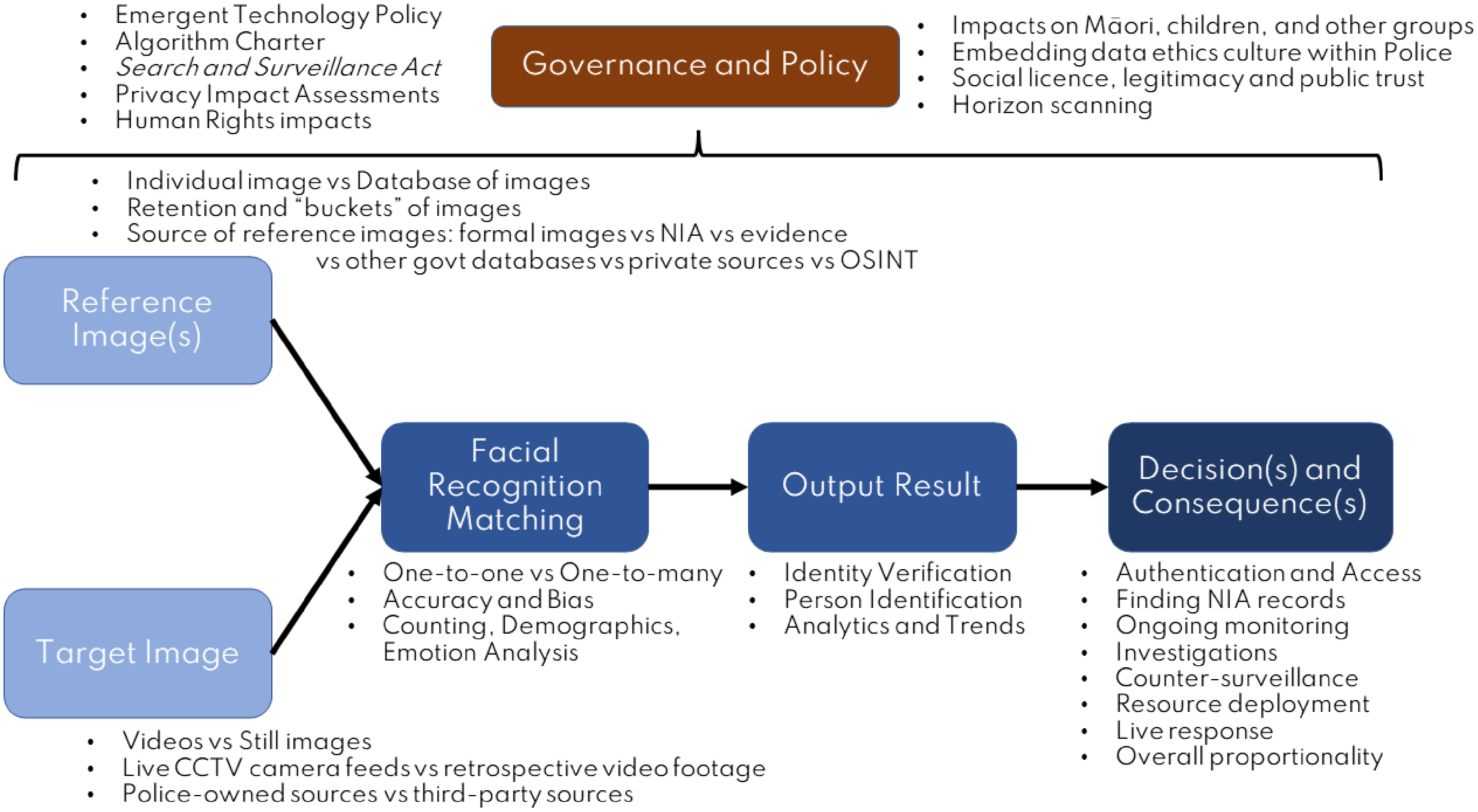
Recommendation 10 – Implement a system for ongoing horizon scanning

There are a number of technologies, including FRT, which have been under development for a long time but which have been generally considered too inaccurate for real-world deployment. However, as the technology continues to develop, the accuracy will improve and attitudes from stakeholders and the public will shift. Police should have an understanding of ‘how accurate is accurate enough?’ using measurable metrics so that they are not caught by surprise. There are other dimensions that also need to be understood for these technologies (e.g. ‘how effective is effective enough?’ and ‘how socially accepted is acceptable enough?’).

We recommend that Police consider:

- Developing a list of significant emergent technologies to monitor (e.g. facial recognition, emotion analysis, drones, robots, and others), particularly where they may be controversial and require the development of social licence,
- Adding resource to the Emergent Technologies workgroup to conduct ongoing Technology Assessment and provide monitoring of those technologies,
- Evaluating the applicability of existing policies and legislation towards these technologies to define the boundaries of what may be appropriate use by Police.

Facial Recognition Technology in Policing: Considerations



Governance and Policy

- Emergent Technology Policy
- Algorithm Charter
- *Search and Surveillance Act*
- Privacy Impact Assessments
- Human Rights impacts

- Impacts on Māori, children, and other groups
- Embedding data ethics culture within Police
- Social licence, legitimacy and public trust
- Horizon scanning

Reference Image(s)

- Individual image vs Database of images
- Retention and "buckets" of images
- Source of reference images: formal images vs NIA vs evidence vs other govt databases vs private sources vs OSINT

Target Image

- Videos vs Still images
- Live CCTV camera feeds vs retrospective video footage
- Police-owned sources vs third-party sources

Facial Recognition Matching

- One-to-one vs One-to-many
- Accuracy and Bias
- Counting, Demographics, Emotion Analysis

Output Result

- Identity Verification
- Person Identification
- Analytics and Trends

Decision(s) and Consequence(s)

- Authentication and Access
- Finding NIA records
- Ongoing monitoring
- Investigations
- Counter-surveillance
- Resource deployment
- Live response
- Overall proportionality

Facial Recognition Technology in Policing: Risk Framework

	Low Risk	Medium Risk	High Risk	Unacceptable
Attributes	• Opt-in • Clear consent • Alternative path available • Low-impact at individual level	• Trained staff in-the-loop making decisions • Information sharing between agencies • Private sector suppliers of data • Independently authorised	• Wide data sources (e.g. OSINT) • Third-party data sources without Police standards • Overseas transfers of data • High-impact at individual level • Inaccurate or biased systems • Combining multiple technologies	• Highly automated (human out-of-the-loop) • Unconstrained use without governance or audit trails
Example Applications	• One-to-one verification (with other factors available) • Authentication and Access • Anonymised counting with data minimisation	• One-to-many verification • Retrospective analysis • Anonymised demographic analysis of groups • Isolated live FRT in controlled environments	• One-to-many identification • Live response • FRT on footage from public spaces • Emotion analysis of groups	• Live person tracking using automated FRT • Profile building • Emotion analysis of individuals