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.

November 2021*

* The report was updated in March 2022 with updated footnoting and editorial corrections, which do not change the meaning or the recommendations.

TABLE OF CONTENTS

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 at 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 FRT equipped camera in a public space 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 to guide safe and effective use of algorithms and data analytics. The human oversight element is of particular relevance to FRT.
- 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 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 involved review of literature, legal reasoning, analysis of theoretical frameworks and stakeholder 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] The contribution of the co-authors on that report is gratefully acknowledged by both authors of this review.

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 **(**Hereinafter Lynch N, Campbell L, Purshouse J, Betkier M (2020))

[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 [3]

Facial recognition technology (FRT) is a collective term for technologies involving identification of an individual person based on an analysis of their facial features. An algorithm compares the features of a collected image with an already stored image.

FRT software takes digital facial images (from a camera or database of facial images) and carries out mathematical operations using geometrics to distinguish faces. The image may be manipulated by the system to the form in which the facial features can be recognised. The algorithm will extract geometric features that describe an individual. 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 against biometric templates previously collected and stored in a database.[4] The result of the comparison is particular to the use case. If a match occurs, the system may alert a human operator.

3.2. Principal Uses

3.2.1. *Verification*

Verification means the comparison of two biometric templates to verify an individual'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*

Identification means comparison of a person's biometric template to an existing database of images to find a 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 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] See Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 1.2 for a more detailed discussion.

[4] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341, at para 23.

3.2.3. *Analytics and Trends*

FRT can extract demographic information about an individual e.g. age, gender, or ethnic background. This is referred to as 'face analysis'[5] and often informs 'video analytics'. It cannot specifically identify an individual but if demographic factors ethnicity or age are inferred from an image and combined with other datasets (such as location data), it could result in the identification of a person.[6]

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[7], there are vendors who have incorporated these capabilities into their products.[8]

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.[9]

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 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

---

[5] Kawulok, M., Celebi, E. and Smolka, B. eds., 2016. *Advances in face detection and facial image analysis*. Springer.
[6] European Union Agency for Fundamental Rights (2019) *Facial recognition technology: fundamental rights considerations in the context of law enforcement* at p. 8.
[7] 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*.
[8] See for example, NEC and Realeye's partnership: https://findbiometrics.com/nec-realeyes-unveil-biometric-emotion-analytics-service-102303/.
[9] 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

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.[10]

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.[11] FRT can be distinguished from other biometrics (such as DNA, iris scans, fingerprints)[12] because an individual's face is generally visible in public.[13] Further, a facial image may be acquired at a distance without the subject person being aware. However, it still involves intrusion on a person's privacy interests. Ruhrmann considers that: [14]

> FRT …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…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…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.

[10] 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).
[11] Cross Government Biometrics Group (April 2009), Guiding Principles for the Use of Biometric Technologies. Available from the Department of Internal Affairs website.
[12] N Lynch, L Campbell, A Flaus and E Mok (2016) *The Collection and Retention of DNA from Suspects in New Zealand* (Wellington: VUP).
[13] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 1.4.
[14] H Ruhrmann (2019), *Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement* (Goldman School of Public Policy) at p. 73.

As Wiles (a former Biometrics Commissioner for England and Wales) comments:[15]

> …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…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 of England and Wales' decision in *R. (Bridges) v Chief Constable of South Wales Police*[16] a distinction was drawn between "intrusive" and "non-intrusive" means of collecting personal data. Live automated FRT was categorised by the Court as "non-intrusive" so did not exceed the limits of the police's powers under common-law.[17] The High Court found that the distinction between intrusive and non-intrusive depended on whether there was an actual intrusion upon an individual's rights in their residence or an intrusion on a person's bodily integrity .[18] The Court found that only these 'physical' intrusions on a person's rights required statutory authorisation. Commentators have noted 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."[19]

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.

---

[15] *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, 2020), para. 37. Available from https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2019

[16] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341.

[17] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.5.

[18] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at para. 74.

[19] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.5.

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 ethnicities and genders.[20] There are multiple potential causes, but it is primarily attributed to a lack of diversity in the datasets that are used to train 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.[21] 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.[22] 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.[23]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. In the state of Michigan, an incorrect FRT match led to an innocent man being arrested, detained, photographed and fingerprinted. According to Kashmir Hill, the case is likely to be "the first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm."[24] Protesters in the city of Detroit called for police to halt the use of FRT due to low accuracy rates.[25] There has also been concerns about police use of FRT against Black Lives Matter protestors, [26] and reportedly FRT was deployed to identify people who took part in a riot at the US Capitol in 2021.[27]

---

[20] Joy Buolamwini, Timnit Gebru *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018).
[21] Michele Merler, Nalini Ratha, Rogerio S. Feris, John R. Smith *Diversity in Faces* (arXiv:1901.10436, April 2019).
[22] Patrick Gother, Megan Ngan, Kayee Hanaoka (2019) *Face Recognition Vendor Test Part 3: Demographic Effects* (NISTIR 8280,), and Paul Marks "Can the Biases in Facial Recognition Be Fixed; Also, Should They?" *Communications of the ACM* (64(3) p 20-22, March 2021).
[23] Kate Kaye "This little-known facial-recognition accuracy test has big influence" *International Association of Privacy Professionals* (online, 7 January 2019).
[24] Kashmir Hill "Wrongfully Accused by an Algorithm" *The New York Times* (online ed, New York, 24 June 2020).
[25] M. L. Elrick (2020) "Detroit protesters take fight against facial recognition tech to city leaders' homes" *Detroit Free Press*.
[26] A. Geogiou (2020) "Black Lives Matter Activist Hunted by NYPD Facial Recognition Technology" *Newsweek*.
[27] J. Vincent (2021) "FBI used facial recognition to identify a Capitol rioter from his girlfriend's Instagram posts" *The Verge*.

The National Institute of Standards and Technology (NIST) is a division of the United States' Federal Department of Commerce.[28] Through its Facial Recognition Vendor Tests, it publishes technical evaluation of a range of commercially available facial recognition algorithms (including verification and identification systems). These tests demonstrate considerable gains in accuracy across the last ten years due to rapid advances in computational power, increases in the breadth of image databases and advances in machine learning algorithms.[29] FRT accuracy rates are likely to be on a trajectory of improvement. Nonetheless, in contexts where collecting good quality facial images is difficult or confidence thresholds are deliberately raised, the rates of error remain meaningfully above zero.[30] The performance metrics of FRT systems and their underlying algorithms are highly dependent on the context, nature of the task and the definition of success.[31] For instance,[32]

> "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)… 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 accuracy of FRT software may also be affected by variables such as gender, ethnicity and age of the individuals whose data has been collected.[33] NIST's reports in the United States found significant variability in performance depending on demographic factors.[34] The geographical location of the algorithm development also significantly impacted performance.[35] As examples, algorithms developed in the United States showed higher numbers of false positive matches for people with West/ East African or East Asian ancestry in a system using "one-to-one" matching, while Chinese-developed algorithms had higher accuracy rates on East Asian faces.[36]

Significantly, the tests demonstrated that women of African-American ethnicity had higher rates of false positives in identification contexts. As Lynch et al note, "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

---

[28] See https://www.nist.gov/. See also Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.
[29] P Grother, M Ngan and K Hanaoka (2018) *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* (NISTIR 8238, November 2018).
[30] NIST: FRVT Quality Assessment, available at pages.nist.gov/frvt/html/frvt-quality.html.
[31] See footnote 29.
[32] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.
[33] See footnote 20 and J Buolamwini (2019) "Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces" *Medium*.
[34] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.
[35] See footnote 9.
[36] See footnote 9 at 2.

as a result of an incorrect match against a database".[37] NIST's tests noted that some algorithms were not as affected by demographic factors. To identify and appropriately manage the risk of disproportionate effect or lack of accuracy against certain groups, it is imperative to assess the accuracy of the algorithm in the context for its proposed use-case.

In Aotearoa New Zealand, the use or proposed use of algorithms trained on datasets derived from other populations gives cause for concern about accuracy rates, particularly for Māori. Relevantly, research has suggested that facial tattoos could disrupt FRT systems.[38] Indigenous data ethics commentator Karaitiana Taiuru has expressed concern that FRT use would cause 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."[39]

A literature search found no studies on the accuracy of FRT 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.[40] 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.

Overall, as Lynch et al note: "assessments of FRT accuracy are heavily context dependent and challenging".[41] 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

[37] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.
[38] Buttle, H. and East, J., 2010. Traditional facial tattoos disrupt face recognition processes. *Perception*, *39*(12), pp.1672-1674.
[39] M Johnsen (2020) "Police facial recognition discrimination against Māori a matter of time – expert" *Radio New Zealand.*
[40] Department of Internal Affairs (2020), "Privacy Impact Assessment: Full Report - One Time Identity"
[41] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.

time (e.g. lighter in winter, darker in summer) which could influence the accuracy of FRT systems.

Assessments of an FRT system's accuracy must consider technical aspects such as accuracy rates; resolution and quality of the image, and the thresholds for sensitivity, in the context of the proposed use-case, for example verification or identification.[42] The scale and the location of the proposed deployment of FRT is also highly relevant. Case by case assessment is essential when assessing appropriate use and the governance and management systems required.[43]

Where accuracy concerns can be significantly mitigated, this does not rule out the need for broader assessments of whether deployment is appropriate and will meet objectives. For example, could the FRT system be 'spoofed'[44] or whether actions by the public like wearing face-coverings or hats could mean the objectives of the use-case are defeated.[45]

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."[46]

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[47].

---

[42] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.
[43] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.2.
[44] Parkin, A., & Grinchuk, O. (2019). Recognizing multi-modal face spoofing with face recognition networks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*. An example would be using a photo image of a person's face to unlock a smartphone.
[45] A report on use of FRT in policing in Wales reported that caps and face coverings impacted the performance of a one-to many identification system. See Davies, Bethan, Martin Innes, and Andrew Dawson. *An evaluation of South Wales police's use of automated facial recognition*. Universities' Police Science Institute, 2018.
[46] Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. Crime Science, 9(1), 1-13.
[47] Phillips, P.J., Yates, A.N., Hu, Y., Hahn, C.A., Noyes, E., Jackson, K., Cavazos, J.G., Jeckeln, G., Ranjan, R., Sankaranarayanan, S. and Chen, J.C., 2018. Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. Proceedings of the National Academy of Sciences, 115(24), pp.6171-6176.

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.[48]

3.6.1. Public Sector

FRT is currently used, and being contemplated to be used, in verification of identity processes across a range of contexts, most notably at the border.[49] These use-cases are principally in the 'verification' category –comparing an individual's biometric template with another, but 'identification' (one to many) use cases are also apparent.[50] Biometric data (including facial images) may be used to make or guide decisions.[51] Detection of identity fraud is the principal use-case.

In 2018, the Department of Internal Affairs signed a ten-year agreement with Enterprise Services New Zealand (the New Zealand arm of DXC Technology, a company based in the United States) which public bodies and private organisations may join.[52] The system is now operational, with the aim of preventing fraud. The system uses FRT to compare photos for new and renewal passport applications with a database of facial images in order to identify those who have multiple identities in the system.

The agreement shows that specified agencies will have automatic access to the products contained in the agreement and others can request to join. Local government bodies can opt in to the agreement and private organisations can make application to join. This saves cost, and also avoids the visibility of the regular tender processes. There is clearly an intent to expand the use of biometrics across the public sector.[53]

3.6.2. Private Sector

Banking – The use of FRT technology in identity verification procedures is widespread in the New Zealand banking context. ASB has a pilot initiative to use FRT for customer identification.[54] Similarly , Westpac New Zealand offers customers facial image matching technology as a means of customer

---

[48] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 1.
[49] Lynch N, Campbell L, Purshouse J, Betkier M (2020), at section 1.5.1.1.
[50] For example, in passport fraud detection. Lynch N, Campbell L, Purshouse J, Betkier M (2020)
[51] Immigration Act 2009, s 30.
[52] P Pennington "Government facial recognition tech deal offers wide access" *RNZ* (online ed, New Zealand, 12 October 2020) quoting Chief Executive of DIA and Enterprise Services New Zealand (2018) *Master Syndicated Agreement: relating to the syndicated procurement of Facial Recognition Services*.
[53] Above.
[54] ASB Bank, "ASB to make 'selfie' ID a reality" https://www.asb.co.nz/documents/media-centre/media-releases/asb-to-make-selfie-id-a-reality.html

identification for new accounts.[55] Heartland Bank is using FRT software in its procedures for remote AML compliance.[56] OriginID sells a FRT-enabled system to accountants and law firms for the same reason.[57] Paymark is testing the use of FRT in payments systems.[58] The Bank of New Zealand uses FRT in its mobile banking application.[59]

Retail security – retailers are increasingly utilising FRT for security and loss prevention purposes. A person was apprehended by security in a Dunedin supermarket May 2018 after he was incorrectly identified as a suspected shoplifter.[60] New World would not disclose whether individual stores were using the system to identify suspects from previously collected watchlists of suspected shoplifters. Media coverage demonstrated political and regulatory concerns around the accuracy of the technology, demonstrating a perceived need for regulatory development.[61] Public opinion varied.[62]

Other large retailers (such as the Warehouse and Mitre-10) have also been reported to be trialling FRT- based security systems.[63] During the Alert Level 3 restrictions in the Auckland region in August 2020, a New World store reportedly requested that customers briefly remove their face covering upon entry to the premises in order for the FRT system to function.[64]

Casinos were one of the first businesses to adopt FRT and use it widely. Casinos use FRT for security: identifying and alerting staff to known cheaters or high value clients when they arrive on the premises.[65] Casinos use FRT in harm minimisation systems. Problem gamblers can self-identify and ask to be placed on an exclusion list, and the system can exclude underage people.[66]

Pandemic related use: FRT is being utilised in a number of ways in the current Covid-19 pandemic.[67] Relevantly, this may accelerate societal acceptance of

---

[55] See https://www.originid.co.nz/westpac-bank
[56] Heartland Bank "Acceptable Forms of Identification and Address Verification" https://www.heartland.co.nz/Uploads/Documents%20and%20Forms/acceptable-forms-of-identification-and-address-verification.pdf
[57] See https://www.originid.co.nz/
[58] A Nadkarni (2019) "Paymark experimenting with facial recognition at Spark's 5G innovation hub" *Stuff.co.nz.*
[59] BNZ "Help & Support - Mobile Touch ID, Fingerprint Login and Face ID" <bnz.co.nz>.
[60] G Block (2018) "Supermarket chain Foodstuffs admits facial recognition technology used in some stores" *New Zealand Herald.*
[61] M Reidy (2018) "PM slams in-store face-scanning tech" *Dominion Post*.
[62] M Rilkoff (2018) "Recognition is reasonable on the face of it" *Stuff.*
[63] G Block (2020) "The quiet creep of facial recognition systems into New Zealand life" *Stuff*.
[64] C Marriner (2020) "New World store with facial recognition cameras reverses mask policy" *New Zealand Herald*.
[65] O. Cole (2020) "Facial Recognition Technology Spreads across New Zealand Casinos" *Casino Guardian*.
[66] G Block (2020) "The quiet creep of facial recognition systems into New Zealand life" *Stuff*.
[67] S Cha (2021) "S. Korea to test AI-powered facial recognition to track Covid-19 cases" *Reuters*.

FRT, in the context of restrictions on liberty and other freedoms in pursuit of public health and welfare. FRT is useful as unlike contact methods of collecting biometrics (such as fingerprint pads or iris scanning) it is non-contact.[68] Technology suppliers are marketing FRT systems for pandemic -related use-cases. In Australia, two states are trialling FRT applications to manage people in home quarantine.[69]

Airline security – FRT can provide a touchless experience moving through check-in, identity checks and security. Covid-19 has accelerated this implementation, with many airlines implementing FRT based systems.[70]

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.

[68] Van Natta, Meredith, et al. "The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic." Journal of Law and the Biosciences (2020).
[69] B 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/
[70] J Snow (2020) "Nano needles. Facial recognition. Air travel adapts to make travel safer" *National Geographic*.

PART 4. COLLECTION AND RETENTION OF FACIAL IMAGES

Examining collection and retention of facial images by Police[71] 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.[72]

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:[73]

- Offender images – estimated at 1.85 million images derived from the records of 800,000 individuals, with a projected increase of 50,000 per year,
- Suspect images – estimated increase of 7,500 images per year,
- Firearms licence images – an average of 245,000 images are in the system at a time. Projected to be 10,000 renewals per year, and an increase of 9,500 new images per year,
- Images of those placed on the child sex offender register – there are 1,500 images at present with a yearly addition of 300 new records,
- Images from FRT processes – projected to be 15,000 additional records yearly,

[71] 'Police' in this report is taken to mean New Zealand Police.
[72] 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
[73] 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.

- Photo line-up production images – 12,000 current images, and a projection of 15,000 additional records yearly
- Images of scars, marks, and tattoos - 2,500 current records, with a projection of 30,000 additional records per year.

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* authorises Police to collect biometrics (which includes photos) from suspects in lawful custody. There is a statutory requirement to dispose of these images as soon as practicable when:

- There is a decision not to proceed with the charge,
- The person has been tried but has been acquitted.

The images may be retained after the following events:[74]

- The person receives diversion,
- The person is convicted,
- 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

Facial images of firearms licence holders held by Police number close to 250,000, which is a significant percentage of the population.[75] 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.[76]

---

[74] Policing Act, s 34A.
[75] New Zealand Police (2020) *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment*, p. 4.
[76] 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.[77] 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.[78] 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,[79] 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.

[77] New Zealand Police: Technology Capabilities List July 2021, p. 17
[78] Above.
[79] 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 several mechanisms to allow agencies to exchange information. Police have current information sharing agreements with other agencies, particularly the Department of Internal Affairs which administers the legislation which governs passports and citizenship. These agreements cover a range of identity information sharing provisions, not limited to facial images.[80]

This agreement allows agencies to exchange information to identify individuals in particular circumstances:

- Where biometric data has been acquired from a person detained in relation to an offence,[81]
- There is good cause to suspect, an intention to charge, and identification is required for the summons,[82]
- Returning offenders who have had biometric data acquired from them.[83]

These agreements were implemented after the Smith case – where a person under Corrections supervision successfully applied for a passport and escaped to another jurisdiction without authorities being alerted.[84]

A Police press release states that the agreement allows "…24/7 access to passport and birth information, making it easier to identify a person police are taking enforcement action against." [85] The legislation requires agencies to publicly report instances of using the agreement. Police report using the system up to 250,000 times over the year's reporting period.[86] Queries are mainly to Immigration New Zealand: 112,380 from the OnDuty app, including for suspects/offenders identity 82,078 times. 252,228 queries were from the desktop application.

[80] New Zealand Treasury (2019) *Impact Summary: Improvements to the accuracy and timeliness of Police information regarding name changes, deaths and non-disclosure directions*.
[81] Policing Act 2008, s. 32.
[82] At s 33.
[83] Returning Offenders (Management and Information) Act 2015.
[84] Enhancing Identity Verification and Border Processes Legislation Act 2017.
[85] New Zealand Police (2019) "Improvements to information sharing between DIA, the Registrar-General, Births, Deaths and Marriage and Police".
[86] New Zealand Police (2020) *Annual Report 2019/20*, p. 145.

These totals include all enquiries, many of which will not involve facial image identification. However, the scale of use suggests use of the system is a routine inquiry. We heard that there are internal guidelines for when images of people can be accessed in this context. Whenever a user accesses data through this process, they will need to select a reason from a drop-down field in the system, and this is then recorded in the Police Annual Report in the relevant section which reports activity under the *Enhancing Identity Verification and Border Processes Legislation Act 2017.*

The New Zealand database of driver licences is operated by Waka Kotahi. 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.

Unlike other information sharing agreements, the Privacy Commissioner does not have legislative oversight powers over the identity information sharing agreement[87] or the law enforcement information sharing agreement.[88]

4.7. Horizon Scan of Possible Developments in Biometrics Regulation

Currently, collection, retention, comparison and matching of facial images by Police is regulated and guided by a complex combination of legislation, regulation and internal policy. Additionally, the common law position on photography and recording in public spaces does not countenance the technological capabilities currently available.

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 joint review of search and surveillance in 2021 noted that "a consistent approach to all biometric information may be considered

[87] Part 10A of the former Privacy Act 1993 and Part 7 (2) of the current Privacy Act 2020.
[88] Part 11 of the former Privacy Act 1993 and Schedule 5, Part 7 subpart 3 Privacy Act 2020 and Schedule 4

desirable" but qualified that DNA has a higher level of personal information compared to other types of biometric data.[89]

- The Privacy Commissioner set out a position paper on biometrics which was released in 2021.[90]
- 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.[91]
- The Law Commission Final Report on DNA (released in late 2020) noted:[92]

> …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…we recommend that the Government considers the adequacy of existing oversight arrangements in the fields of biometrics and forensic science.

A case study of a regulator in a comparable jurisdiction, is the Biometrics Commissioner role in Scotland, who has established a Code of Practice for biometric data use (encompassing facial images) in policing.

The legislation in Scotland 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 combination with other information…to establish the identity of an individual."[93]

The functions of the Scottish Biometrics Commissioner are to:

- Review law, policy and practice relating to collection, retention, use and disposal of biometric data by Police Scotland,
- Keeps the public informed and aware of powers and duties related to biometric data (e.g. how the powers are used and monitored, and how the public can challenge exercise of these powers)

[89] New Zealand Law Commission/Ministry of Justice (2017) *Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012* at 2.38.
[90] Privacy Commissioner (2021) Office of the Privacy Commissioner position on the regulation of biometrics.
[91] Lynch N, Campbell L, Purshouse J, Betkier M (2020), Recommendation 11.
[92] New Zealand Law Commission (2020) *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara* – Recommendation 45.
[93] Scottish Biometrics Commissioner Act 2020, s 23(1) and (2).

- Monitor the impact of the Code of Practice and raise awareness of the Code.

- 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.[94]
- 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, retention, storage, 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.

[94] Cross Government Biometrics Group (2009) *Guiding Principles for the Use of Biometric Technologies for Government Agencies.*

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 police use of FRT 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 current system for image management (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 scars, marks and tattoos (SMTs).

The system will not be freely available for access, except 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.[95] 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.

[95] 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.[96] 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.

[96] 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

Clearview AI was briefly tested in a non-operational environment in early 2020. Internal advice was that if Clearview was contemplated to be used on an ongoing basis for investigations, a Privacy Impact Assessment and formal review of legality was vital. 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.[97] 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

[97] 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.[98]

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-

[98] 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.

party FR systems as they would do their own. For example, if Police decide to 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 people visited and the time the people spent at the station's counter. [99] 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

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

of these technologies, potentially separate to policy on FR specifically. We 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 uses/ potential uses of FRT in the policing context in 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.

Before the case of *Hamed,* [100] it was commonly considered that Police video surveillance was lawful because it was not prohibited by legislation or the common law.[101] This was the prevailing view in *Ngan*, *Fraser* and *Gardiner*.[102] Similarly, under the legislation governing search and surveillance, police surveillance in public spaces is lawful and no warrant is required unless there is trespass.[103] In *Lorigan* (a case concerning a surveillance device with night-vision capabilities in a public place) held the Police's actions were lawful as there was "no statutory or common-law prohibition and it would not have been unlawful for a citizen to do".[104] Notably, the minority view in *Hamed* was that the surveillance was unlawful, even where there was no trespass.[105] This view (which we agree with) is that the police differ from individual citizens and should have lawful authority before doing something, as opposed to an individual citizen who can do anything that she or he is not prohibited by law from doing.

Another issue is whether the use of a camera with FRT capability 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 the *Bridges* case did not rule on this point, but did not note that a video surveillance with FRT capability had a higher level of intrusiveness when compared to ordinary video surveillance. [106]

A number of cases in this jurisdiction have considered whether video camera surveillance can be considered a "search". In *Hamed,* it was said that surveillance in a public space did not constitute a "search" as there was no intrusion by the state on the individual's reasonable expectation of privacy. But a distinction was drawn between what a human could observe and additional technical capabilities such as infra-red capability. [107] In the case of *Lorigan* (discussed above), the Police were using a video camera with night-vision equipment for surveillance. The installation was with the consent of the landowner, and the camera's view was equal to that which a member of the public walking the street would have seen. The Crown accepted that this activity constituted a 'search' for the purposes of s. 21 of the *Bill of Rights Act*, similar to the majority in the *Hamed* case.[108] In *Lorigan*, the Court said (applying *Ngan* and *Hamed*) that the test for a "search" was whether the police

[100] *Hamed v R* [2011] NZSC 101.
[101] For an English law perspective see J Purshouse (2020) "Facial Recognition Technology, the Metropolitan Police and the Law" Policing Law Blog
[102] R v *Ngan* [2007] NZSC 105, *R v Fraser* [1997] 2 NZLR 443, *R v Gardiner* (1997) 15 CRNZ 13.
[103] Search and Surveillance Act 2012, s 46; Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016); and Law Commission/Ministry of Justice (2017) *Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012*.
[104] *Lorigan v R* [2012] NZCA 264, para. 29.
[105] *Hamed v R* [2011] NZSC 101, para. 47.
[106] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, paras 85-89.
[107] *Lorigan* at para. 17 and *Hamed* at para 167.
[108] At paras 15 – 16.

surveillance was an intrusion into the individual's reasonable expectation of privacy. In *Lorigan*, the video surveillance was considered to be a search as the night-vision capability meant that it differed from conventional video surveillance, and captured data that could not be acquired by the human eye. This is salient as a FRT equipped camera has capabilities of a speed and scale above that of a human.

Key Point – Warrantless use of a FRT equipped camera device in a public space 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, by means of the Informational Privacy Principles ("the principles".[109] The principles regulate collection, processing, use and disclosure of personal information either by private companies or by public authorities. Facial biometrics are personal information, so any collection or processing of facial images must comply with the principles.

Individuals cannot use the courts to enforce the principles[110], except for the right under principle 6(1) to know whether or not a public sector agency holds any personal information about a individual and the right to access this information. People who have a complaint about interference with privacy must first raise it with the body concerned. The next step is a complaint to the Privacy Commissioner, with an appeal to the Human Rights Review Tribunal.[111]

There is nothing in the Privacy Act 2020 that prohibits FRT use by public or private bodies, as long as it complies with the principles.[112] Relevant from the principles are: that information collection is necessary and for a lawful purpose

[109] Privacy Act 2020, s.22.
[110] Privacy Act 2020, s. 31
[111] Part 5 of the Privacy Act 2020.
[112] Privacy Commissioner (2021) *Office of the Privacy Commissioner position on the regulation of biometrics.*

connected with the function or activity of that agency, that the agency must collect personal information directly from the person (subject to some qualifications), that the agency must take reasonable steps to notify the person that the information will be collected, that the agency must collect the information in a reasonable and fair manner that does not unduly intrude on the person, that the agency must hold the information securely, that the agency must permit people to access and correct their information, that the agency must ensure the information is accurate, that the agency must destroy the information when no longer required, and that there are restrictions on the use and disclosure of unique identifiers.[113] A new principle, relating to disclosure of personal information outside New Zealand was established by the Privacy Act 2020.

Unlike in other jurisdictions, New Zealand's legislation does not recognise a concept of sensitive data (such as biometrics) that deserve additional safeguards. [114] The Privacy Commissioner's guidance on biometrics does recognise the particular sensitivity and warns of the consequence of misuse or data breaches.[115] 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.[116]

In a broader sense, individual and collective conceptions of privacy may vary heavily based on age, cultural background and factors individual to that person, as well as general societal perceptions of privacy. [117] Consideration of appropriate use of FRT must be mindful of the varying concepts of privacy understood across te ao Māori and those of various ethnic and religious backgrounds. Even where significant public benefit accrues from FRT use, this will affect individual privacy interests, which different people will experience differently dependent on their background and characteristics. [118]

Privacy is a nebulous and culturally loaded concept that is difficult to define. In analysing appropriate use of FRT, the key concepts are:

---

[113] A biometric template might be considered a unique identifier under the Privacy Act but as Lynch et al 2020, section 5.5. state this would be out of line with other identifiers such as IRD numbers, and further, a better interpretation would be that the biometric template is not assigned but intrinsic to the individual.
[114] Privacy Commissioner (2021) Office of the Privacy Commissioner position on the regulation of biometrics.
[115] Privacy Commissioner (2021) Office of the Privacy Commissioner position on the regulation of biometrics.
[116] 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.
[117] New Zealand Law Commission/Ministry of Justice (2016) *Review of the Search and Surveillance Act 2012*, at para 2.34.
[118] C Garvie and L Moy (2019) "America Under Watch: Face Surveillance in the United States" .

- Informational privacy – generally defined as the right to have control over the collection, storage and use of your personal information,[119]
- Spatial privacy – the right to be free from intrusions on bodily integrity and private spaces such as the residence.[120]

FRT has the greatest potential impact on a person's informational privacy. As discussed earlier a person's face is unique to that person and the biometric template which a FRT system processes is clearly personal information. In the case of Hamed, the court recognised that individuals have the right to be protected from intrusions into private spaces .[121] 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."[122]

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.

6.4. Human Rights

Human rights mean the rights and freedoms that individuals are entitled to. In New Zealand, our human rights arise from domestic and international sources, including 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.

FRT may impact human rights in the following ways: [123]

- The right to freedom of thought, conscience and religion; the right to freedom of expression; Freedom to assemble and to freely associate (as an example where FRT is used to monitor lawful protest activity),

[119] Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. The handbook of information and computer ethics, 131-164.
[120] Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *U. Pa. J. Int'l L.*, *38*, 483.
[121] *Hamed v R* [2011] NZSC 101 at para. 11.
[122] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.5.
[123] European Union Agency for Fundamental Rights (2019) *Facial recognition technology: fundamental rights considerations in the context of law enforcement*.

- The right to free movement (for instance, at borders or in public spaces where a person does not want to be monitored),
- The right to be free from discrimination (e.g. where lack of accuracy or bias is contained in FRT systems),
- 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).

Human dignity may also be impacted by FRT according to the European Union, and any collection of biometrics must respect the dignity of the person. [124] People may be reluctant to be in public places if there is increased FRT surveillance, and automation of surveillance may lead to increased interactions with law enforcement.

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'.[125] Scholars note that children's 'particular vulnerability … relative to adults might make

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

them … natural candidates for heightened protections from facial recognition technologies.'[126]

Children and young people are entitled to the same human rights protections as adults. Additionally, children and young persons have a specific human rights treaty (the Children's Convention[127]) which recognises their vulnerability, requires that their best interests are paramount and that they are not discriminated against. Tamariki and rangatahi Māori are likely to be most impacted by any deployment of FRT.[128] In the context of youth justice, the Children's Convention recognises that children must be treated differently due to their vulnerability and capacities. Human rights bodies are increasingly recognising that children's rights (particularly freedom of expression and privacy) are impacted by surveillance by new technologies. [129]

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.[130] 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.[131]

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

---

[126] Barrett, Lindsey. 'Ban Facial Recognition Technologies for Children - and for everyone else'. *B.U. J. SCI. & TECH. L.*, Vol. 26 (2020): 2
[127] 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.
[128] Ministry of Justice (2020) *Youth Justice Indicators Summary Report.*
[129] Keen, C., 2020. Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy. New Media & Society 1- 20. MV de Azevedo Cunha (2017)"Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy."
[130] 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
[131] 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

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.[132]

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 peaceful protest and assembly, and this typically takes place in public spaces.[133] Contemporary social movements like the School Strike for Climate have demonstrated the power of children's participation in the public space.[134] If FRT was to be used to monitor protests in public spaces, this could impact children's rights to 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

We have already discussed the technical aspects of discrimination and bias in FRT, but there are additional considerations in the societal context of Aotearoa New Zealand. The principles of Te Tiriti o Waitangi require that the specific

[132] 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.

[133] A Daly (2016) *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).

[134] Tattersall, A., Hinchliffe, J., & Yajman, V. (2022). School strike for climate are leading the way: how their people power strategies are generating distinctive pathways for leadership development. Australian Journal of Environmental Education, 1-17.

impact on Māori must be considered.[135] Māori are disproportionately impacted by the criminal justice system, at all stages from apprehension to imprisonment. Though they are 16% of the population, "Māori are 38% of people proceeded against by Police, 42% of people convicted, and 51% of people in prison."[136] The influencing factors are many, including the effects of colonisation,[137] the mono-cultural nature of the criminal justice system, biased decisions and the disproportionate impact of adverse life events for Māori.[138]

As Lynch et al note, "this disproportionate effect means that those whose images populate facial image databases created by the Police, are likely to be disproportionately of Māori ethnicity."[139] There is no breakdown by ethnicity available for the Police image database but since the DNA database is known to contain disproportionate numbers of profiles from Māori, inferences about disproportionality may be drawn. If FRT is used, this will enable intensified policing and surveillance of Māori. 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. [140]

As Lynch et al note "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".[141] As Garvie et al note , a FRT system "does not see race, sex, orientation or age."[142] This fact does not mean that FRT systems can prevent bias in policing outcomes.[143] As noted earlier, there is evidence that FRT systems have lesser accuracy on some faces, and ethnicity and gender are relevant factors.

---

[135] Waitangi Tribunal (2017) *Tū Mai Te Rangi! The Report on the Crown and Disproportionate Reoffending Rates*.
[136] Hāpaitia te Oranga Tangata: Safe and Effective Justice (2019) "Our justice system needs to change".
[137] See footnote 135 above.
[138] *Ināia Tonu Nei – Hui Māori Report - The time is now: We lead, you follow* (2019).
[139] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.8.
[140] 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.
[141] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.7.
[142] Garvie, C., Bedoya, A. and Frankle, J., 2016. The Perpetual Line-Up. Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology,p. 57.
[143] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.7.

As noted in the introductory section, there are particular concerns around accuracy in relation to tā moko and moko kauae.[144] 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, which is likely to occur in an image database unless there is regular data cleaning linked to the Births, Deaths, and Marriages system.[145] Death notices are currently received by the Biometrics team in Police, and the related NIA profile is marked as deceased, but not expunged.

As Lynch et al note:[146]

> 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 principles hold that indigenous peoples have authority over individual and collective data (including biometric data),[147] Te Mana Raraunga (Aotearoa's Māori data sovereignty group) have expressed concern on the implications of the all-of-government FRT agreement for Māori, notably that the "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".[148] There may be particular issues where Police amass a collection of images of predominantly Māori faces.

---

[144] 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.
[145] We acknowledge and thank Karaitiana Taiuru for his time and consideration in making these points in consultation with the authors.
[146] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.7.
[147] Tsosie, R. (2020). The legal and policy dimensions of Indigenous Data Sovereignty (IDS). In *Indigenous Data Sovereignty and Policy* (pp. 204-225). Routledge; Kukutai, T., & Taylor, J. (2016). Data sovereignty for indigenous peoples: current practice and future needs. In *Indigenous data sovereignty: Toward an agenda*. ANU Press.
[148] Te Mana Raraunga (2020) "Te Mana Raraunga Statement on Department of Internal Affairs facial recognition system procurement"

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 for Aotearoa New Zealand

New Zealand is the first country to establish standards for algorithm usage by government and public sector agencies.[149] The Charter sets principles for public sector agencies using algorithms to make or guide decisions which agencies can publicly commit to. The term "algorithm" is undefined, with a focus on the impact of the decision made using the algorithm rather than the complexity of the algorithm itself.

The Algorithm Charter requires:[150]

- Transparency in algorithm use,
- Respect for the Treaty partnership,
- Algorithms must have a focus on people,
- Algorithms must use data that is fit for purpose,
- Safeguard privacy, human rights and ethics,
- Retain oversight by humans.

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

The Government Chief Data Steward and the Privacy Commissioner have jointly issued guidelines for public sector use of data and analytics:[151]

- Must consider and demonstrate, positive societal benefit from collection and use of public data,
- Transparency is essential for accountability and supports collaboration, partnership, and shared responsibility.
- Data is a powerful tool, but analysis has inherent limitations to predict and describe results.
- Analytical processes should inform human decision-making but should never completely replace human decision making
- Ensure data is fit for purpose – using the right data in the correct context can improve decision-making and analytical models and avoid potentially harmful outcomes.

[149] C Graham-McLay (2020) "New Zealand claims world first in setting standards for government use of algorithms" *The Guardian.*
[150] *Algorithm Charter for Aotearoa New Zealand* (2020).
[151] Privacy Commissioner and Chief Government Data Steward. (2018). Principles for the Safe and Effective Use of Data and Analytics.

- Focus on people – keep the people behind the data in mind and consider how to protect people against misuse of data.

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.[152] The independent panel has also reviewed the report and provided further advice.

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 safe use of algorithms and data analytics. The human oversight element is of particular relevance to FRT.
- 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.

[152] 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

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,[153] 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.

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[154] but without much verifiable data such as statistics on outcomes.[155]

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.[156] Evaluations of trials of automated live FRT across the United Kingdom have found problems with inaccuracy and false

[153] 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

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

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

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

positives.[157] Body worn cameras showed some positive effect on the crime rate but no evidence for FRT.[158]

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,
- 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): [159]

- "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".

[157] B Davies, M Innes and A Dawson, "An Evaluation of South Wales Police's Use of Automated Facial Recognition," (September 2018).; P Fussey and D 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.

[158] J Park and M Pang, 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

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

In New Zealand Police's Briefing to the Incoming Minister, the Commissioner defined the concept as: [160]

> 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.

It is likely that FRT deployment could affect the legitimacy of Police, specifically if use is non-consensual or there is a lack of transparency.[161] As Lynch et al caution:[162]

> "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. 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 regarded by the public as unfair or discriminatory, or there is widespread use without clear legal authorisation, there is a danger that this will affect police legitimacy.[163] It is important that the public can assess that use is lawful and justified.

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

6.10. Social Licence/Public Opinion

Gulliver et al have defined the concept of social licence as: [164]

> "…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."

[160] New Zealand Police 'Briefing to the Incoming Minister of Police – Part A – Overview of Portfolio' November 2020
[161] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.7.
[162] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 4.7.
[163] 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.
[164] Gulliver, P., Jonas, M., McIntosh, T., Fanslow, J. and Waayer, D., 2018. Qualitative research: Surveys, social licence and the integrated data infrastructure. Aotearoa New Zealand Social Work, 30(3), pp.57-71, p. 60.

Social licence can never override fundamental protections such as consent, human rights and privacy but can be a relevant consideration in development of law and policy.[165] Social licence can change rapidly (such as in the aftermath of the Christchurch terror attack[166]). The current global Covid-19 pandemic may also be changing attitudes to restrictions on privacy and liberty for public welfare and safety reasons.[167]

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 public opinion on, and comfort with, the use of FRT in policing. We qualify this discussion that there is little or no insight into indigenous peoples' or minority groups, or any studies specifically on New Zealand.

In studies of public opinion across the UK, US and Australia, a majority of a sample of the public surveyed[168] were comfortable with state use of FRT for law enforcement, if there was appropriate regulation of the use. In the UK study, almost half of the sample believed that there should be the option to opt out of FRT surveillance.

In the UK and Australian studies, those who were uncomfortable with police use of FRT cited infringement on privacy, normalisation of surveillance, lack of

---

[165] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 3.4.
[166] Crothers, C., & O'Brien, T. (2020). The contexts of the Christchurch terror attacks: social science perspectives. Kōtuitui: New Zealand journal of social sciences online, 15(2), 247-259.
[167] Lewandowsky, S., Dennis, S., Perfors, A., Kashima, Y., White, J. P., Garrett, P., ... & Yesilada, M. (2021). Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom. Plos one, 16(1), e0245740.
[168] A Smith (2019) "More than half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly" (5 September 2019) Pew Research Center, DM West (2018) "Brookings survey finds 50 percent of people are unfavorable to facial recognition software in retail stores to prevent theft" Brookings; Ada Lovelace Institute (2019) *Beyond face value: public attitudes to facial recognition technology*. Available at https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/; and Roy Morgan (2017) "Australians not concerned about use of mass facial recognition technology".

opt-out or consent mechanisms and lack of trust in the police to use the technology ethically as their reasons.

In the Australian study, those who were comfortable using FRT cited views in support such as having nothing to hide, that security a vital protection against terrorists and to catch the 'bad guys,' prioritising security over privacy and believing that societal expectations around privacy were loosening.

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. [169]

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%).[170] 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.[171] 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'.[172]

In the United Kingdom, fans who became aware of the use of live automated FRT at football matches began to wear face coverings and displayed signage in protest. South Wales Police used live automated FRT in early 2020 at a soccer match between Cardiff City and Swansea City. This was criticised by supporters' groups and civil liberties campaigners as being stigmatising.[173]

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

[169] 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
[170] 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.
[171] 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.
[172] 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/>
[173] S Morris (2020) "Anger over use of facial recognition at south Wales football derby" *The Guardian.*

ethicists and more – and debated on the opportunities and risks posed by biometric technologies.

Some relevant themes from the findings include:[174]

- 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 license would have to be carefully gauged, including genuine engagement with diverse communities.

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.[175]

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.

[174] 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.
[175] 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 in policing 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.[176]

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 (South Wales Police,[177] the Metropolitan Police,[178] and public private partnership schemes[179]). Under the Protection of Freedoms Act 2012, there is a statutory basis for the collection and retention of DNA and fingerprints but not other biometrics such as facial images, gait analysis, or voiceprints. There are no laws governing the use of FRT in the jurisdictions of the United Kingdom. Scholars have argued that police use of FRT may not have lawful basis as it is not specifically authorised by legislation .[180] The Law Society for England and Wales doubts that widespread use of FRT meets the Data Protection Act's test of strict necessity because of problems with accuracy because the technology is "highly unproven".[181] The police view is that the legal

[176] 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.
[177] Big Brother Watch (May 2018), *Face Off: The lawless growth of facial recognition in UK policing* Available at https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf
[178] National Physical Laboratory and Metropolitan Police Service (February 2020), *Metropolitan Police Service Live Facial Recognition Trials*, available at https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf
[179] Dan Sabbagh "Facial recognition technology scrapped at King's Cross site" *The Guardian* (online ed, United Kingdom, 2 September 2019).
[180] Purshouse, J., & Campbell, L. (2019). Privacy, crime control and police use of automated facial recognition technology. *Criminal Law Review*, *2019*(3), 188-204 and Fussey, P., Davies, B., & Innes, M. (2021). 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology*, *61*(2), 325-344.
[181] Michael Veale (2019) *Algorithms in the Criminal Justice System* (The Law Society of England and Wales,) at 42.

basis is sufficient, on a combination of data protection legislation, codes of practice for surveillance and general common-law principles.

7.1.2. *The Bridges Decision*

The city of Cardiff was the location for the first judicial review of police use of live automated FRT in a public space. South Wales Police (SWP) had been using a mobile camera van to run a FRT equipped camera with a 'watchlist'. SWP has received a large government grant to run tests of FRT for policing. Bridges (a civil liberties campaigner) challenged the legality of SWP's use of FRT on the basis of contravention of the Human Rights Act 1998, the Data Protection Act, and that the decision to use the technology was not in line with the Equality Act 2010.

The Divisional Court refused Bridges' application for a judicial review to rule SWP's use of FRT unlawful.[182] On appeal, the Court of Appeal ruled that the finding that the use of live automated FRT was 'in accordance with the law' was an error. The Court discussed whether the guidance and regulation of the technology was accessible and predictable and enough to prevent 'overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights'.[183] The Court found that statutory authorisation was not necessary, but that there was insufficient regulation under the data protection legislation, the code of practice for surveillance camera use and SWP's own policies to guide discretion on the parameters of the 'watchlist' and the locations where FRT could be deployed. [184] This finding suggest that if there were sufficient guidelines and policies, that this would mean deployment would satisfy 'in accordance with the law' requirement of Article 8(2) (which provides for the right to respect for private and family life). The Court held that SWP's deployment of FRT was a proportionate interference with the right to respect for private and family life. The Court overturned the original finding that there was sufficient data protection impact assessment and held that the SWP failed 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."[185]

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 and Wales. We summarise some main points here, but this is an area worth monitoring.[186] We particularly note that the College of Policing is working on

[182] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341.
[183] *Beghal v Director of Public Prosecutions* [2015] UKSC 49, [2016] AC 88 at [31] and [32] per Lord Hughes.
[184] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [96].
[185] Above at [199].
[186] Purshouse, J. and Campbell, L., 2021. Automated facial recognition and policing: a Bridge too far?. *Legal Studies*, pp.1-19.

Authorised Professional Practice guidelines on the use of the technology, which were not yet available at the time of writing.[187]

Bodies such as the Biometrics and Forensics Ethics Group[188] and the Surveillance Camera Commissioner[189] have issued guidelines which are relevant for the use of FRT in policing. These are useful and can be cited in court, but an individual may not take a complaint on the basis of contravention of these guidelines, nor do they affect admissibility of evidence.

The Information Commissioner's Office provides guidance for police 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 level of intrusion,
- Police forces 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."[190]

London Policing Ethics Panel has proposed a framework to guide trials of emerging technology by policing (which is directly relevant to FRT. The Panel suggests four principal considerations: serving the public; robust trial design; respect for equality, dignity and human rights; and addressing concerns and outcomes.[191]

The House of Commons Science and Technology Committee in July 2019 reiterated its recommendation from a 2018 Report, that live automated FRT should not be deployed until concerns over the technology's effectiveness and potential bias have been fully resolved.[192]

---

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

[188] Biometrics and Forensic Ethics Group (2019) *Ethical Issues arising from the police use of live facial recognition technology – Interim Report* (Facial Recognition Working Group).

[189] Surveillance Camera Commission (2019) *The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems: Section 33 of Freedoms Act 2012*.

[190] London Policing Ethics Panel (2019) *Final Report on Live Facial Recognition* at p. 8.

[191] Above.

[192] 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].

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."[193] 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:[194]

> 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."[195]

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.[196] 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:

- 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.

---

[193] *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>.
[194] At paragraph 8.
[195] At paragraph 9.
[196] *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).

- 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 live FRT should be created.
- Collaborative use of live FRT should be authorised by a senior police officer.

7.2. Scotland

Unlike other jurisdictions in the United Kingdom, Scotland has a moratorium on police use of live FRT. A strategic plan called Policing 2026 did include a proposal to trial live FRT,[197] but there was immediate criticism from politicians. The Justice Sub-Committee on Policing found that there was evidence that the live FRT software discriminated against females and those from ethnic minority backgrounds; there was no justification for investment in FRT; that prior to any decision to deploy automated live FRT, an 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 FRT would be a major departure from the principle of policing by consent.[198]

Police Scotland's response was that live FRT was not in use or planned to be used, that it would ensure safeguards were in place before deployment, and agreed that the impact of its use should be understood fully before it is introduced.[199]

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.

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:

---

[197] Police Scotland (2017) *Policing 2026: Our 10 Year Strategy for Policing in Scotland* at pages 39 and 43.
[198] Justice Sub-Committee on Policing (2020) *Facial recognition: how policing in Scotland makes use of this technology*. SP Paper 678 1st Report, 2020 (Session 5).
[199] Duncan Sloane (2020) quoted in the above report,

- 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.[200]
- 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."[201]
- 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 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:[202]

---

[200] 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

[201] Draft regulation, at para 18

[202] 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

> 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.[203] 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

A team at Georgetown Law Center on Privacy & Technology (led by Clare Garvie) has analysed use of FRT by law enforcement [204] FRT is used widely in the US by federal, state and local police, generally for identification of those who refuse to give their details or are incapable of doing so. Police can photograph a suspect person and run an immediate FRT search through a system in the patrol car.[205] Police forces are using FRT to search databases of suspect and offender images or databases of driver licence photos to generate a list of potential matches. A 'hot list' can be created, which will automatically be matched against real-time video surveillance or already-collected footage, and can issue an alert where there is a match.[206] Driver licencing bodies can compare new applications for licences to existing facial images in the database, alerting to fraudulent use of images or identity theft.[207]

Some jurisdictions have already placed significant constraints on use of FRT. Both Oregon and New Hampshire have banned FRT analysis of police body-

[203] 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
[204] Garvie, C., Bedoya, A.M. and Frankle, J., 2019. The perpetual line-up. Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology (Garvie et al).
[205] Garvie et al, at p. 10.
[206] Garvie et al, at p. 12.
[207] Garvie et al, at p. 12.

worn camera footage,[208] Maine and Vermont have placed limits on FRT analysis of drones used by police,[209] Massachusetts is the first state to pass a comprehensive statutory regulation scheme for law enforcement use of FRT.[210] Michigan does not allow retention of facial images or FRT matches from those who are acquitted or have not had charges laid.[211]

In 2019, the city of San Francisco (then followed by the cities of Oakland and Berkeley) stopped any use of FRT by police and other agencies under the city's jurisdiction. This includes any use of data derived from external FRT systems.[212] In 2020, the city of Portland, Oregon prohibited any public or private use of FRT.[213] A hiatus has been imposed in a number of US states: in 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.[214] 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.[215]

Maine has passed the strongest anti-facial recognition laws in the country which[216] "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. The Georgetown Law Centre has produced a comprehensive set of recommendations for ethical use of FRT in policing While these

---

[208] Or Rev Stat § 133.741(1)(b)(D); and NH Rev Stat Ann § 105-D:2(XII).
[209] Me Rev Stat Ann, title 25 § 4501(5)(D); and Vt Stat Ann, title 20 § 4622(d)(2).
[210] K Hill (2021), "How One State Managed to Actually Write Rules on Facial Recognition" *New York Times*.
[211] Mich Comp Laws Ann § 28.243(7)-(8). See Garvie et al, p. 35.
[212] D Lee (2019) "San Francisco is first US city to ban facial recognition" *BBC News*.
[213] R Metz (2020) "Portland passes broadest facial recognition ban in the US" *CNN Business.*
[214] Connor Hoffman "State Sentate to vote on facial recognition moratorium bill" *Niagra Gazette* (online ed, Niagra Falls, 21 July 2020).
[215] 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>.
[216] *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/

recommendations arise in the US legal context, the recommendations are relevant to other jurisdictions. The most salient recommendations include:

- FRT searches should not be permitted unless there is an individualised suspicion of offending,
- Databases of facial images used for FRT should not include acquitted people or those whose charges have been discontinued or dismissed,
- Speculative searches of the driver licence database should only be allowed pursuant to a court order,
- Searches of driver licence databases should be confined to investigation of serious criminal offending,
- Live FRT surveillance should be confined to significant events which threaten life and should be authorised by a court order,
- FRT should never be used to surveill people on the basis of race, ethnicity, religion or political views,
- Any use of FRT should be reported to the public and have sufficient governance and audit procedures
- Any state funding for FRT systems should be contingent on transparency, oversight and accountability
- Until there is statutory authorisation, halt FRT searches of state driver licence and ID card databases,
- Establish publicly available policies on use of FRT, which have statutory backing,
- Ensure that FRT systems have maximum accuracy through careful use of procurement and governance processes.
- Have sufficient governance in place to ensure accuracy – such as certified face examiners, procedures to minimise racial bias, such as internal audit procedures.

7.5. Australia

Police forces across Australia's states and territories are reported to use FRT, but it is difficult to obtain information and statistics on use.[217] Various law enforcement agencies, including Australian Federal Police and state police in Victoria, South Australia and Queensland have been found to use Clearview AI despite initial police denials.[218] As previously discussed, Clearview uses FRT on a database of publicly available images such as public social media profiles.[219] Like in England and Wales and Aotearoa New Zealand), the legal position in Australian jurisdictions is that if law enforcement is not specifically prohibited from using FRT, no statutory authorisation is required.

[217] N Daly and A Dickson (2020) 'Facial surveillance is slowly being trialled around the country' *ABC News*.
[218] J Goldenfein (2020) 'Australian police are using the Clearview AI facial recognition system with no accountability' *The Conversation.*
[219] J Goldenfein (2020) 'Australian police are using the Clearview AI facial recognition system with no accountability' *The Conversation.*

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[220]. 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.

In 2017, a federal -level agreement on Identity Matching Services was signed between the states and territories.[221] This agreement is contingent on legislation to govern exchange of facial images and other identity data, for a range of purposes, including policing and national security.

The Identity Matching Services have a number of components, including a document verification service, a face verification service (involving one-to-one FRT matching to verify identity), a face Identification Service (one-to-many matching to identify a known person or ascertain whether a person has multiple identities in the system), One Person One Licence Service "a narrowly focused check, on a constrained one-to-many basis, of facial images within the National Driver Licence Facial Recognition Solution"; a facial recognition analysis utility service enabling each state or territory's driver licencing authority to carry out biometric matching, and the identity data sharing service.[222]

Agencies with access to face identification services may use it only for certain purposes, mainly related to safety and security.[223] The private sector does not have access to FRT-related services 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.[224] No other FRT related services will be made available to the private sector.[225]

Part 8 of the Intergovernmental Agreement foreshadows 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 will exercise ministerial oversight of the Identity Matching Services".

---

[220] Byron Kaye "Australia says U.S. facial recognition software firm Clearview breached privacy law" (4 November 2021) Reuters <reuters.com>.
[221] Council of Australian Governments (2017) Intergovernmental Agreement on Identity Matching Services , Australian Government Department of Home Affairs (2019) *Privacy Impact Assessment: Law Enforcement, Crime and Anti-Corruption Agency Use of the Face Matching Services, NFBMC (v.1.0)*.
[222] Council of Australian Governments (2017) *Intergovernmental Agreement on Identity Matching Services* (part 4.
[223] At [4.21].
[224] At part 5.
[225] At [5.5].

Concerning monitoring of the agreement, there is a memorandum of understanding between the Office of the Australian Information Commissioner and the Attorney General's Department on the National Facial Biometric Matching Capability,[226] setting out the role of the Information Commissioner in relation to its role of assessing and advising the Attorney General in relation to FRT. While the primary focus appears to be in relation to funding the purpose of the 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".[227] Beyond this, each agency must enter into a separate agreement on data sharing and a separate memorandum of understanding with the Attorney-General's Department, setting out the terms and safeguards.

The Federal *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 discussed above. This lengthy and complex bill encompassed facial verification services, facial identity services and addressing quality issues. It lapsed at the dissolution of Parliament.

7.6. Self-Regulation by Multi-National Tech Companies

Suppliers of FRT have acted to restrict their own use of the technology. In mid-2020, Amazon, IBM and Microsoft announced a halt to their supply of FRT to law enforcement in the US. This was a reaction to protests about racial injustice in the US criminal justice system, and specifically concerns about bias and disproportionate impact of FRT. Amazon initially implemented a one-year moratorium on sales of its "Rekognition" product to police departments.[228] 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.[229] IBM informed legislators that it would cease development and supply of FRT systems and software, stating that it was appropriate to have "a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies."[230] Tech supplier

[226] Office of the Australian Information Commissioner (2017) *MOU in relation to National Facial Biometric Matching Capability.*
[227] Council of Australian Governments (2017) *Intergovernmental Agreement on Identity Matching Services* at para 5.1.
[228] "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/
[229] *Facial Recognition Technology Report* (2021) United States Government Accountability Office at page 12.
[230] L Hirsch (2020) 'IBM gets out of facial recognition business, calls on Congress to advance policies tackling racial injustice' *CNBC*. https://www.cnbc.com/2020/06/08/ibm-gets-out-of-facial-recognition-business-calls-on-congress-to-advance-policies-tackling-racial-injustice.html

Microsoft also announced a moratorium on supply of FRT to law enforcement until federal regulation was developed. [231] However, it appears this ban only applies in the US, as it is utilised by overseas law enforcement, notably NSW Police.

These tech companies are not the top suppliers of FRT to US law enforcement. Suppliers such as Clearview AI, NEC, Ayonix, Cognitec and iOmnisicent continue to supply FRT to law enforcement.[232] 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.[233]

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.

[231] L Magid (2020) 'IBM, Microsoft And Amazon Not Letting Police Use Their Facial Recognition Technology' *Forbes*.
[232] L Fenier and A Palmer (2021) 'Rules around facial recognition and policing remain blurry' *CNBC*. https://www.cnbc.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html
[233] 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

FRT has a range of use-cases, which "create a spectrum of risk in terms of impact on human rights".[234]

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.[235]

These risk categories use some aspects of the risk matrix first published in *Facial Recognition Technology in New Zealand – Towards a Legal and Ethical Framework*, but our updated framework is tailored to the policing context.

---

[234] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 7.3. 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

[235] 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

Those attributes which were first published in that report appear in quotation marks.

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.

Attributes of Lower- Risk FRT Activities[236]

- 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",[237]
  - "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,

[236] Lynch N, Campbell L, Purshouse J, Betkier M (2020), section 7.3. Those attributes which were first published in that report appear in quotation marks.
[237] Andreotta, A.J., Kirkham, N. and Rizzi, M., 2021. AI, big data, and the future of consent. *AI & Society*, pp.1-14.

- "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)."

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 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[238]

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"[239].

[238] As recommended by Lynch N, Campbell L, Purshouse J, Betkier M (2020).
[239] Lynch N, Campbell L, Purshouse J, Betkier M (2020), recommendation 8.

- 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.[240] 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:
  - Reflect on whether facial images which have been collected from children and young people (in categories which fall outside the formal image legislative regime in the Policing Act) should have special retention rules since separate legislative principles govern the youth justice system,
  - Consider whether indefinite retention of non-formal images is in line with other contexts where biometric data is retained. For example, statutory periods for retention of DNA are variable based on the offence and the offender. 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,
  - As recommended in the Lynch et al report, consider whether retention policies for facial images are in line with the Clean Slate statutory regime, which allows expungement of criminal records for less serious offending,[241]

[240] Photography (Forensic Imaging); CCTV guidelines – Crime Prevention Cameras CCTV in Public Places
[241] Lynch N, Campbell L, Purshouse J, Betkier M (2020), recommendation 11.

- As recommended in the Lynch et al report, align with the DNA regime in providing publicly available data on the ethnicity of those from whom facial images are collected,[242]
- 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,
- 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[243] 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

[242] Lynch N, Campbell L, Purshouse J, Betkier M (2020), recommendation 11.
[243] 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.

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.

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.

Māori experts suggest that facial images represents individual and collective whakapapa.[244] Where a person has tā moko or moko kauae, the facial image contains additional personal and collective information. There may also be further accuracy implications that disproportionately affect Māori.

Personal information (such as facial images) is collected by Police in the context of a criminal justice system where Māori are appear disproportionally in apprehension, arrest and conviction statistics. Independent governance mechanisms that have appropriate representation of Māori and assess against culturally appropriate ethical frameworks are crucial.[245] Alongside social licence sits cultural licence, and different perspectives on rights (e.g. individual and collective) must be considered during technology assessments. Māori experts have expressed concern over data sovereignty in the context of FRT,[246] particularly when those companies supplying the technology are based overseas.

Documents on emergent technologies show little evidence of consideration of the principles of Te Tiriti principles or potential disproportionate impact on Māori, although this has been raised by the Expert Panel. We heard that Police

[244] M Johnsen (2020) "Police facial recognition discrimination against Māori a matter of time – expert" *Radio New Zealand News.*
[245] The Law Commission has made relevant recommendations in the DNA context - Law Commission (2020) *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara – Final Report.*
[246] Te Mana Raraunga (2020) "Press release: Te Mana Raraunga Statement on Department of Internal Affairs facial recognition system procurement" Available at https://www.temanararaunga.maori.nz/nga-panui

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.
- As was recommended in the Lynch et al report, conduct further and ongoing consultation with Māori scholars and community representatives to fully explore any potential cultural issues related to the collection, retention and comparison of images of faces.[247]

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 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, [248]

[247] Lynch N, Campbell L, Purshouse J, Betkier M (2020) at section 7.3.

[248] 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

- 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.[249]

Recommendation 7 – Policy statement on FRT 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 at present, 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 can capture an image (particularly a facial image) and when a warrant is required , 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.[250] The 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 involving collection of facial images 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.

[249] 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/.
[250] Office of the Inspector-General of Intelligence and Security *Review of NZSIS use of closed circuit television (CCTV)* (June 2021) at 4-6.

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.

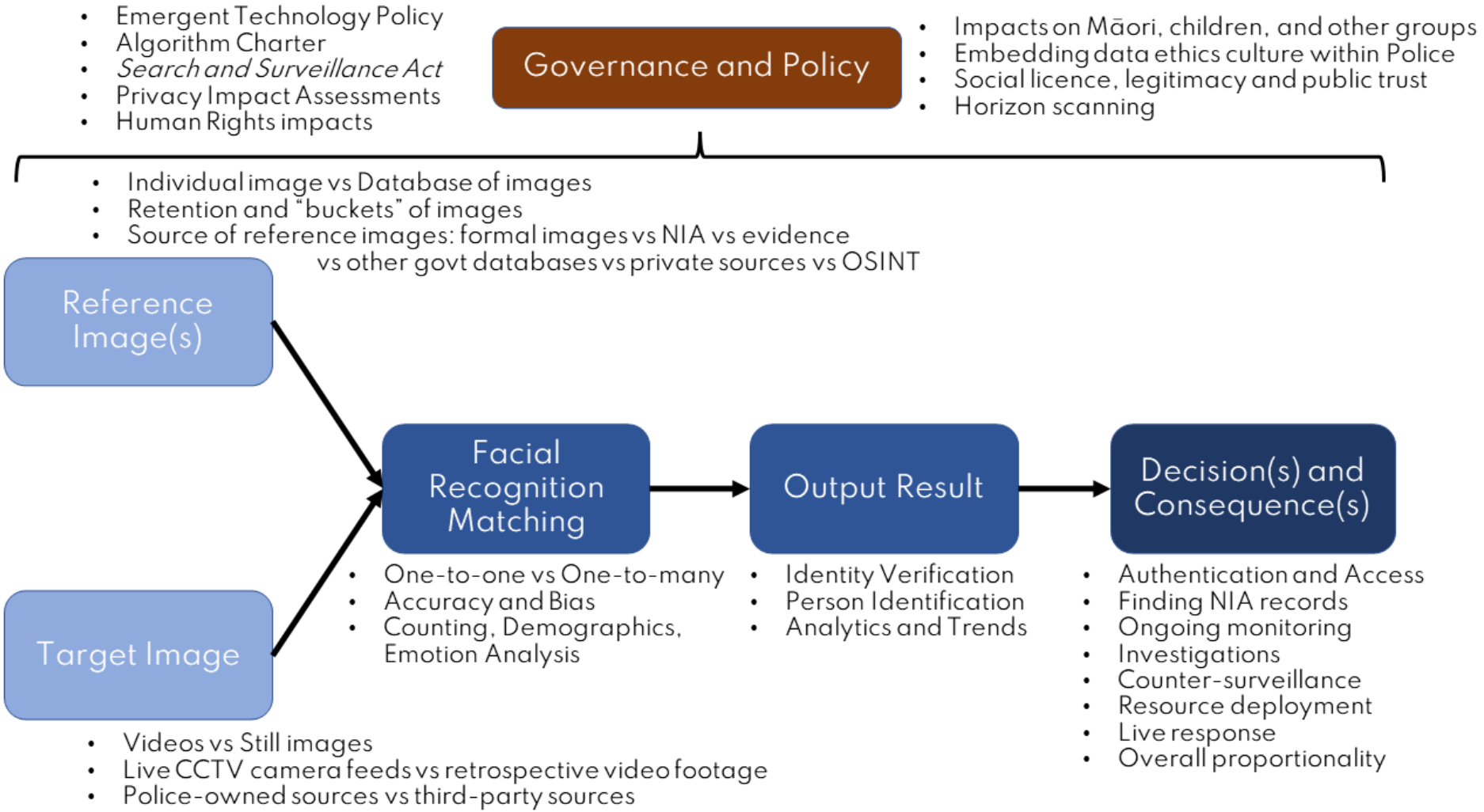
Recommendation 10 – Implement a system for ongoing horizon scanning

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



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