FACIAL RECOGNITION TECHNOLOGY IN NEW ZEALAND

TOWARDS A LEGAL AND ETHICAL FRAMEWORK

The Law Foundation NEW ZEALAND
SUPPORTING INDEPENDENT LEGAL THINKING.

Nessa Lynch, Liz Campbell, Joe Purshouse, Marcin Betkier

Facial Recognition Technology in New Zealand
Towards a Legal and Ethical Framework

Design: Jo Kinley, Hullaballoo Design

The Law Foundation NEWZEALAND
SUPPORTING INDEPENDENT LEGAL THINKING.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Many people contributed to this work.

We acknowledge the funders. The Law Foundation, through its Information Law and Policy Project, provided the grant which made this project possible. Thank to Lynda Hagen and Richman Wee in particular, as well as the Trustees of the Law Foundation.

The Victoria University of Wellington Faculty of Law also provided support.

Our research and editorial assistants – Stephen, Liesbet and Anna were essential to the project.

Allison Kay was invaluable in keeping financial and other reporting on track.

Participants at the workshop in October 2019 provided valuable insights and feedback.

Many thanks to Sharelle Kooyman from the Faculty of Law who organised the workshop and associated activities with her usual calm and efficiency.

The ideas were tested at several conference presentations and seminars; thank you to those participants.

Several colleagues generously gave their time to look over drafts of sections. A number of journalists and other researchers generously shared Official Information Act requests and other information. All errors are of course our own.

This is an area of technology, law and regulation which moves rapidly. Our report was generally finalized in October 2020, but we were able to incorporate some newer material in our recommendations section, up to the publication date of late November.

Author Biographies

Associate Professor Nessa Lynch is based at the Faculty of Law, Victoria University of Wellington. Her scholarly expertise is in criminal justice processes and sentencing, especially youth justice, and she has published and presented nationally and internationally in these areas.

Previous work in the area of biometrics includes leading a Law Foundation funded three-year project examining the collection and retention of DNA from suspects, and she served on the expert advisory group which advised the Law Commission on the review of the *Criminal Investigations Bodily Samples Act*. She is a Member of the Data Ethics Advisory Group which provides ethical review of use-cases for data in the public sector.

Associate Professor Lynch is particularly interested in the intersections between academic research and policy, and has spent time on secondment at the Ministry of Justice. She has consulted for a range of government and non-governmental organisations, internationally and New Zealand, particularly in youth justice reform.

Professor Liz Campbell is the inaugural Francine McNiff Chair of Criminal Jurisprudence at Monash Law, having previously been Professor of Criminal Law at Durham University, UK. She is adjunct professor at Queensland University of Technology School of Justice and University College Cork. Professor Campbell is an expert in corporate crime, organized crime, corruption, and biometric evidence.

Professor Campbell is an appointed member of the United Kingdom Home Office Biometrics and Forensics Ethics Group, an advisory non-departmental public body, which provides independent ethical advice to ministers on issues related to the use of biometrics and forensics. Previously she chaired Durham Constabulary's Ethics Committee and served on the NHS Research Ethics Committee (Scotland). This aspect of her work is of particular significance in appraising possible regulation models.

AI/data science, which encompasses FRT, is a prioritized research pillar at Monash University, and Professor Campbell is an active and engaged research affiliate of the Monash Data Futures Institute. She was a part of a Monash University Interdisciplinary Research project on Australian public attitudes toward AI, Data Science & Society in 2020.

Dr Joe Purshouse has held the post of Lecturer in Criminal Law at the University of East Anglia since 2016. Prior to this, he completed a PhD in the School of Law, University of Nottingham under the supervision of Professor Paul Roberts and Professor John Jackson. His thesis examined the extent to which the privacy rights of those subject to police surveillance are recognised and afforded adequate protection under English law. Dr Purshouse's scholarly expertise is in the intersections between criminal process, criminology and human rights.

Dr Purshouse has published several papers critically assessing the regulation of different forms of state surveillance in Europe, including DNA retention, criminal records disclosure, and automated facial recognition surveillance. His research has received extensive national and international media coverage. He is a member of the EU Horizon Cyber Crime Driver Stakeholder Board.

Dr Marcin Betkier is a Lecturer at the School of Law of Victoria University of Wellington. He completed a PhD at the School of Law under the supervision of Prof Nicole Moreham and Prof Susy Frankel. His thesis explained legal, technical, and commercial aspects of Internet services to propose a new, usercentric regulatory system which would effectively protect privacy of individuals and, at the same time, facilitate the effective operation of data-driven economy. He also has a Master's degree in Computer Science from Warsaw University of Technology, Master's degree in Law from Koźmiński University in Warsaw, and postgraduate MBA studies from Koźmiński University. Marcin also worked for 15 years in the ICT sector in different roles – technical, commercial, and legal. He specialises in data privacy (protection), market regulation, and competition law and policy. More information can be found in www.linkedin.com/in/mbetkier/.

Marcin's new book Privacy Online, Law and the Effective Regulation of Online Services (Intersentia, Cambridge UK, September 2019) is, as described by its reviewer, 'a valuable and remarkable read' which gives 'precious insights towards the possible modification of the existing legal framework and ICT technological architecture'.

Research and Editorial Assistants

Stephen Woodwark completed his LLB/BA in 2019 at Victoria University of Wellington and then went on to his current role as a Judge's Clerk to the Chief District Court Judge. Prior to this Stephen was a Case Resolution Officer at the Independent Police Conduct Authority. Outside the legal sphere, Stephen is a triathlete and an occasional salsa dancer.

Liesbet Vercruyssen is an LLB(Hons) and BA student at Victoria University of Wellington. Throughout her studies she has also worked as a legal clerk in the private sector. Liesbet will complete her degree in early 2021.

Anna McTaggart is an LLB(Hons) and BA student at Victoria University of Wellington. She has worked as a law clerk in the Treaty team at Crown Law and is interested in criminal law. Anna will complete her degree in early 2021 and hopes to pursue a career in the public sector.

EXECUTIVE SUMMARY

'The algorithms of the law must keep pace with new and emerging technologies.[1]

This technology allows remote, contactless, data processing, even without a person's knowledge. In the current digital environment, where people's faces are available across multiple databases and captured by numerous cameras, facial recognition has the potential to become a particularly ubiquitous and intrusive tool. The increased surveillance enabled by this technology may ultimately reduce the level of anonymity afforded to citizens in the public space.[2]

1 FRT AND ITS USE

The use of automated facial recognition technology (FRT) is becoming commonplace globally and in New Zealand. FRT involves the use of an algorithm to match a facial image to one already stored in a system, is used in automated passport control and other border control measures, as a biometric identifier in the banking, security and access contexts, and on social media platforms and various other consent-based applications.

2 VALUE AND RISKS OF FRT

FRT offers accuracy, speed and convenience in identity management in the commerce, travel, immigration, border control and security contexts.

The ability to identify and intercept an individual through automated crosschecking of images could be of immense value in the investigation of crime, counter-terrorism, and immigration. However, there are critical implications for the right to privacy and the right to be free from discrimination, and its use can compound existing biases. It is unlike other biometrics such as DNA and fingerprints in that facial images can be collected at a distance and their collection, use and storage is not specifically covered by legislation in New Zealand.

3 CONTRIBUTION OF THIS REPORT

This report contributes to the understanding of how and when this rapidly emerging technology should be used and how it should be regulated. It is centred in what has been described as the 'second wave' of algorithmic accountability –

> While the first wave of algorithmic accountability focuses on improving existing systems, a second wave of research has asked whether they should be used at all—and, if so, who gets to govern them.[3]

This project seeks to address the regulation gap through ascertaining how FRT can and should be regulated in New Zealand. While the benefits that might be offered by FRT surveillance are increasingly observable, its effect on civil liberties is subtler, but certainly pernicious. Given the potential for FRT to be used as a key identity and access management tool in the future, there are pertinent questions around how images are being collected and stored now by the private sector. Where are these images being stored? Who has access to this data? What else might the images be used for?

Without a detailed appraisal of the benefits of state FRT surveillance, and an understanding of the ethical issues raised by its use, any framework for the regulation of this activity cannot hope to engender public confidence that its use is fair and lawful.

1 *R (On Application of Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019)* [1].

2 *Commission Nationale de l'Informatique et des Libertés*, Facial Recognition: For a Debate Living Up to the Challenges, November 2019 www.cnil.fr/en/facial-recognition-debate-living-challenges

3 Frank Pasquale, "The Second Wave of Algorithmic Accountability" (11 November 2019) LPE Project www.lpeproject.org/blog

4 METHODOLOGY AND APPROACH

We are a project team with extensive expertise in the theory and practice of biometrics, data privacy and state surveillance, with established collaborative relationships and a track record of impactful co-authored publications. Our experience extends to bridging the gap between academic scholarship and policy and practice, including comparative insight into ethical issues, governance and regulation in this space.

The methodology for this project used a combination of literature review, legal reasoning, analysis of theoretical frameworks and stakeholder consultation and interviews to produce an accessible but insightful analysis of the use of FRT in New Zealand, the risks and benefits of the technology, and the options for regulation, governance and oversight.

The principal phases of the project were:

Phase 1 – Literature review and scoping: This phase involved surveying the literature and stocktaking uses of FRT nationally and internationally.

Phase 2 – Issues paper: This phase involved the writing of an issues paper which outlined the key questions and scoped some preliminary recommendations.

Phase 3 – Workshop and panel discussion: A workshop was held in Wellington in October 2019. Attendees were drawn from New Zealand Police, MBIE, the Privacy Commissioner, the Office of the Prime Minister's Chief Science Advisor, the Law Commission, Artificial Intelligence Forum of NZ, Department of Internal Affairs, Department of Prime Minister and Cabinet, the private sector and academic colleagues. Two international experts – Clare Garvie of the Centre for Privacy and Technology at Georgetown University in Washington DC and Rachel Dixon, the Privacy and Data Protection Deputy Commissioner for the State of Victoria, attended and participated in the workshop, as well as all members of the research team. A public panel discussion was held at Victoria University of Wellington on 17 October 2019.[4]

Phase 4 – Report Writing: 2020 was an exceptional year in many ways, and Covid-19 impacted our work in many ways. Like academic colleagues around the world, our research was impacted by lockdowns, increased teaching duties and cancellation of conferences, seminars and research trips. Government operations in New Zealand was also significantly impacted as civil servants were deployed on the Covid-19 response. Our thanks to our funders for permitting an extension to the time available for drawing down the funding.

Phase 5 – Peer review and publication: Several colleagues from the academic and public sectors generously gave their time to peer review our recommendations and other sections. Any errors are of course our own.

5 OUTLINE OF THE REPORT

Section 1 – stocktakes the use of FRT across New Zealand and comparable jurisdictions,

Section 2 – discusses the content and application of the human rights framework,

Section 3 – discusses ethical standards for the use of technologies such as FRT, public attitudes and social licence,

Section 4 – considers the threats that FRT may pose to human rights,

Section 5 – analyses the application of existing laws and regulation in New Zealand,

Section 6 – considers models of regulation from comparable jurisdictions,

Section 7 – draws together general and specific recommendations.

4 Faculty of Law, Victoria University of Wellington "Automatic Facial Recognition Technology–Legal and Ethical Issues" (21 October 2019) *YouTube*. www.youtube.com/watch?v=fnHEKDvBTJs

6 SUMMARY OF RECOMMENDATIONS

Section 7 details our conclusions and recommendations:

Recommendation 1: Create a new category of personal information for biometric information,

Recommendation 2: Provide individuals with additional control over personal information,

Recommendation 3: Establish a Biometrics Commissioner or other oversight mechanism,

Recommendation 4: Implement high-quality Privacy Impact Assessments,

Recommendation 5: Add enforceability and oversight to Algorithm Charter,

Recommendation 6: Transparency in use of FRT,

Recommendation 7: Implement a code of practice for biometric information,

Recommendation 8: Information sharing agreements for facial images must be appropriate and transparent,

Recommendation 9: A moratorium on the use of live AFR by Police,

Recommendation 10: Consultation and consideration of legislation,

Recommendation 11: Review of collection and retention of facial images by Police,

Recommendation 12: Threshold before comparison can be made in Police's image system,

Recommendation 13: Oversight of the Police's image database,

Recommendation 14: Oversight of emerging technology such as FRT,

Recommendation 15: Regulate surveillance using FRT in public places.

SECTION 1

THE USES OF FACIAL RECOGNITION TECHNOLOGY

1.1 INTRODUCTION

This section stocktakes the uses of FRT in Aotearoa New Zealand and in comparable jurisdictions. Every technology has benefits and risks, and FRT is no different. Any potential regulation must balance the public interest in availability and use of a technology with potential risks to collective and individual rights and interests.

This section begins by outlining what FRT is, and then considers its use across various sectors in New Zealand and in other jurisdictions. Although our focus in this report is generally the use of FRT by the state, particularly in policing, many problematic uses of the technology arise in use of private sector applications by the state. It is thus appropriate to discuss uses by the private sector.

Our description of various uses is a high-level summary gleaned from publicly available sources and consultations with stakeholders and is not exhaustive, nor particularly detailed. Yet, it demonstrates the wide extent of use and potential uses and the potential societal benefits, which frames later discussions of threats and benefits.

1.2 WHAT IS FRT?

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

It is reported that face recognition was being used as far back as the 1960s,[1] with the United States' Defense Advanced Research Project's Agency creating a basic database in the early 1990s.[2] Facebook began implementing an automatic 'tagging' system on their network in 2010. Their system suggested 'tags' with names for faces in photos.[3] By 2017, Apple's I-Phone X was the first phone which could be unlocked using 'FaceID' – the brand name for Apple's facial recognition technology system.[4]

The technological operations of FRT comprise the following:[5]

- Collection/acquisition of images,
- Face detection,
- Normalisation,
- Feature extraction,
- Storage of raw data and features (face templates),
- Comparison,
- Use for primary purpose (e.g. identification of a wanted person),
- Potential reuse for other purposes,
- Potential disclosure,
- Deletion of raw data and/or features (face templates).

The software takes digital images (e.g. those collected from a camera or stored in image database) and performs mathematical operations to detect faces of individuals. Data describing faces are normalised (e.g. scaled, rotated, aligned, etc.) to the form in which the facial features can be recognised. The FRT algorithm extracts from the normalised face images features that individually describe a particular person. Those features are stored and compared (or matched) with features

1 Kelly Gates *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, New York, 2011).

2 Peter Trepp "How Face Recognition Evolved Using Artificial Intelligence" FaceFirst www.facefirst.com.

3 Nicolas Jackson "Facebook will start using facial recognition next week" *The Atlantic* (online ed, United States, 16 December 2010).

4 Luana Pascu "Apple patents potential new Face ID biometrics system, to launch face recognition to iMac" (17 June 2020) Biometric Update www.biometricupdate.com.

5 Article 29 Working Party *Opinion 02/2012 on facial recognition in online and mobile services* (WP 192 2012) at 2; *R. (On Application of Bridges) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019)* [24].

that had been previously collected and are on a list (or in a database) available to the algorithm.[6] The outcome of the comparison depends on the use scenario. If a match is found, the computer may, for example, signal that match to the human operator or perform other (or additional) automated tasks. The critical issues for further legal analysis may lay outside of the comparison (or recognition) operation. For example, it may be crucial where collected raw data come from, what happens to those data and face templates, whether they are retained or deleted, how they are accessible and potentially reused.

1.3 PRINCIPAL CATEGORIES OF USE OF FRT

A report by the European Union categorises the three principal uses of FRT as:[7]

Verification [one to one comparison] This involves the comparison of two biometric templates to verify a person's identity. The SmartGate system used at the airport is a good example of this use.

Identification [one to many comparison] This involves the comparison of an individual's biometric template to another stored in a database. An example of this is the automated FRT system used by police forces which can extract facial images from video footage and compare against a 'watchlist'.

Categorisation FRT may also be used to extract information about particular characteristics of a person such as race, sex and ethnicity. This is also known as 'face analysis.'[8] This analysis could predict or profile a person based on their facial image. It does not specifically identify a person, but if characteristics are inferred from a facial image and potentially linked to other data (e.g. location data), it could de facto enable the identification of an individual.[9]

1.4 LEVEL OF INTRUSIVENESS

The threats that FRT may pose to the rights and interests of the individual are discussed in more detail in other chapters, but it is worth briefly commenting here on the level of intrusiveness involved in the collection of facial images.

FRT differs from other biometrics (DNA, iris scan, fingerprint)[10] in that a person's face is generally public and its image can be collected from a distance, and without the knowledge of the person. Yet, it does involve intrusion on privacy:[11]

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

As England and Wales' Biometrics Commissioner has noted:[12]

> …unlike existing police biometrics whose acquisition is quite complicated, digital facial image capture is easy and the subject may not even be aware that it has happened. For the same reason, faces in public places can be easily scanned and matched. In other words, this is potentially much more intrusive of an individual's privacy than existing police biometric

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

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

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

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

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

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

12 Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020) at [37].

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.

1.5 CURRENT AND FUTURE APPLICATIONS

In a New Zealand context, there has been a noticeable increase in discussion of its potential applications, with adoption of the technology on the increase in both the private and public sectors. As noted, our primary focus in this report is use by the state sector, but state use inevitably leverages the private sector. The increasing use also contributes to questions of social licence.

1.5.1 Identity Verification

1.5.1.1 Electronic identity credential management

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

The Department of Internal Affairs (DIA) have used facial recognition technology in the production process for New Zealand passports since 2012. The FRT used to process passports is undergoing upgrades, with the purpose of improving efficiency and increasing the accuracy of facial recognition algorithms. The replacement technology went into production in September 2020.[13]

Many New Zealanders will have applied for a RealMe identification credential.[14] This is a government-operated identity service, which allows a person to have a verified electronic identity credential, which may be used to access a range of government services. This system is administered by DIA. It allows registered users to apply for and renew passports, driving licences, submit tax returns, apply for police vetting, register births, deaths and marriages, apply for student loans and claim Covid-19 related assistance.[15] Private sector companies (such as banks) are also part of the scheme.[16]

The system has a legislative framework under the *Electronic Identity Verification Act 2012* which provides for "...a whole of government shared service to enable a centralised approach to be taken in relation to the verification of an individual's identity by electronic means while protecting the individual's privacy."[17] Part of the process for applying for a RealMe credential is the collection of a facial image. This can be done using one's own device or at a commercial photo service provider. Under s. 46 of the *Electronic Identity Verification Act*, an applicant may be required to submit a photograph which the Chief Executive may compare with existing images within the database or with other databases.[18] Facial recognition software may be used in this comparison.[19]

The privacy statement for RealMe demonstrates how FRT may be used: [20]

> The photo taken during the application process, or retrieved from DIA's passports database, will be stored for future one-to-many matching, for the purposes of protecting individuals' identity and detecting fraud.
>
> If you are eligible and choose to use RealMe digital photo capture services, your photo and video/ frames of your liveness test will be stored within the application server to allow for automated facial recognition matching, reference by DIA for assessment of your application, quality assurance and other duties to support the Identity Verification Service. Your captured image and liveness video may also be reused to retest biometric facial recognition thresholds to better improve our service.

A facial image must be provided to use the RealMe service. Use of an electronic identity credential is not compulsory for accessing services, but it is expected that this service will

13 Official information Request to Department of Internal Affairs (17 November 2020).

14 Almost 800,000 verified identities have been issued. "How we have grown" www.realme.govt.nz.

15 "Where to use RealMe®" RealMe www.realme.govt.nz.

16 "Where to use RealMe®" RealMe www.realme.govt.nz.

17 Electronic Identity Verification Act 2012, s 3(2)(b).

18 Electronic Identity Verification Act 2012, s 46(5).

19 Electronic Identity Verification Act 2012, s 46(6).

20 "Identity Verification Service Privacy Statement" (20 July 2020) RealMe www.realme.govt.nz.

become more widespread. A review of the digital identity services is ongoing and expected to be completed in 2021.[21]

Another aspect is the *Identity Information Confirmation Act 2012* – this empowers a service operated by DIA. Registered organisations may confirm the accuracy and validity of identity information against official databases (passports, birth, deaths and citizenship databases).[22]

DIA is also exploring options to use web photo capture technology to develop One Time Identity, a verification process which would allow customers to prove their identity to a client organisation online in near real-time.[23]

1.5.1.2 Immigration

Under the *Immigration Act 2009*, Immigration New Zealand (INZ) is empowered to collect biometric information from visa applicants including photographs.[24] Biometrics may also be collected from 'a person who is proposing to board a craft for the purposes of travelling to New Zealand'.[25]

These are then converted to digital images which can be used in a facial recognition system: "biometric information processes are either manual or semi-automated. For example, hard copy photographs are scanned to provide a digital image. Passport photographs can be collected directly from passports."[26]

Biometric information such as facial images may be used in decision-making.[27] Fraud prevention through detection of identity fraud is the principal reason why FRT is used. INZ states that the key reasons are:[28]

- Identify and check the identity of foreigners seeking resettlement,
- Help identify refugees under New Zealand's quota programme,
- Identify and check people under investigation at the border,
- Record the identity of deportees and stop them re-entering New Zealand under another identity,
- Identify and check people suspected of breaching the Act,
- Expose assumed identities.

As part of an Approved Information Sharing Agreement (AISA), DIA is working with INZ to obtain access to photos held by immigration, enabling the completion of a liveness check and comparison at the time a person applies for citizenship. Under the Te Ara Manaaki programme, DIA is also moving away from requiring the physical presence of a person to confirm identity. Using similar technology to RealMe, people applying for citizenship could choose to capture their own photo for a citizenship application, which can be compared against an authoritative source. To ensure they are a living person, the applicant would be asked to perform liveness checks as part of their application.[29]

NEC (a Japanese corporation) has contracted with DIA to update the passport system in New Zealand for the next 10 years starting January 2021. The programme will be used to check photos against the DIA database and detect fraud. NEC has a 'close relationship' with police as its technology is used for finger and palm print biometrics, however states that its FRT is not being used by police. The company has been criticised in the United States and UK for some of its practices.[30]

1.5.1.3 Border control

SmartGates that utilise FRT are now a common sight in New Zealand and international airport terminals. Proponents of FRT perceive increased efficiency in

21 "Identity Verification Service Privacy Statement" (20 July 2020) RealMe www.realme.govt.nz.

22 The list of confirmation organisations is listed here: Te Tari Taiwhenua: Department of Internal Affairs "Organisations approved to use Confirmation Service" www.dia.govt.nz.

23 Official information Request to Department of Internal Affairs (17 November 2020).

24 Immigration Act 2009, s 60.

25 Immigration Act, s 100. This does not apply to citizens or resident visa holders. Non-citizens leaving New Zealand may also be the subject of biometrics collection (Immigration Act 2009, s 120).

26 Ministry of Business, Innovation and Employment *Privacy impact assessment report: Collection and handling of biometrics at the Ministry of Business, Innovation and Employment* (May 2016) at 35.

27 Immigration Act 2009, s 30.

28 How Immigration New Zealand uses biometric information: New Zealand Immigration "Biometric information" www.immigration.govt.nz.

29 Official information Request to Department of Internal Affairs (17 November 2020).

30 Phil Pennington "Global facial recognition company working closely with NZ govt" *RNZ* (online ed, New Zealand, 19 August 2020).

border processing over more "archaic" methods.[31] It appears rarer for privacy concerns to be raised over use of FRT and collection of biometric data in the context of international travel, particularly given the volume of use. This may indicate that privacy interests are outweighed by concerns of personal and national security, though some discontent has been expressed.[32]

In April 2019, it was announced that the New Zealand Customs Service would be implementing a face-to-face human review process where an eGate rejects a passenger.[33] A report was produced by Customs in March following an internal review in response to an incident where a person of interest left the country with another person's passport.[34] In 2016, a New Zealand man of Asian ethnicity was attempting to renew his passport when the automatic system rejected his photo on the basis his eyes were closed.[35] Such inaccuracy could have particularly serious consequences in this context, where national security may be at stake.

1.5.1.4 The new all-of-government contract for biometrics

Journalist Phil Pennington from Radio New Zealand has done extensive investigation into the recent signing of an all-of-government contract for biometrics, including facial images.[36] His research yielded a copy of the Master Syndicated Agreement signed by the Chief Executive of DIA.[37] DIA signed a ten-year agreement in 2018 which many public and private organisations will be able to join.[38] The deal was signed with Enterprise Services New Zealand, the New Zealand subsidiary of DXC Technology, a United States company. The system is now operational. The aim of the technology is to prevent fraud. The FRT system compares passport photos with a database to identify those with multiple identities. DXC uses software from the Japanese firm NEC. As a result of the deal, the passport photos and data of 4.5 million New Zealanders (those aged over 11) will now be managed by Enterprise Services New Zealand, whereas previously the DIA managed this information.[39]

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

1.5.1.5 International examples

Selected European Union external borders (Greece, Hungary, Latvia) researched whether FRT can help to detect whether someone is lying. Facial recognition technology was used alongside other technologies in a border control process where computer animated 'border-guard' asked travellers questions to detect whether they were lying. "The unique approach to

31 Amanda Cropp "Border reform next in queue" *Dominion Post* (online ed, Wellington, 30 September 2017).

32 Kelly Yamanouchi "Privacy Advocates Raise Concerns as Delta Airlines Expands Use of Facial Scanning at Atlanta International Airport" (19 September 2019) Governing www.governing.com; and "Future facing: Ticketless plane travel and face scanners, what it means for privacy" *New Zealand Herald* (online ed, New Zealand, 12 June 2019).

33 New Zealand Customs Service "Customs confirms changes after eGate system review" (11 April 2019) www..beehive.govt.nz.

34 New Zealand Customs Service *Remediation Report: Review of eGate Processes and the Use of the Decision Review Tool* (28 March 2019).

35 James Regan "New Zealand passport robot tells applicant of Asian descent to open eyes" *Reuters* (online ed, Sydney, 7 December 2016).

36 Phil Pennington, Government facial recognition tech deal offers wide access RNZ (online edition) 12 October 2020, containing links to documents obtained under the Official Information Act.

37 Phil Pennington "Government facial recognition tech deal offers wide access" *RNZ* (online ed, New Zealand, 12 October 2020), containing links to documents obtained under the Official Information Act.

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

39 Chief Executive of the Department of Internal Affairs and Enterprise Services New Zealand *Master Syndicated Agreement: relating to the syndicated procurement of Facial Recognition Services* (14 December 2018). Released under the Official Information Act, copies on file with the authors.

40 Phil Pennington "Government facial recognition tech deal offers wide access" *RNZ* (online ed, New Zealand, 12 October 2020).

'deception detection' analyses the micro-gestures of travellers to figure out if the interviewee is lying."[41]

In Singapore, FRT is being introduced as part of the national identity scheme.[42] The country's digital identity program, SingPass, will use face verification processes to give citizens access to both private and government services. The technology is used to identify a person accessing services and ensure that they are present when being identified, protecting against the use of photos, videos or deepfakes.[43] The technology is already used in one bank and some branches of the county's tax office. Further intended uses are identity verification at secure locations such as ports and to ensure that students taking tests are who they say they are.

1.5.2 Policing

As we discuss in later sections, the use of FRT in policing is probably the most controversial and impactful use of FRT.

1.5.2.1 Use of FRT in Policing in New Zealand

Journalist George Block from Stuff has written extensively on the Police's plan to upgrade their FRT capability. His investigation revealed that a request for proposals released in mid-2018 shows that Police have an existing image management system called 'Photo Manager' with some FRT capability.[44] Concerns were raised in 2018 when New Zealand Police were looking to update their surveillance capabilities.[45] The RFP indicated that Police were seeking to acquire as part of this system:

- "An innovative mobile and desktop forensic capability solution(s) with the capability to link/identify individuals from images captured and/or stored by Police."[46]
- "A photo database able to import, store and search facial images in separate categories; such as Suspect (unknown id), Prisoner/Arrestee, Firearms Licences, Missing Persons,[47] Individuals included in Child Sex Offender Register (CSO)"
- "Facial recognition technology capable of searching external facial images (e.g. CCTV images) against the facial images database and search images within the database against other images within the database."
- A system capable of capturing, storing and searching distinguishing marks like scars and tattoos and clothing descriptions.[48]

In late 2019, Block's article reported that an American company, Dataworks Plus has been chosen to upgrade the police's current biometric system. Unlike United States-based Dataworks Plus systems, the system would not run facial recognition against drivers licences as the NZ Transport Agency, rather than the police, control this database. According to Datawork Plus's vice president and general manager, Todd Pastorini, the algorithm would help to narrow down the hundreds of thousands of images in the database to a list of the top 100, allowing investigators to select the best match from this shorter list.[49]

A report from RNZ in August 2019 indicated that Police were interested in the potential of accessing live camera feeds from the Auckland Transport network.[50]

41 European Commission "Smart lie-detection system to tighten EU's busy borders" (24 October 2018) www.ec.europa.eu.

42 Tim McDonald "Singapore in world first for facial verification" *BBC News* (online ed, Singapore, 25 September 2020).

43 For a New Zealand perspective on deepfakes see Curtis Barnes and Tom Barraclough, Perception Inception – Preparing for deepfakes and the synthetic media of tomorrow (Law Foundation: Wellington, 2019.

44 New Zealand Police *Request for Proposals ABIS 2 (Automated Biometric Identification Solution)* (TN 18/03, RFP released 15 January 2018) (copy on file with authors).

45 Tom Hunt "Police eyeing up newer, smarter CCTV facial recognition technology" *Stuff* (online ed, New Zealand, 18 April 2018).

46 New Zealand Police *Request for Proposals ABIS 2 (Automated Biometric Identification Solution)* (TN 18/03, RFP released 15 January 2018) (copy on file with authors) at 4. Our thanks to George Block from Stuff for sharing this with us.

47 New Zealand Police *Request for Proposals ABIS 2 (Automated Biometric Identification Solution)* (TN 18/03, RFP released 15 January 2018) (copy on file with authors) at 3.

48 George Block "Privacy concerns over police's new 'state of the art' facial recognition system" Stuff (online ed, New Zealand, 5 December 2019).

49 George Block "Privacy concerns over police's new 'state of the art' facial recognition system" Stuff (online ed, New Zealand, 5 December 2019).

50 Phil Pennington "Police open to using facial recognition from Auckland Transport CCTV cameras" *RNZ* (online ed, New Zealand, 15 August 2019).

1.5.2.2 The Clearview Test

Clearview is a searchable database of around 3 billion images which have been sourced from public information on social media platforms and other websites. It is in heavy use by police forces, particularly in the United States.[51] The Clearview website contains some information about how the system works. According to the company it searches the 'open web', It does not "search any private or protected info, including in your private social media accounts."[52] Clearview claims that the app can detect offending particularly child sexual abuse and terrorism.

It has been reported that several social media platforms such as Facebook, Twitter and LinkedIn have accused the company of violating their terms of reference.[53] Investigations have been launched in the UK and Australia into use of Clearview AI.[54]

A number of journalists have investigated police use of Clearview in New Zealand.[55] From media reports and an Official Information Act request,[56] it appears that the timeline was as follows:

- Members of a Police unit focussed on high tech crimes approached Clearview in January 2020 seeking to test the app,
- No clearance was received from senior management nor was the Privacy Commissioner consulted,[57]
- The team tested Clearview by uploading images of police staff and suspects,
- Images included "images of wanted people who police say looked "to be of Māori or Polynesian ethnicity", as well as "Irish roof contractors",[58]
- Police concluded that the system did not work well, particularly as there was only one successful match. this may be because the Clearview database was focused on US populations and had fewer stored images of people from New Zealand, rather than a deficit in the algorithm itself, which raises concerns that another party could apply a similar methodology and address the data deficit to achieve better results,
- It was reported that Clearview claimed to have detected the Christchurch mosque shooter.

Justice Minister Andrew Little criticised the Police for failing to seek any clearance before testing the system: [59]

> It clearly wasn't endorsed, from the senior police hierarchy, and it clearly didn't get the endorsement from the [Police] Minister nor indeed from the wider cabinet … that is a matter of concern.

1.5.2.3 Stocktake of New Technologies

A stocktake of new technologies was commissioned by Police Commissioner Andrew Coster in May 2020 to ensure that no other similar technologies had been trialled.[60] This review was catalysed by concerns around the Police's use of Clearview AI's FRT system,[61] but also covered other forms of technology. The review was

51 Kashmir Hill "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (online ed, New York, 18 January 2020).

52 "How Clearview AI Works" www.clearview.ai.

53 Heather Somerville "Facial-Recognition Startup Clearview Moves to Limit Risk of Police Abuse" *The Wall Street Journal* (online ed, New York, October 20 2020).

54 The Associated Press "UK, Australia investigate Clearview facial recognition firm" *ABC News* (online ed, Australia, 10 July 2020).

55 Mackenzie Smith "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI" *RNZ* (online ed, New Zealand, 15 May 2020).

56 Mackenzie Smith "Police trialled facial recognition tech without clearance" *RNZ* (online ed, New Zealand, 13 May 2020).

57 Mackenzie Smith "Police trialled facial recognition tech without clearance" *RNZ* (online ed, New Zealand, 13 May 2020).

58 Mackenzie Smith "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI" *RNZ* (online ed, New Zealand, 15 May 2020).

59 Mackenzie Smith "Police trial of facial recognition technology 'a matter of concern' - Andrew Little" *RNZ* (online ed, New Zealand, 12 May 2020). In an OIA response to Dr Andrew Chen, Minister Little said that he had had no correspondence with government agencies or other Ministers about the use of facial recognition technologies. Letter from Minister Little to Dr Andrew Chen available at https://fyi.org.nz/request/13896/response/52528/attach/8/201030%20A.Chen.pdf.

60 Mackenzie Smith "Police 'stocktake' surveillance tech after Clearview AI facial recognition trial" *RNZ* (online ed, New Zealand, 18 May 2020); and Mackenzie Smith "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI" *RNZ* (online ed, New Zealand, 15 May 2020).

61 Principal Advisor: Privacy, Assurance Group, PNHQ *Assurance review of emergent technologies* (New Zealand Police, July 2020), at 1. Released under the Official Information Act, copy on file with authors. Our thanks to Mackenzie Smith for sharing this with us.

carried out by the Police's Assurance Group and released under the Official Information Act in November 2020.[62]

The key findings of the review were:[63]

- Police make limited use of new technologies in comparison to other law enforcement agencies,
- "Use of Clearview AI software was a relatively short test, which was approved by an internal governance group, albeit not at Executive level.",[64]
- "Opportunities have been missed to inform or consult some stakeholders before certain trials of 'new tech'."[65]
- In comparison to other jurisdictions, "New Zealand Police's use of emergent technologies has been reasonably conservative and carefully thought-through."[66]

The review carried out a stocktake of trials of emergent technologies that have been or are currently being undertaken by the Police. Those related to FRT or with potential use of FRT are mentioned here:

Clearview AI – Short, non-operational test was carried out. Advice was provided that if the software was to be considered for ongoing investigatory use then a formal legal review and Privacy Impact Assessment (PIA) would be necessary.[67]

Brief Cam – "Used to analyse CCTV footage acquired by Police to establish the presence of a known face or a car movement."[68] Estimated to drastically cut time Police spend analysing evidential CCTV footage.

NewX – "Searches unstructured data and platforms for faces, guns, and body markings (tattoos)."[69]

Cellebrite – searches lawfully seized cellphones for data. "Includes a facial recognition capability that Police has not made use of."[70]

Automated Biometric Information Survey (ABIS) – will provide ABIS with an upgraded FRT algorithm. The system was planned to be deployed by September 2020, but it was not possible to ascertain whether this deployment has taken place on schedule. The system will also enable search capability across scars, marks and tattoos. The tool is not available to Police staff in general, only by formal request. A Privacy Impact Assessment and security certification and accreditation are ongoing considerations.[71]

Remotely Piloted Aircraft Systems aka 'drones' – use endorsed by Police Executive in 2019.[72]

Axon Citizen (Evidence.com) – Used to store various types of video evidence. No AI or FRT capabilities.[73]

Front Counter Person Tracking and Counting – Cameras used to assess the volume of people entering a police station, when they visit and the length on time spent at a counter.[74]

The review further reported on emergent technologies that are being considered for potential use. The following two had the potential to incorporate FRT:

Body-Worn Cameras - but FRT was not mentioned in relation to this technology in the report.[75]

Digital Information Management – "It is likely the tenders will list AI and potentially facial recognition as part of the requirements."[76]

62 Principal Advisor: Privacy, Assurance Group, PNHQ *Assurance review of emergent technologies* (New Zealand Police, July 2020). See also Phil Pennington 'Audit reveals new tech tools in police's digital armoury' RNZ (online ed, New Zealand, 5 November 2020).

63 At 1.

64 At 1.

65 At 1.

66 At 1.

67 At 2.

68 At 2.

69 At 2.

70 At 3.

71 At 3.

72 At 3.

73 At 3.

74 At 4.

75 At 5.

76 At 5.

The report also noted that many technological tools used by have an inbuilt FRT capability that is not used e.g. mobility devices.[77]

Police also seem to draw a distinction between live AFR on real-time CCTV footage vs. processing of stored CCTV footage during investigation using FRT, though as we discuss in the recommendations section, the impact on individual and societal rights is similar.

1.5.2.4 Police collection of images

Police have already amassed a significant collection of images which could underpin future use of FRT. The Privacy Impact Assessment for the ABIS program includes numbers of current and projected records in various categories within the police's photo manager system:[78]

- Prisoner – 1.85 from 800,000 individuals current records. There will be an estimated 50,000 additional records per annum,
- Suspect – it is projected there will be an additional 7,500 records per annum,
- Firearms licence holders – 245,000 records at any one time, with 10,000 renewals and 9,500 new records estimated per annum,
- Missing persons – 200 current records, with an estimated 300 additional records per annum,
- Child protection (child sex offender register) -1,500 current records, with an estimated 2,300 additional records per annum,
- Facial recognition, search, compare, match and report – an estimated 15,000 additional records per annum,
- Photo line-up production – 12,000 current records (20-60 minutes to prepare standard line-ups). There will be an estimated 15,000 additional records per annum (10 minutes to prepare standard line-ups),
- Scars, marks, tattoos and logos – capture, search, match and report – 2,500 current records, with an estimated 30,000 additional records per annum.

Under the *Policing Act 2008*,[79] Police can take the photo[80] of someone who is in the lawful custody of the police and is being detained for committing an offence at a police station or another place being used for the time being for police purposes. A similar provision was in force under the *Police Act 1958*.[81]

These images must be destroyed 'as soon as practicable' when a decision is made not to proceed with a prosecution or the person is acquitted. Images could be retained if the person admits the offence and undergoes diversion, the person is convicted, a Youth Court order is made or the person is discharged without conviction.[82] Under the previous legislation, the images could be retained unless the person was acquitted.[83]

The power to retain custody images is thus more restricted that in other jurisdictions.[84] Police forces in the United Kingdom are reported to have 12.5 million images in a database, which may be searched using FRT. [85]

As we discuss in section 4 and in the recommendations section, there are concerns as to the over-representation of certain groups of people, particularly Māori, on police databases, and thus the effect of any use of FRT is likely to be disproportionately felt. Karaitiana Taiuru, an expert in indigenous ethics in data collection, stated that it is only a matter of time before a Māori person is wrongfully arrested due to a wrong match in police use of FRT.[86]

There is an information sharing agreement between the DIA's Registrar-General and the New Zealand Police, enabling the sharing of facial images. [87] We discuss the implications of these agreements in more detail in the recommendations section.

77 At 5.

78 National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020).

79 Policing Act 2008, s 32.

80 Policing Act 2008, s 32(5)(b).

81 Police Act 1958, s 57.

82 These actions must arise from the offence for which the particulars were taken: Policing Act 2008, ss 34 and 34A.

83 Police Act 1958, s 57(3).

84 See *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681.

85 "Police unlawfully retaining custody images, claims Norman Lamb" *BBC* (online ed, United Kingdom, 6 February 2018).

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

87 Official information Request to Department of Internal Affairs (17 November 2020).

1.5.2.5 Use by Police in other jurisdictions

1.5.2.5.1 United States

Considerable analysis on the use of FRT systems by police in the US has been done by Clare Garvie of Georgetown University.[88] FRT is in widespread use in the US policing context. Police can use FRT to identify people that they encounter who refuse to be identified or cannot identify themselves. They can take the person's photo with a device, process it through software they have in their patrol car, and receive a near-instantaneous response from the system.[89] Police use FRT to identify suspects. When investigating a crime, they run a picture of a suspect captured from a security camera or other device through a database of mugshots or drivers licences and create a list of candidates for further investigations. This can also be used when police believe that a suspect is using a pseudonym.[90] FRT can be used for real-time video surveillance. When the police are looking for an individual, they can upload an image of them to a 'hot list'. A FRT program compares images from real-time video surveillance to this hot list to find the individuals. When a match is found, police are alerted. Similar searches can also be run on archival footage.[91] FRT is also used to catch those using fraudulent identification. Departments of Motor Vehicles can compare the faces of new applicants for identification against the existing faces in its database. Individuals who may be using the same person's photo and a pseudonym as fraudulent identification are flagged.[92]

Discrimination and bias in FRT usage has been a key criticism. As examples: protesters in Detroit demanded the police stop using FRT due to its difficulties identifying the faces of black citizens accurately.[93] Police in the US used FRT to track and find prominent Black Lives Matter protestor in relation to an assault on an officer.[94]

A man in Michigan was arrested for a crime he did not commit due to faulty facial recognition match. He was detained overnight, had mugshot and fingerprints taken. "[H]is case may be the first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm, according to experts on technology and the law."[95]

IBM, Amazon and Microsoft have stopped supplying FRT to the police until there are legal protections in place to regulate the technology. Comes in the wake of the BLM movement and protests of racial injustice in the US.[96]

It has also been reported that activists are using FRT systems to track police officers.[97]

1.5.2.5.2 United Kingdom

As is discussed in more detail in later sections, police forces in the United Kingdom are making use of FRT, particularly live FRT. A recent decision of the Court of Appeal of England and Wales illustrates the usage of the technology in policing.[98] The appellant, Mr Bridges, is a resident of Cardiff, in Wales. He was scanned by FRT, which had been (overtly) deployed by South Wales Police on a public street in Cardiff city centre, and on another occasion at a protest at a defence exhibition. The system used is named "AFR Locate" and operates by capturing facial images from a CCTV camera and automatically comparing biometric data from the images with images derived from a "watchlist". A police camera operator may then review any matches, before deciding on further actions or interventions.

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

89 At 10.

90 At 11.

91 At 12.

92 At 12.

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

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

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

96 Dev Kundaliya "After IBM and Amazon, Microsoft bans facial recognition sales to police" (12 June 2020) Computing www.computing.co.nz.

97 Kashmir Hill "Activists Turn Facial Recognition Tools Against the Police" *The New York Times* (online ed, New York, 21 October 2020).

98 *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

In 2019, the South Wales Police trialled a facial recognition app on officers' phones. The apps allowed officer who were on patrol and spotted someone who looked like a person of interest to take a photo and confirm on the spot whether that is actually the person they were looking for or not. It could also be used to identify 'vulnerable' people instantaneously.[99]

The Metropolitan Police reportedly use live FRT to locate people on watchlists.[100] When people walk through a public area, their faces are scanned and compared to those who are wanted by the police or courts, seeking matches.

Police have also been reported to be investigating FRT that can spot anger and distress in CCTV footage in order to detect crime.[101] Further reports indicate that Police looking at using retroactive FRT to solve cold cases but questions of ethics have delayed the trial.[102]

1.5.2.5.3 China

Chinese authorities have been reported to be using FRT to track and control the minority Uighur population: "The facial recognition technology, which is integrated into China's rapidly expanding networks of surveillance cameras, looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review."[103] "The police are now using facial recognition technology to target Uighurs in wealthy eastern cities…. Law enforcement in the central Chinese city of Sanmenxia, along the Yellow River, ran a system that over the course of a month this year screened whether residents were Uighurs 500,000 times." "Uighurs often look distinct from China's majority Han population, more closely resembling people from Central Asia. Such differences make it easier for software to single them out."

China's vast surveillance camera system deploys FRT to watch almost every citizen.[104] The technology has been used to fine, reprimand and publicly humiliate citizens for things such as wearing sleepwear in public or jaywalking. Some experts say this is an attempt by the government to achieve behavioural engineering on a mass scale.

In 2018, Chinese police started using sunglasses equipped with FRT to identify suspected criminals in public places.[105] When a police officer sees a suspicious individual, they can take a photo of their face with the glasses. The image is then run through an internal database and if there is a match, the person's personal information including name and address will be sent to the police officer. The technology has been used to identify people accused of a range of crimes including hit-and-runs and human trafficking. It is also used to identify people using fake IDs.

In Hong Kong, the police used FRT to identify protestors in the demonstrations against the state in 2019.[106] To avoid identification, protesters began shielding their faces with masks, umbrellas and other coverings as well as destroying hundreds of CCTV cameras. This led the police to ban face coverings, an offence that carries a one-year prison sentence.

1.5.2.5.4 Hungary

Hungary plans to deploy a CCTV system of 35,000 cameras with FRT across the country. The system will be used to maintain public order and for road safety by capturing drivers' license plates and facial images. There are concerns that the Bill that allows this lacks substantial data protection guarantees.[107]

99 South Wales Police "South Wales Police trial new facial recognition app on officer's mobile phones" (8 August 2019) www.south-wales.police.uk.

100 Metropolitan Police "Live Facial Recognition" www.met.police.uk.

101 Fiona Hamilton "Police facial recognition robot identifies anger and distress" *The Times* (online ed, United Kingdom, 15 August 2020).

102 Fiona Hamilton "Police facial recognition robot identifies anger and distress" *The Times* (online ed, United Kingdom, 15 August 2020).

103 "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority" *The New York Times* (online ed, New York, 14 April 2019).

104 Alfred Ng "How China uses facial recognition to control human behavior" (11 August 2020) CNET www.cnet.com.

105 "Chinese police spot suspects with surveillance sunglasses" *BBC News* (online ed, United Kingdom, 7 February 2018).

106 Trey Smith "In Hong Kong, Protesters Fight to Stay Anonymous" (22 October 2019) The Verge www.theverge.com.

107 Abraham Vass "CCTV: Is It Big Brother or the Eye of Providence?" *Hungary Today* (online ed, Hungary, 18 January 2019).

In Hungary, police use FRT during police checks if someone cannot identify themselves during the check.[108] "In this case, the police officer would be authorized to take a photograph, take fingerprints, and record the individual's external physical features "by perception and measurement". What is more, the photo can be checked right on the spot through an electronic facial recognition system to prove and confirm the individual's identity. This practically means that police would only bring individuals in to the police department "for further data verification" if this method fails too."[109]

1.5.2.5.5 European Union

The European Union funded project *Towards the European Level Exchange of Facial Images* (TELEFI) is undertaking a study on how facial recognition is currently being used for the investigation of crime across European Union Member States. The project is currently underway.[110]

1.5.2.5.6 Germany

In May 2020, the Hamburg police deleted the biometric database for facial recognition that was created during the investigations into the rioting around the G20 summit in 2017. "The reason given by the police was that the database was no longer required under criminal law with regard to the G20 riots."[111]

1.5.2.5.7 Argentina

An investigation by Human Rights Watch found that Argentinian officials may be using FRT to track down children suspected of committing crimes.[112] The investigation found that children were added to CONARC, a national database in Argentina that holds information including IDs of people who have been suspected of criminal activity. This database is used by law enforcement in Buenos Aires alongside FRT to track down people suspected of committing crimes. The technology uses the headshots of suspects to search the city's subway camera system in real time and identify alleged offenders. The system has been the subject of controversy as it was implemented with no public consultation and has led to numerous false arrests. The government has publicly denied that CONARC includes minors, however, Human Rights Watch identified at least 166 children listed across different versions of the database between 2017 and 2020. The use of FRT to track children suspected of crimes is particularly concerning as the technology has been shown to be bad at identifying children.

1.5.3 Social Media

FRT is commonplace in much of our everyday technology. The popular FaceApp uses Artificial Intelligence to alter photos. While not directly linked to FRT, the available technology portrays the degree to which photos can be manipulated by AI and related privacy concerns.[113] This has potential implications in regard to security and law enforcement, where photos could be altered in order to 'cheat' FRT systems.

The Chinese version of TikTok is using facial recognition to censor live streaming by foreigners and children. Checks their face against their state ID to check they are not foreigners e.g. from Hong Kong.[114]

Twitter, Facebook and Linkedin have all told Clearview AI to stop using photos from their platforms.[115]

Facebook uses FRT to suggest 'tags' of people in photos.[116] This technology was not used in Canada and the European Union due to concerns about privacy.[117]

108 Abraham Vass "Police to Use Facial Recognition From Now On" *Hungary Today* (online ed, Hungary, 11 December 2019).

109 Abraham Vass "Police to Use Facial Recognition From Now On" *Hungary Today* (online ed, Hungary, 11 December 2019).

110 "About TELEFI Project" TELEFI Project www.telefi-project.eu.

111 The Hamburg Commissioner for Data Protection and Freedom of Information "Hamburg Police deletes the biometric database for facial recognition created in the course of the G20 investigations" (press release, 28 May 2020).

112 Karen Hao "Live facial recognition is tracking kids suspected of being criminals" (9 October 2020) MIT Technology Review www.technologyreview.com.

113 Tim Biggs "The fact and fiction of FaceApp" *Stuff* (online ed, New Zealand, 18 July 2019).

114 Laurence Dodds "China's TikTok twin using facial recognition to censor foreigners" *New Zealand Herald* (online ed, New Zealand, 13 July 2020).

115 Kashmir Hill "Twitter tells facial recognition trailblazer to stop using site's photos" *New Zealand Herald* (online ed, New Zealand, 24 January 2020).

116 In the past, Facebook's FRT has been found to be more accurate than the FBI's. Although, the comparison between the two is not exact as Facebook has more data to draw on; Russell Brandom "Why Facebook is beating the FBI at facial recognition" (7 July 2014) The Verge www..theverge.com.

117 Tom Kelly "Facebook Can Now Find Your Face, Even When It's Not Tagged" (19 December 2017) Wired www.wired.com.

1.5.4 Locating Missing Children

FRT may be used to find missing children.[118] Nearly 3,000 missing children were identified during a trial of the app in New Delhi.

A company in China is using crowdsourcing and FRT to find children who have been the victims of trafficking.:[119]"In a typical usage scenario, a user chances upon a child whom she suspects has been trafficked. The user takes a photo of the child and sends it to Zhongxun. Upon receipt of the photo, Zhongxun uses a machine learning facial recognition algorithm to compare the submitted photo against its database of photos of missing children in real-time."[120]

A Chinese man was stolen from parents when he was two-years-old. Police used facial recognition technology to analyse an old photo of him and simulated an image of him as an adult. Found him this year, when he was 32.[121]

In the European Union: "facial recognition systems used by the police and border guards may help trace missing and abducted children, including child victims of crime, and prevent child abduction. [EU Agency for Fundamental Rights's] small scale survey at border posts shows that children reported as missing are frequently encountered at border-crossing points."[122]

Police in Gujarat in India tested FRT to track missing offenders and missing children: "…the already existing database of criminals and missing people has been uploaded in the system and whenever those people come in the view of the police's CCTV network, an alert will be received by the police about their exact location."[123]

1.5.5 Travel and airports

The use of FRT is also on the rise in New Zealand airports. Between 2015 and 2016, the Customs Minister stated that "SmartGate use also increased with 1.15 million passengers using the gates between December and February – a 15 per cent increase on the previous year".[124] Wellington airport is planning on introducing technology to verify international travellers at bag-drop next year, the idea being to speed up the process.[125]

Use of FRT to speed up border control procedures has been recommended by the Tourism Export Council.[126]

Like in New Zealand, many countries utilise smart-gate technologies in border control processes.[127] Many airlines are looking to implement curb-to-gate FRT.[128] Using FRT at check-in, baggage drop, access to lounge and boarding means that no ticket or passport is needed for identity-checking.[129] Most United Kingdom airports use FRT at 'eGates' to help process passengers through passport checks.[130]

Rudolph et al have researched the use of FRT at departure gates in the United States. Congress never provided a rationale for the biometric exit program, but visa overstay fraud has been suggested as a

118 Anuradha Nagaraj "Indian police use facial recognition app to reunite families with lost children" *Reuters* (online ed, United States, 15 February 2020).

119 Chei Sian Lee, Dion Hoe-Lian Goh, Sei-Ching Joanna Sin, Hamzah Osop and Yin Leng Theng "Finding trafficked children through crowdsourcing" (2019) 55 Proceedings of the Association for Information Science and Technology 811.

120 Chei Sian Lee, Dion Hoe-Lian Goh, Sei-Ching Joanna Sin, Hamzah Osop and Yin Leng Theng "Finding trafficked children through crowdsourcing" (2019) 55 Proceedings of the Association for Information Science and Technology 811.

121 "Man kidnapped as toddler 32 years ago reunited with parents thanks to facial recognition" *New Zealand Herald* (online ed, New Zealand, 20 May 2020).

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

123 "Gujarat Police Tests Facial Recognition System To Track Missing Offenders" *NDTV* (online ed, India, 15 August 2020).

124 New Zealand Customs Service "Record summer passenger numbers" (press release, 31 March 2016).

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

126 Ministry of Business, Innovation and Employment E*lectronic Travel Authority (ETA): Summary of Submissions Report* (August 2018).

127 Future Travel Experience "Automated Border Control: Facilitation vs Security?" (April 2011) www.futuretravelexperience.com; and Danny Thakkar "Smart Gates on Autopilot" Bayometric www.bayometric.com.

128 Jason Davis "Biometric screening at airports is spreading fast, but some fear the face-scanning systems" *NBC News* (online ed, United States, 15 March 2018); and Chris Burt "NEC to provide curb-to-gate facial biometrics for Star Alliance frequent flyers" (26 July 2019) Biometric Update www.biometricupdate.com.

129 Chris Burt "Heathrow curb-to-gate biometrics said to be world's biggest single deployment" (29 April 2019) Biometric Update www.biometricupdate.com.

130 Centre for Data Ethics and Innovation *Snapshot Series: Facial Recognition Technology* (May 2020).

reason.[131] However, the current data on this fraud suggests it is not a significant enough issue to justify the resource-intensive biometric exit program. Congress has also never explicitly granted the authority to scan Americans' faces at the border, despite having many opportunities to do so.[132] Therefore, the current scanning of American faces through the program may not comply with federal law.

The biometric exit program raises broader concerns about the expansion of government surveillance.[133] This may have a chilling effecting on freedom of speech and association as airports increasingly become sites of political demonstration and speech.

Qantas have trialled using FRT for the ticketing process. The airline company held trials in Brisbane and Sydney where people used their face instead of a boarding pass. In Los Angeles, the company is currently trialling a system where FRT will replace both boarding passes and passports.[134]

Some ridesharing companies are considering using FRT to confirm that the passenger entering the vehicle is the right passenger and that the driver of the vehicle matches the person who is licensed to drive, in order to improve passenger safety.[135]

1.5.6 Banking and Finance

FRT may serve a number a of functions in the banking, finance and anti-money laundering sector, mainly in identity verification.

1.5.6.1 Identity verification

Most or all New Zealand banks report using FRT technology in identity verification procedures.

ASB bank has previously announced a pilot scheme for using FRT as a means of identifying customers,[136] and Westpac has implemented image matching for setting up an account.[137] Heartland Bank uses FRT to maintain compliance with anti-money laundering laws,[138] and the company OriginID is marketing a FR tool to accountants and lawyers for anti-money laundering compliance.[139] Paymark is considering the use of FRT as a means to create a seamless experience for customers when paying for products.[140] "By implementing face recognition as the key step in multi-factor authentication, banks are able to mitigate their exposure to risk and fraud, saving themselves millions of dollars in the process."[141] BNZ uses FRT to allow customers to log into their mobile banking application.[142] Cooperative Bank also uses this technology.[143]

Whatever the improvements to efficiency and customer experience, the privacy of biometric data remains a

131 Harrison Rudolph, Laura M. Moy and Alvaro M Bedoya *Not Ready for Takeoff: Face Scans at Airport Departure Gates* (Georgetown Law Center on Privacy & Technology, 21 December 2017) at 5.

132 Harrison Rudolph, Laura M. Moy and Alvaro M Bedoya *Not Ready for Takeoff: Face Scans at Airport Departure Gates* (Georgetown Law Center on Privacy & Technology, 21 December 2017) at 7.

133 Harrison Rudolph, Laura M. Moy and Alvaro M Bedoya *Not Ready for Takeoff: Face Scans at Airport Departure Gates* (Georgetown Law Center on Privacy & Technology, 21 December 2017) at 11.

134 Qantas "Facial Recognition" www.qantas.com.

135 Some ridesharing companies are considering using facial recognition to confirm that the passenger entering the vehicle is the right passenger and that the driver of the vehicle matches the person who is licensed to drive, all in the name of passenger safety: Grab "Grab partners with Ministry of Transport to implement facial recognition technology in Malaysia" (press release, 11 April 2019).

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

137 Westpac "Westpac EasyID" www.westpac.co.nz.

138 Heartland Bank "Biometrics" www.heartland.co.nz.

139 OriginID "APLY ID: A SaaS solution for AML compliance" www.originid.co.nz/aplyid.

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

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

142 BNZ "Help & Support - Mobile Touch ID, Fingerprint Login and Face ID" www.bnz.co.nz.

143 The Co-operative Bank "Terms and Conditions for our Digital Services" www.co-operativebank.co.nz.

concern. In recognition of these concerns, Paymark stated that "No retailer or third party will have access to any facial identity data".[144]

1.5.6.2 Anti-Money-Laundering

A New Zealand company is designing FRT to be used for Anti-Money Laundering.[145] Their competitor, TICC also offers a similar service.[1] The technology enables Anti-Money Laundering services to verify the identity of their clients and the entire process can be completed online.

FRT is also used in Anti-Money Laundering efforts in the UNITED KINGDOM. SmartSearch, a company that provides Anti-Money Laundering services in the UK introduced FRT to help customers provide visual confirmation of ID in 2020.[146] This is thought to be particularly useful during the Covid-19 pandemic as the process can be carried out remotely.

1.5.7 Retail Security

Businesses are also employing FRT for security purposes. In May 2018 a man was taken aside by staff at a New World supermarket in Dunedin after he was mistakenly identified as a shoplifter.[147] The parent company Foodstuff refused to identify which of its stores were using FRT to identify shoplifters from existing held lists of suspect individuals. Both the Prime Minister and Privacy Commissioner noted concerns around the inaccuracy of the technology based on overseas research, highlighting the need for regulation.[148] Members of the public expressed a range of views.[149]

It has been reported that the Warehouse and Mitre 10 trialling FRT for security purposes in January 2020.[150] During the recent return to Covid-19 Alert Level 3 in the Auckland region, a New World store in Auckland was criticised for asking customers to remove their facemasks briefly when entering the store in order for the FRT to be able to scan their face properly.[151]

Is the future staff-less stores? NEC is working with 7-Eleven in Japan and Taiwan and a pilot of FRT for shopping after-hours. As an example, a 7-Eleven store could be closed from midnight to 5am. Special customers who have enrolled their face can open the door, shop, pay by face and leave the store"[152]

1.5.8 Customer Loyalty/ Tracking

FRT can be used in several contexts in customer loyalty and tracking in the retail environment. In the United States, fast food chains have self-service ordering kiosks – the customer can register using loyalty program and then when they enter the chain and walk towards kiosks, they will be recognised using FRT: "food orders from previous visits are remembered and easily selected again or quickly modified."[153]

FRT is also used to blend the online and offline retail experiences.[154] For example, video analytics data from a retail shop can inform offers for advertising online. Alternatively, browsing behaviour in online shops can inform how retail staff should interact with customers in-store.

FRT used by supermarkets, to identify what products customers are looking at and provide them with further information on them via a digital display.[155] Fonterra has indicated that it is looking into "using facial recognition equipment to see how consumers reacted when trying products".[156] Commentators report "billboards that engage with passing customers by using simplistic facial-recognition software that can identify the costumer

144 Darren Hopper "Facial Recognition - The future of payments?" (9 April 2019) Paymark www..paymark.co.nz.

145 RealAML "RealAML Launches Industry-first Facial Recognition" (press release, 16 July 2020).

146 Rozi Jones "SmartSearch launches facial recognition feature" *Financial Reporter* (online ed, United Kingdom, 5 May 2020).

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

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

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

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

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

152 NEC "Facial Recognition in 2020 – 8 trends to watch out for" (25 November 2019) www.nec.co.nz.

153 Girish Nazhiyath "Looking Customer Loyalty Right in the Face" (2 January 2018) NEC Today www.nectoday.com.

154 Jesse Davis West "3 Ways Future Stores Will Use Face Recognition for Retail" (2019) FaceFirst www..facefirst.com.

155 NEC "Facial Recognition in 2020 – 8 trends to watch out for" (25 November 2019) www.nec.co.nz.

156 Jono Galuszka "NZ must target the top products" *Manawatu Standard* (Palmerston North, 18 March 2017).

gender, age, and even their mood. By this information gathering the billboard can offer a real time personalized advertising."[157]

FRT may be used in in advertising and marketing. For example, in Italy, at a train station, there were digital advertising screens that had FRT equipped cameras. The cameras gathered information on people walking past including detecting human faces, how long people looked at the advertising for, information on gender, age range, distance from column, one of five facial expressions that range from happy to sad. This information was used to carry out statistical analysis that identified the level of satisfaction of the advertisements. However, this uses face detection algorithms and not FRT.

It has been reported that:

> "emotional analytics company Realeyes has been helping advertisers code the attention levels and emotional reactions viewers have to their campaigns. Typically, 200 to 300 participants are paid to take part through their own computer webcams or mobile devices. They must consent to having their reactions analyzed in real time as they watch videos… Media executives use the data to see, for example, if there is a dip in attention at a point in an advertisement. They can then alter the media or just push their most effective videos while dropping the others."[158]

1.5.9 Smart Cities

NEC has been partnering with local governments in New Zealand to develop "smart city" capabilities.[159] In Wellington, trials were held with sensor cameras that could detect screaming, paint fumes from graffiti and identify groups that may end up in fights.[160] NEC's technologies do have FRT capabilities, however these are not currently used by local government in New Zealand.

1.5.10 Attendance Tracking

Churches in various countries around the world are using FRT to track the attendance of their members.[161]

FRT is also being advertised to workplaces as a means of increasing efficiency for payroll management.[162] This may have implications for employment law, particularly where an employee refuses to provide their biometric data to an employer.[163]

1.5.11 Security and Access

FRT may be used for authentication or verification purposes such as entry to secured places e.g. military bases, border crossings, nuclear power plants or to access restricted resources including medical records.[164]

FRT might be used as back-end verification systems to uncover duplicate applications for things such as benefits that require other forms of identification. The United States, New Zealand and Pakistan and other countries have used FRT for applications such as passports and visas.[27]

During the Tampa Super Bowl XXXV in America, stadium goers underwent facial recognition scans as they passed through the stadium turnstiles. Cameras scanned for people on watchlists. It is thought that this was taking advantage of the control in the stadium as people had to pass through turnstiles to enter.[165]

157 Sharon Nakar and Dov Greenbaum "Now you see me. Now you still do: Facial Recognition Technology and the growing lack of privacy" (2020) 23 JOSTL 88.

158 Arthur Piper "ABOUT FACE: The Risks and Challenges of Facial Recognition Technology" (2019) Risk Management 18.

159 NEC "NEC New Zealand, providing smart city solutions to the Wellington City Council to create smart city" www..nec.com.

160 Collette Devlin "Wellington City Council and NEC camera technology watching commuters" *Stuff* (online ed, New Zealand, 7 April 2016).

161 Mary-Ann Russon "30 churches around the world using facial recognition to track congregants that skip services" *International Business Times* (online ed, United States, 26 June 2015).

162 Ramco "Ramco Systems drives Payroll modernization across Australia & New Zealand" (April 2019) www.ramco.com.

163 See *Fensom v KME Services NZ Pty Limited* [2019] NZERA Christchurch 728, where the employee refused to use 'Timecloud' a timecard facial recognition system. The ERA found that the dismissal of this employee was unjustified as the employer had not acted reasonably in implementing the system without appropriate consultation and safeguards.

164 Lucas D Introna and Helen Nissenbaum *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (The Center for Catastrophe Preparedness and Response, July 2009).

165 Lucas D Introna and Helen Nissenbaum *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (The Center for Catastrophe Preparedness and Response, July 2009); and Vickie Chachere "Biometrics Used to Detect Criminals at Super Bowl" *ABC News* (online ed, Australia, 8 January 2006).

FRT may be used to unlock people's phones, instead of a password or pin number e.g. Apple's face ID.[166] Some argue that this is normalising the use of FRT for people, making them more comfortable with its use in other places.

FRT may be used in hotels and resorts to identify people at check-in, access to their rooms, spa, dining etc.[167]

It has been reported that a bus safety system can scan drivers' eyes to see where they are looking, if they are paying sufficient attention to the road or whether they are distracted or tired.[168]

1.5.12 FRT in Educational Settings

Educational settings, such as schools and universities utilise FRT to track attendance and monitor students.

1.5.12.1 FRT in schools

Education providers in New Zealand have looked to FRT as a means of monitoring attendance.[169]

The technology is used in some US schools for security, automated registration and assessing student engagement.[170] It is often advertised to schools as a safety tool, particularly to help prevent school shootings. The use of FRT in schools is one of the public settings in which we are seeing the implementation of the technology at scale.[171]

In China, the technology has been used to catch students cheating in high school exams.[172]

In Sweden, the Data Protection Authority has begun fining schools for using FRT in roll-call systems. This is in part due to the inability of students to freely give consent to their use.[173]

Even in New Zealand, discussion has begun around the use of FRT to track attendance in schools.[174] The technology could help address issues of truancy and the social costs that come with it, although some are sceptical as to how effective this would be.

Many concerns over the use of FRT in schools have been raised. These include privacy concerns, the effect of FRT in children's development, and the potential amplification of current inequalities in school systems, particularly considering the greater inaccuracies that have been found in identifying people of colour.[175]

Consequently, protests over the use of FRT in schools and universities have begun to arise. In March 2020, students in New York protested the use of surveillance cameras and FRT in public schools.[176] Concerns were raised that the use of FRT put students' identities at risk. Further, there was a lack of transparency and regulation by the FRT companies around who had access to and controlled the facial images of children and how these images may be used in the future.

166 Apple "Use Face ID on your iPhone or iPad Pro" (20 May 2020) www.support.apple.com.

167 NEC "Facial Recognition in 2020 – 8 trends to watch out for" (25 November 2019) www.nec.co.nz.

168 NEC "Facial Recognition in 2020 – 8 trends to watch out for" (25 November 2019) www.nec.co.nz.

169 Jessica Long "Facial recognition trial at tertiary providers could lead to wider use in schools" *Stuff* (online ed, New Zealand, 26 February 2019).

170 Mark Andrejevic and Neil Selwyn "Facial recognition technology in schools: critical questions and concerns" (2020) 45 Learn Media Technol 115.

171 Mark Andrejevic and Neil Selwyn "Facial recognition technology in schools: critical questions and concerns" (2020) 45 Learn Media Technol 115 at 118.

172 Stella Qiu and Ryan Woo "Chinese exam authorities use facial recognition, drones to catch cheats" *Reuters* (online ed, Bejing, 8 June 2017).

173 Mark Andrejevic and Neil Selwyn "Facial recognition technology in schools: critical questions and concerns" (2020) 45 Learn Media Technol 115 at 120.

174 Jessica Long "Facial recognition trial at tertiary providers could lead to wider use in NZ schools" *Stuff* (online ed, New Zealand, 26 February 2019).

175 Nila Bala "The danger of facial recognition in our children's classrooms" (2020) 18 DLTR 249 at 249.

176 Shawna De La Rosa "New York City students protest school surveillance cameras" (25 March 2019) Education Dive www.. educationdive.com.

1.5.12.2 FRT and Universities

In university settings, FRT has found some new uses. Some consent apps aimed at university students utilise FRT.[177]

The use of FRT has also been widely contested on college campuses, particularly in the US. On 2 March 2020, students at US universities organised a national day of action to protest the use of FRT on college campuses in the US.[178] More than 150 university faculty members, staff and researchers in the US signed an open letter against the use of FRT on college campuses.[179] They claimed that students should not have to compromise their right to safety and privacy for their education. Following protests at UCLA, the college decided not to implement any FRT on campus.[180]

In January 2020, Waikato University opened a tender to upgrade their campus CCTV and Surveillance Systems that sought "AI and Analytics driven solutions", including use of FRT for attendance tracking."[181]

1.5.13 FRT And Combatting Crimes Against Children

FRT is used to combat crimes again children in several ways. In North America, a non-profit organisation uses FRT to identify and prevent child pornography and sex trafficking.[182] The technology can compare images of missing children with advertisements for sexual services, identifying any matches and alerting authorities.

In Australia last year, the Department of Home Affairs suggested that FRT could be used to verify that viewers of pornography were over the age of 18 to protect young people from harmful content.[183]

However, accuracy issues exist around using FRT on images of children. Some studies of the technology suggest that FRT is less accurate when it comes to identifying younger people.[184]

1.5.14 Gambling and Casinos

Casinos were one of the earliest adopters and most widespread users of FRT. Casinos can use FRT for security purposes, identifying cheaters or advantage players when they arrive on the premises and alerting casino staff.[185] Further, FRT can help casinos to meet their obligations to minimise harm from gambling by identifying people who have opted to be placed on self-exclusion lists or individuals who are underage.[186]

SkyCity is using FRT to record customer visitation to ensure that they can support the Ministry of Health with contact tracing if required.[187]

One New Zealand based company, Reveal, provides data and analytics services to a number of casinos including Marina Bay Sands in Singapore.[188]

1.5.15 Agriculture, Companion Animals and Conservation

There have been some quintessentially New Zealand adaptations of FRT. The agricultural sector, particularly sheep farming, is beginning to realise the value of

177 John Danaher "Could There Ever be an App for that? Consent Apps and the Problem of Sexual Assault" (2018) 12 Crim Law Philos 143 at 150.

178 Kari Paul "'Ban this technology': students protest US universities' use of facial recognition" *The Guardian* (online edition, United Kingdom, 3 March 2020).

179 "Fight for the Future: More Than 150 College Faculty Staff Sign Open Letter Against Facial Recognition on Campus" *Targeted News Service* (online ed, New York, 28 February 2020).

180 Laura Hautala "UCLA cancels on-campus facial recognition program after backlash" (19 February 2020) CNET www.cnet.com.

181 University of Waikato "RFI - Smart Systems Development & Integration - CCTV Surveillance Systems" (17 January 2020) Government Electronic Tender Service www.gets.govt.nz.

182 Tom Simonite "How Facial Recognition Is Fighting Child Sex Trafficking" *Wired* (online ed, United States, 19 June 2019).

183 Ariel Bogle "Porn age filter for Australia recommended by parliamentary committee" *ABC News* (online ed, Australia, 5 March 2020).

184 Lindsey Barrett "Ban Facial Recognition Technologies for Children - And for Everyone Else" (2020) 26 JOSTL 223 at 258.

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

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

187 Rebecca Moore "Two Auckland men pass police checkpoint to go to Hamilton casino amid Level 3 restrictions" *One News* (online ed, New Zealand, 17 August 2020).

188 Reveal "Customer Engagement Systems" www..reveal.co.nz.

FRT in the identification of livestock.[189] It is likely that such technology could provide another method of detecting sheep rustling, which can have a significant impact on farmers as "estimates put losses to rustling at $120million a year".[190]

Pets in New Zealand are also purportedly reaping the potential rewards with FRT being used for reuniting lost pets with their owners.[191]

Scientists at Michigan State University created a facial recognition program that could identify individuals in a group of red-bellied lemurs with 98 percent accuracy. It is hoped that this technology could be used in the future to track endangered animal populations.[192] Facial recognition software that can identify individual lions in the wild had been designed in Kenya. It is hoped that this technology will help researchers track the movements of lions throughout Africa, providing an alternative to other tracking technologies that can be expensive and difficult to implement. Similar facial recognition technologies are being used in the conservation of other animals including Bengal tigers, wild chimps and penguins.[193]

FRT could be used to identify and locate predators such as possums and rats in the New Zealand bush. Cameras could help inform conservationists of what predators are left in areas as they move to eradicate them.[194]

1.5.16 FRT and Covid-19

FRT is being adopted globally to help prevent the spread of Covid-19.[195] During this pandemic, the public may be more accepting of the risks of FRT in exchange for the health and public safety benefits. FRT is particularly appealing during this time because it provides a non-contact way of collecting biometric data, unlike fingerprints or iris scans. [196] FRT companies are customizing their products to specifically deal with the Covid-19 pandemic. In some jurisdictions, including China and Russia, these programs have been rolled out on a large scale. Privacy advocates are concerned that the panic around Covid-19 will cause the public to turn a blind eye to the privacy risks of FRT.

For example, existing FRT that was planned to be used in airports to provide a touchless experience is likely to be implemented sooner. This is because the touchless technology is thought to help prevent the spread of Covid-19.[197] While some airlines have already started rolling out the technology, interest is up from other airlines and airports due to the pandemic.

A report by UNICEF states that FRT may be used in the following contexts in the Covid-19 response:[198]

- Match an unknown individual (such as someone breaking movement restrictions) against a population database to identify them (one-to many matching) ,
- Monitor movement in public of a known set of individuals (such as positive cases subject to a quarantine order) by matching unknown individuals to a 'watchlist' (one-to-few matching) ,
- Require individuals subject to a quarantine order to download a specific application and upload a 'selfie' each day, used to verify identity, which is matched against the device's location data to ensure compliance with the order (one-to-one facial matching with a stored record that does not necessarily require centralized storage).

189 John McKenzie "Groundbreaking facial recognition software under development in Dunedin – for sheep" *One News* (online ed, New Zealand, 9 July 2019).

190 Richard Davison "Southland farm owners 'extremely gutted' by $65k stock theft" *New Zealand Herald* (online ed, New Zealand, 21 May 2019).

191 Sue Dudman "New tool helps to recover lost pets" *Wanganui Chronicle* (Wanganui, 27 March 2018).

192 Carl Engelking "Facial Recognition Software: The Next Big Thing in Species Conservation?" *Discover* (online ed, United States, 18 February 2017).

193 Marrissa Fessenden "Researchers Are Using Facial Recognition Software To Save Lions" *Smithsonian Magazine* (online ed, United States, 7 July 2015).

194 Artificial Intelligence Research "Facial recognition for conservation" (17 July 2017) www.onartificialintelligence.com.

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

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

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

198 Gabrielle Berman, Karen Carter, Manuel Garcia-Herranz and Vedran Sekara *Digital contact tracing and surveillance during COVID-19: General and child-specific ethical issues* (UNICEF, WP 2020-01, June 2020).

- The Polish government has developed a compulsory app like this.[199] People who are required to quarantine must download the app. The app prompts users to take a selfie at the address they provided to Polish authorities at random times throughout the day, sometimes more than once. Failure to respond to the request within 20 minutes can result in the police coming to a person's residence to check they are there.

1.5.16.1 Russia

The Russian government has used the pandemic as an opportunity to roll out greater surveillance measures in its largest cities.[200] FRT has been used to identify those who are breaching quarantine and isolation rules.[201] In March, authorities reported catching and fining 200 people though the use of this technology.[202] Around the same time, the police chief stated an intention to add 9,000 cameras to the existing network of 170,000 in Moscow.

Russia is also trialling FRT to make payments in grocery stores to reduce physical contact and the spread of the covid-19 virus.[203]

The large FRT system that was rolled out earlier this year had received significant backlash from the public. However, it is believed that the use of the technology to monitor compliance with pandemic restrictions is increasing public acceptance of the technology.[204]

1.5.16.2 China

The Covid-19 pandemic has driven the extensive development and expansion of new uses of FRT in China.

FRT has been combined with thermal imaging technology to help detect those with high temperatures, particularly in public spaces.[205] This can be used by staff in locations with high-density flows of people such as bus stations, train stations and airports.[206] It can also be used to flag those who are not wearing facemasks. This technology has been incorporated into police forces. A police 'smart helmet' uses FRT alongside other technology to alert police to those with fevers, also displaying the subject's name and medical history on the visor.[207]

Chinese authorities have developed an app that uses FRT to track the users' movements, as well as those in their proximity so that either can be tested should the other return a positive test for the virus.[208] Another app categorises citizens into red, yellow and green codes, depending on their contact with Covid-19. Some residential area access control systems use FRT to prevent those without a green code from entering.[209]

FRT is also used to monitor the movements of those in quarantine and isolation. Police used FRT to identify a man in Hangzhou who had breached his quarantine after returning home after a business trip.[210]

In March, a 'Healthcare Bus' was introduced in China. The bus uses FRT and infrared thermal imaging to scan people's faces when they board. The technology alerts the driver if someone with a fever boards and

199 Katri Uibu "Poland is making its citizens use a 'selfie' app during the coronavirus crisis" *ABC News* (online ed, Australia, 25 April 2020).

200 Eliza Mackintosh "What you need to know about coronavirus on Monday, March 30" *CNN* (online ed, United States, 30 March 2020).

201 Luke McGee "Power-hungry leaders are itching to exploit the coronavirus crisis" *CNN* (online ed, United States, 1 April 2020).

202 Luke McGee "Power-hungry leaders are itching to exploit the coronavirus crisis" *CNN* (online ed, United States, 1 April 2020).

203 Chris Burt "Biometric checks and facial recognition payments to support social distancing, fight spread of covid-19" (23 March 2020) Biometric Update www.biometricupdate.com.

204 Mary Ilyushina "How Russia is using authoritarian tech to curb coronavirus" *CNN* (online ed, United States, 29 March 2020).

205 Lily Kuo "'The new normal': China's excessive coronavirus public monitoring could be here to stay" *The Guardian* (online ed, Hong Kong, 9 March 2020).

206 Binoy Kampmark "The Pandemic Surveillance State" *The Scoop* (online ed, New Zealand, 22 March 2020).

207 Oliver Wainwright "10 Covid-busting designs: spraying drones, fever helmets and anti-virus snoods" *The Guardian* (online ed, United Kingdom, 25 March 2020).

208 Afua Hirsch "The coronavirus pandemic threatens a crisis for human rights too" *The Guardian* (online ed, United Kingdom, 19 March 2020).

209 Maya Wang "China: Fighting COVID-19 With Automated Tyranny" (1 April 2020) Human Rights Watch www.hrw.org.

210 Yingzhi Yang and Julie Zhu "Coronavirus brings China's surveillance state out of the shadows" *Reuters* (online ed, United States, 8 February 2020).

also identifies people not wearing facemasks. The bus also has special air vents that can sterilise the vehicle in twenty minutes.[211]

1.5.16.3 New Zealand

The use of FRT to combat the pandemic has not seen such a dramatic update in New Zealand. However, small developments may be noted. New Zealand developers have created an app that uses FRT to enable those in quarantine to self-monitor their health, in an attempt to ease some of the pressure on the healthcare system.[212] Further the wearing of masks in public spaces has been found to reduce the accuracy of FRT.[213]

1.5.16.4 Singapore

In Singapore, FRT is being used to move towards 'touchless' workplaces.[214] Sensors that utilise FRT are used to match the faces of staff, automatically open doors, track attendance and take the temperature of staff.

1.5.16.5 United States

In New York, the Transit Authority called on Apple to update its FRT used for unlocking phones to enable people with masks to do so. This came about amid concerns that people were taking their masks off on public transport to unlock their phones.[215]

1.5.16.6 United Kingdom

FRT has been used in the UK as a way to log into the National Health Service app.[216] Some suggest that it could also be used for Covid-19 'immunity passports.' These 'passports' are a way for people to carry documented proof that they have previously contracted the Covid-19 virus and are consequently immune.

1.5.16.7 Malaysia

The Malaysian palace has installed FRT and thermal imaging to detect and identify people who may be infected.[217]

1.6 CONCLUDING REMARKS

This section has surveyed the many and evolving uses of FRT in Aotearoa and comparable jurisdictions. Our primary interest in this report is the use of FRT by the state, but state use is inevitably tangled with private sector suppliers and transfer of information between state and private sector.

211 Lucy Ingham "Coronavirus-fighting smart bus rolled out in China" *Verdict* (online ed, United Kingdom, 31 March 2020).

212 NEC New Zealand "Kiwi Developers And Global Technology Leader NEC Team Up To Fight Spread Of COVID-19" (press release, 26 March 2020).

213 Matt O'Brien "Covid-19 coronavirus: Pandemic masks thwarting face recognition tech" *New Zealand Herald* (online ed, New Zealand, 28 July 2020).

214 Asia Corporate News Network - ACN Newswire "The Ramco Innovation Lab Singapore Demos Touch-less Attendance System With Thermal Scan" (press release, 19 March 2020).

215 Leah Asmelash "New York's MTA is asking Apple to create a Face ID that works with masks" *CNN* (online ed, United States, 11 August 2020).

216 Jane Wakefield "Coronavirus: NHS app paves the way for 'immunity passports'" *BBC* (online ed, United Kingdom, 26 May 2020).

217 Chris Burt "Biometric checks and facial recognition payments to support social distancing, fight spread of covid-19" (23 March 2020) Biometric Update www.biometricupdate.com.

SECTION 2

THE HUMAN RIGHTS FRAMEWORK – RIGHTS AND REMEDIES

2.1 INTRODUCTION

The overarching issue for this report is an analysis of the threats FRT poses to human rights and consequently what the appropriate parameters of its use may be. The primary lens for this analysis is the human rights framework, which is derived from both national and international sources. The section which follows considers existing ethical frameworks and other standards. These sections frame the discussion of threats to human rights (section 4) and existing and potential regulation (sections 5, 6 and 7).

In this section we consider issues such as:

- What human rights are relevant in considering the use of FRT,
- The source of these rights,
- How people enforce their rights and seek remedies if those rights are affected by the use of FRT.

The focus is on the human rights framework of Aotearoa New Zealand, but with some comparative material where relevant.

2.2 WHAT HUMAN RIGHTS MAY BE IMPACTED BY FRT?

Human rights are the basic rights and freedoms that all people are entitled to. A person's human rights arise from a mixture of international and national sources.

The impact of technology, artificial intelligence and data-driven decision-making is a fast-evolving area of human rights analysis:[1]

> The impact of Artificial Intelligence (AI) on human rights is one of the most crucial factors that will define the period in which we live. AI-driven technology is entering more aspects of every individual's life, from smart home appliances to social media applications, and it is increasingly being utilised by public authorities to evaluate people's personality or skills, allocate resources, and otherwise make decisions that can have real and serious consequences for the human rights of individuals…finding the right balance between technological development and human rights protection is therefore an urgent matter.[2]

The specific threats that FRT may pose to a person's human rights are explored more thoroughly in a later chapter. But, it is worth listing here which rights could be affected, before considering the sources and enforceability of these rights.[3]

Some of the principal areas of human rights that may be affected by the use of FRT are as follows:

- Freedom of thought, conscience and religion (e.g. where facial recognition systems are used to monitor protests);
- Freedom of expression (e.g. where facial recognition systems are used to monitor protests);
- Freedom of assembly and association (e.g. where facial recognition systems are used to monitor protests);
- Freedom of movement (e.g. where facial recognition systems are used in border control);
- Freedom from discrimination (e.g. where facial recognition systems run on biased algorithms);
- Privacy/respect for private life (e.g. where facial recognition equipped cameras are used in public spaces);

1 See Mathias Risse "Human rights and artificial intelligence: An urgently needed agenda" (2019) 41 HRQ 1; Steven Livingston and Mathias Risse "The future impact of artificial intelligence on humans and human rights" (2019) 33 Ethics Int Aff 141; and Janneke Gerards "The fundamental rights challenges of algorithms" (2019) 37 NQHR 205.

2 Council of Europe Commissioner for Human Rights *Unboxing Artificial Intelligence: 10 steps to protect Human Rights* (Council of Europe, May 2019).

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

- 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 facial recognition is used in surveillance by the police);
- Minimum standards of criminal procedure (e.g. where evidence of identity from a facial recognition match is sought to be introduced into evidence).

To better understand the threats to human rights that may be posed by FRT, and to better frame the recommendations made, this section will outline the various general human rights standards as well as those targeted to groups such as indigenous peoples, children and persons with disabilities.

2.3 NEW ZEALAND'S CONSTITUTIONAL STRUCTURE

Unlike some other jurisdictions which are referred to in this report, Aotearoa New Zealand does not have a written constitution. In the introduction to the Cabinet Manual, Sir Kenneth Keith describes the constitution thus:[4]

> The New Zealand constitution is to be found in formal legal documents, in decisions of the courts, and in practices (some of which are described as conventions). It reflects and establishes that New Zealand is a constitutional monarchy, that it has a parliamentary system of government, and that it is a democracy. It increasingly reflects the fact that the Treaty of Waitangi is regarded as a founding document of government in New Zealand. The constitution must also be seen in its international context, because New Zealand governmental institutions must increasingly have regard to international obligations and standards.

The Treaty of Waitangi signed by Māori and by the British Crown in 1840, is considered the founding document of Aotearoa.[5] Any discussion of existing or proposed regulation must consider the implications for the continuing Treaty partnership between the contemporary State and Māori. The principles derived from the Treaty include protection, partnership, a duty to act in good faith, a duty to consult, and that the Treaty is an agreement that may be adapted for new circumstances.[6] Commentators have cautioned that "dominant Westernised conceptualisations of rights have been criticised for their ties to colonialism and individualistic focus."[7] Palmer and Butler, who have published a draft Constitution for Aotearoa/New Zealand would set out the bi-cultural values underpinning the state as based on:

> "…freedom and opportunity; on human dignity and tolerance; on kaitiakitanga [guardianship] and sustainability; on mana and tikanga Māori [customary practices]; on a sound economy; on fairness and equality; on a strong sense of community, human compassion and the family, especially the care of children; on the responsible use of authority; and upon democracy:"[8]

Further, New Zealand follows a dualist model, where international treaties (such as international human rights treaties) must be formally incorporated before they are considered binding.[9] Another highly relevant consideration is that New Zealand does not have an over-arching or supreme bill of rights under which rights may be protected.[10] There are two relevant pieces of ordinary statute – the *New Zealand Bill of Rights Act 1990* (which sets out key civil and political rights derived from the International Convention on Civil and Political

4 Kenneth Keith "Introduction" in Cabinet Office, Department of the Prime Minister and Cabinet *Cabinet Manual* (Wellington, 2017).

5 Matthew Palmer *The Treaty of Waitangi in New Zealand's Law and Constitution* (Victoria University Press, Wellington, 2008); and Janet McLean "Crown Him with Many Crowns: The Crown and the Treaty of Waitangi." (2008) 6 NZJPIL 35.

6 Janine Hayward '"Flowing from the Treaty's Words": The Principles of the Treaty of Waitangi', in Janine Hayward and Nicola R Wheen (eds) *The Waitangi Tribunal: Te Roopu Whakamana i te Tiriti o Waitangi* (Bridget Williams Books, Wellington, 2004) 29.

7 Paula King, Donna Cormack and Mark Kopua "Oranga Mokopuna-A tāngata whenua rights-based approach to health and wellbeing" (2018) 7 MAI Journal 187.

8 Andrew Butler and Geoffrey Palmer "The Proposed Constitution" (2016) Constitution Aotearoa NZ: 2017 Archive www.archive.constitutionaotearoa.org.nz.

9 Alberto Costi (ed), *Public International Law: A New Zealand perspective* (Wellington, LexisNexis, 2020) chs 4 and 11.

10 Margaret Wilson *The Struggle for Sovereignty: New Zealand and Twenty-First Century Statehood* (Bridget Williams Books, Wellington, 2015); and Janet McLean "Legislative invalidation, human rights protection and s 4 of the New Zealand Bill of Rights Act" (2001) NZL Rev 421.

Rights) and the *Human Rights Act 1993* (largely focussed on the right to be free from discrimination). These are discussed in more detail below.

These pieces of legislation are not accorded any special status, and the Government may (and often does[11]) enact legislation which is inconsistent with the rights set out in these Acts. As Palmer and Butler emphasise "these laws are therefore vulnerable to being overridden by a bare parliamentary majority. This vulnerability is not theoretical or fanciful."[12] The United Nations Human Rights Committee has called on New Zealand to strengthen its bill of rights.[13]

2.4 THE DOMESTIC HUMAN RIGHTS FRAMEWORK

2.4.1 New Zealand Bill of Rights Act 1990

The *New Zealand Bill of Rights Act* 1990 (NZBORA) was enacted in 1990. The Preamble of the NZBORA describes its purpose as the affirmation and promotion of human rights and fundamental freedoms and the expression of New Zealand's commitments to the International Convention on Civil and Political Rights. The aim of the NZBORA is to 'create a set of rights for individuals which limit the power of executive, government and public actors'.[14] NZBORA qualifies the exercise of rights through s 5: "reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." It reflects 'rights and freedoms long established in the Anglo-New Zealand tradition'.[15] The Canadian Charter of Rights and Freedoms had a significant influence on the drafting of the NZBORA.[16]

2.4.1.1 Status of the NZBORA

NZBORA differs from similar instruments in other jurisdictions,[17] in that it is not 'supreme law' and cannot be used by the Courts as a basis to strike down legislation.[18] A statutory meaning consistent with the rights protected in the NZBORA is preferred.[19] However, if there is a direct conflict with the terms of the statute, the statute will remain in force.[20] That situation has been criticised by the United Nations Human Rights Committee.[21] The NZBORA can be considered to be an expression of fundamental values. It may be used in the purposive interpretation of legislation,[22] and as a 'benchmark for acceptable governmental conduct and law'.[23] Pursuant

11 Geoffrey Palmer and Andrew Butler *Constitution for Aotearoa New Zealand* (Victoria University Press, Wellington, 2016) at 163, citing over 30 instances of this occurring in the period 1990-2016.

12 Geoffrey Palmer and Andrew Butler *Constitution for Aotearoa New Zealand* (Victoria University Press, Wellington, 2016) at 162.

13 *Concluding Observations of the United Nations Human Rights Committee on New Zealand* CCPR/C/NZL/CO/6 (31 March 2016) at [10(a)] and [10(c)].

14 Ministry of Justice *Re-Evaluation of the Human Rights Protections in New Zealand* (2000) at [25].

15 Paul Rishworth, Grant Huscroft, Scott Optician and Richard Mahoney *The New Zealand Bill of Rights* (Melbourne: Oxford University Press, 2003) at 1.

16 Geoffrey Palmer "A Bill of Rights for New Zealand: A White Paper" [1984-1985] I AJHR A6; and Kenneth J Keith '"Concerning Change": The Adoption and Implementation of the New Zealand Bill of Rights Act 1990" (2000) 31 VUWLR 37.

17 United States Constitution; Canadian Charter of Rights and Freedoms, pt 1 of the Constitution Act 1982, being sch B to the Canada Act 1982 (UK); and Constitution of Ireland.

18 The White Paper 'A Bill of Rights for New Zealand' (1985) proposed the enactment of a Bill of Rights that would have the power to strike down inconsistent legislation, but this was not met with approval by the Parliamentary Select Committee on Justice and Law Reform. See Final Report of the Justice and Law Reform Select Committee "On a White Paper of a Bill of Rights for New Zealand" [1998] AJHR 3. See also Claudia Geiringer "The Principle of Legality and the Bill of Rights Act: A Critical Examination of *R v Hansen*" (2008) 6 NZJPIL 59.

19 New Zealand Bill of Rights Act 1990, s 6.

20 New Zealand Bill of Rights Act 1990, s 4. See also Ministry of Justice *Re-evaluation of the Human Rights Protections in New Zealand* (2000).

21 *Concluding Observations of the United Nations Human Rights Committee on New Zealand* CCPR/C/SR. 2026 (17 July 2002). See also Janet McLean "Legislative Invalidation, Human Rights Protection and s 4 of the New Zealand Bill of Rights Act" (2001) 4 NZ L Rev 421; and Claudia Geiringer "Inaugural Lecture: Mr Bulwark and the Protection of Human Rights" (2014) 45 VUWLR 367 at 385.

22 See *Flickinger v Crown Colony of Hong Kong* [1991] 1 NZLR 439.

23 Paul Rishworth, Grant Huscroft, Scott Optician and Richard Mahoney, *The New Zealand Bill of Rights* (Melbourne: Oxford University Press, 2003) at 26.

to s. 7 of NZBORA, the Attorney-General may report the results of a 'rights vetting' for any legislation before Parliament.[24]

2.4.1.2 Options for an Individual Whose Rights Under NZBORA Have Been Breached

Further sections will illustrate the potential threats which FRT can pose to individual and collective rights. It is worth a brief exploration about how individuals may use NZBORA where they believe their rights have been breached. In other jurisdictions, individuals may use domestic human rights legislation to advance a judicial review of the effect of a piece of legislation or policy affecting their rights. This has been the case in the *Bridges* decision, which is discussed in more detail in Section 4. Here, Mr Bridges alleged that the use of an automated facial recognition technology system had breached his right to a private life.[25]

New Zealand's system does not allow the same pathways for an individual to seek recognition and redress for a breach of human rights. The NZBORA does not presently have a provision which empowers a declaration of inconsistency or incompatibility.[26] This is unlike other jurisdictions (for instance, Ireland).[27] Petrie has discussed the distinction between 'indications of inconsistency' and 'declarations of inconsistency'.[28] 'Indications of inconsistency' occur where "a judge pronounces or otherwise concludes that a statutory provision breaches a protected human right or civil liberty".[29] This does not strike down the legislation, merely indicates that it is inconsistent. There are a number of examples of situations where the courts have made indications of inconsistency.[30] By comparison, a 'declaration of inconsistency' occurs where "a judge reaches a similar conclusion to that within an IoI [indication of inconsistency], but then issues a formal declaration that the statutory provision gives rise to a rights breach."[31]

In 2010, Parliament passed legislation which restricted all convicted prisoners from voting.[32] Previous to this amending legislation, only prisoners convicted and sentenced to terms of imprisonment for three years or more lost the ability to vote. This Bill was vetted and declared to be contrary to the Bill of Rights under s. 7, but the Bill proceeded to legislation regardless. In *Taylor v Attorney-General*,[33] the claimants sought a declaration that the amending legislation was inconsistent with section 12(a) of the Bill of Rights Act and could not be justified under s. 5: "reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".

At the High Court, Heath J found that:[34]

> Where there has been a breach of the Bill of Rights there is a need for a Court to fashion public law remedies to respond to the wrong inherent in any breach of a fundamental right. Should the position be any different in respect of the legislative branch of Government? In my view, the answer is "no".

On appeal to the Supreme Court, the majority of the Supreme Court held that the High Court did have the power to make such a declaration.[35] The three primary reasons supporting the decision was that there was an inconsistency with the *Human Rights Act*

24 Catherine Rodgers "A Comparative Analysis of Rights Scrutiny of Bills in New Zealand, Australia and the United Kingdom: Is New Zealand Lagging Behind its Peers?" (2012) 21 APR 4; and Grant Huscroft "The Attorney-General's Reporting Duty" in Paul Rishworth, Grant Huscroft, Scott Optican and Richard Mahoney (eds) *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003). See also Janet L Hiebert "Rights-vetting in New Zealand and Canada: similar idea, different outcomes" (2005) 3 NZJPIL 63.

25 *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

26 Tom Hickman "Bill of Rights Reform and the Case for Going Beyond the Declaration of Incompatibility Model" [2015] NZ L Rev 35.

27 Gerard W. Hogan,, and Gerry Whyte. *The Irish Constitution*. LexisNexis/Butterworths, 2003.

28 Nicholas Petrie "Indications of Inconsistency" (2019) 78 CLJ 612.

29 Nicholas Petrie "Indications of Inconsistency" (2019) 78 CLJ 612 at 613.

30 *Moonen v Film and Literature Board of Review* [2000] 2 NZLR 9 (CA); Claudia Geiringer "On a Road to Nowhere: Implied Declarations of Inconsistency and the New Zealand Bill Of Rights Act" (2009) 40 VUWLR 613; and Claudia Geiringer "The Dead Hand of the Bill of Rights? Is the New Zealand Bill of Rights Act 1990 a Substantive Legal Constraint on Parliament's Power to Legislate?" (2007) 11 OLR 389.

31 Nicholas Petrie "Indications of Inconsistency" (2019) 78 CLJ 612 at 615.

32 Electoral (Disqualification of Convicted Prisoners) Amendment Act 2010.

33 *Taylor v Attorney-General* [2015] NZLR 791.

34 *Taylor v Attorney-General* [2015] NZLR 791 at [61].

35 *Attorney-General v Taylor* [2018] NZSC 104.

which empowers the Human Rights Tribunal to make a declaration of inconsistency, that there had been a commitment under the International Convention on Civil and Political Rights to provide an effective remedy for breaches of human rights, and that the making of the declaration is a real remedy which is consistent with the usual function of the courts.[36]

A bill which is currently before Parliament (*Bill of Rights (Declaration of Inconsistency) Amendment Bill 2020)* will provide a mechanism whereby the Government may consider and potentially respond to a declaration of inconsistency under the NZBORA or the *Human Rights Act*. It is intended to further the constitutional relationship of mutual respect between Parliament and the judiciary,[37] and was announced before the Supreme Court had handed down the decision in Taylor. The bill would require the Attorney- General to report to Parliament soon after a declaration of inconsistency is made by a Court.[38]

In addition, the Courts have extended the ambit of the NZBORA to provide a range of remedies for breaches of rights despite the fact that Parliament did not include any express mention of remedies in the BORA.[39] *Simpson v Attorney-General [Baigent's Case]* involved an appeal against the High Court striking out of the appellant's cause of action against the police for an alleged unreasonable search of a dwelling.[40] One of the appellant's claimed causes of action was that the police had breached s 21 of the BORA by conducting an unreasonable search of the dwelling. The Court of Appeal held that damages could be awarded despite the express absence of a remedies provision in the NZBORA. The usual remedy for such a breach, namely the exclusion of the evidence in question, was not considered appropriate, as the appellant was innocent of any wrongdoing. This judgment demonstrated the Court's willingness to take a purposive approach to human rights legislation, and recognition on the part of the Courts that effective remedies should be available for breaches of rights.[41]

2.4.2 The Human Rights Act 1993

Another relevant piece of domestic human rights legislation is the *Human Rights Act* 1993 (HRA). The HRA protects people in New Zealand from discrimination on a number of grounds including ethnic or national origin, race, sex, political opinion, amongst others.[42] It applies to the public sector (with some limitations)[43] and the private sector, in matters such as employment, education, provision of services and membership of organisations.

The HRA could be relevant where a person alleges a FRT system was used in a discriminatory manner. Individuals who allege that their rights have been breached may make a claim to the Human Rights Review Tribunal,[44] but must have made a claim to the Human Rights Commission first.[45]

36 John Ip "Attorney-General v Taylor: A Constitutional Milestone?" [2020] NZ L Rev 35.

37 Bill of Rights (Declaration of Inconsistency) Amendment Bill 2020 (230-1) (explanatory note) at 1-2.

38 Bill of Rights (Declaration of Inconsistency) Amendment Bill 2020 (230-1) (explanatory note), cl 4.

39 In fact, in a number of cases, the Courts have commented that the lack of a specific remedies clause in the NZBORA has left the Courts responsibility in according appropriate remedies where there are proven violations unimpeded. See for example *R v Butcher* [1992] 2 NZLR 257 (CA) at 269 per Gault J; *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA) at 718 per McKay J; and *R v Shaheed* [2002] 2 NZLR 377 (CA) at 410 per Blanchard J. If the Courts were unable to grant remedies for a breach, the NZBORA would be tantamount to "window-dressing": *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA) at 691 per Casey J. See also *R v Goodwin* [1993] 2 NZLR 153 (CA) at 191; and *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667 (CA) at 717 per McKay J.

40 *Simpson v Attorney-General [Baigent's Case]* [1994] 3 NZLR 667.

41 See also the comments of the Supreme Court in *Taunoa v Attorney-General* [2007] NZSC 70, which upheld and consolidated *Baigent's Case*. Elias CJ and McGrath J considered that the ICCPR imposes a responsibility on State Parties to provide an effective remedy for breaches of human rights in their domestic legal systems (at [106] and [364]–[365]). Recent cases where damages have been awarded under NZBORA in relation to treatment by Police and correctional officers include *Attorney-General v Udompun* [2005] 3 NZLR 204; *Greenwood v Attorney-General* [2006] DCR 586; *Beagle v Attorney-General* [2007] DCR 596; *Taunoa v Attorney-General* [2007] NZSC 70, [2008] 1 NZLR 429; *Oosterman v Attorney-General* DC Rotorua CIV-2006-063-384, 1 July 2008; and *Van Essen v Attorney-General* [2013] NZHC 917, [2014] NZAR 809.

42 Human Rights Act 1993, s 21.

43 Part 11- e.g. for employment in national security, people with certain disabilities can be discriminated against, as well as people aged less than 20 (s 25).

44 See Part 4 of the Human Rights Act 1993.

45 Human Rights Commission "How to make a complaint" www.hrc.co.nz.

2.5 PRIVACY LEGISLATION AND PRINCIPLES

A later section considers the application of the privacy regime in more detail.

The *Privacy Act 1993* (and its successor the *Privacy Act 2020* coming into force on 1 December 2020) is a flexible legislative regime that permits almost all personal information activities but places limits through the privacy principles (Informational Privacy Principles, IPPs) and places activities under the 'jurisdiction' of the Privacy Commissioner. IPPs regulate collection, processing, using and disclosure of personal information either by private companies or by public authorities. That means that every operation on information comprising human faces, such as photograph or video, requires compliance with those principles.

The IPPs do not confer on an individual any right that is enforceable in a court of law, except for the right to confirmation whether a public sector agency holds any personal information about individual and right to access to that information.[46] Individuals who believe that an organisation has interfered with their privacy should raise this with the organisation concerned in the first instance. If unsatisfied, the individual can make a complaint to the Privacy Commissioner, and then to the Human Rights Review Tribunal.[47]

The relationship between s 21 NZBORA (the right to be free from unreasonable search and seizure) and the privacy principles was a subject of the Supreme Court decision in *R v Alsford*.[48] The majority in that case held that even if personal information was obtained by means of a breach of the privacy principles, that fact may be not relevant to the infringement of s 21 and to the admissibility of the evidence based on that personal information. The infringement of s 21 should be assessed only based on the existence of reasonable expectations of privacy which makes the search 'unreasonable'.[49] The consequence of *Alsford* is that Police may simply request and obtain from the third party without a production order the personal information as to which there is no reasonable expectation of privacy. It is worth noting that Elias CJ in a minority decision expressed reservations to the restriction of applicability of s 21. She expressed a 'provisional view' that access to personal information with the breach of principles related to disclosure of the *Privacy Act 1993* constituted unreasonable search and seizure.[50]

2.6 INTERNATIONAL HUMAN RIGHTS STANDARDS

People in New Zealand have a range of human rights which arise from international law. Some are incorporated into domestic law (as foreshadowed above), others are given strength through judicial application. Again, the application of international human rights law to the area of technologies such as FRT is a developing field.[51]

2.6.1 Status of International Instruments in New Zealand Law

New Zealand has a dualist system.[52] The dualist theory of international law describes domestic law and international law as two distinct legal systems. International law governs relationships between states while domestic law governs national relationships between individuals, and with Government.[53] For an international treaty to be binding, it must be incorporated into international law.

As to the effect of unincorporated treaties in a dualist system, in the 1994 decision in *Tavita*, concerning the

46 Privacy Act 2020, s 31.

47 Part 5, Privacy Act 2020.

48 *R v Alsford* [2017] NZSC 42.

49 See *R v Alsford* [2017] NZSC 42 at [73]. The personal information in question was the energy consumption information requested from energy providers.

50 At [123].

51 Lorna McGregor, Daragh Murray and Vivian Ng "International Human Rights Law as a Framework for Algorithmic Accountability" (2019) 68 ICLQ 309.

52 Fiona de Londras "Dualism, Domestic Courts, and the Rule of International Law" in Mortimer Sellers and Tadeusz Tomaszewski (eds) *The Rule of Law in Comparative Perspective* (Springer, Dordrecht, 2010) 217.

53 Andrew Butler and Petra Butler "The Judicial Use of International Human Rights Law in New Zealand" (1999) 29 VUWLR 173.

effect of the Convention on the Rights of the Child in New Zealand, Cooke P stated that:[54]

> A failure to give practical effect to international instruments to which New Zealand is a party may attract criticism. Legitimate criticism should extend to the New Zealand Courts if they were to accept the argument that, because a domestic statute giving discretionary powers in general terms does not mention international human rights norms or obligations, the executive is necessarily free to ignore them.

In *New Zealand Air Line Pilots Association Inc v Attorney-General*, Keith J stated the general principle that it was a "presumption of statutory interpretation" that in "so far as its wording allows legislation should be read in a way which is consistent with New Zealand's international obligations".[55] Thus, although international standards are "very persuasive",[56] they are not binding and they cannot override domestic statutes.[57]

2.6.2 International Convention on Civil and Political Rights

The International Convention on Civil and Political Rights (ICCPR)[58] provides for a range of civil and political rights, most of which are incorporated into the NZBORA.

The concept of 'dignity' specifically mentioned in the ICCPR's preamble may be particularly relevant to the collection and comparison of facial images:

> "Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,
>
> Recognizing that these rights derive from the inherent dignity of the human person"

A report by the European Union notes that processing of facial images may affect human dignity in the following ways: [59]

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

Article 17 of the ICCPR also 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."

2.6.3 Children's Rights

The implications of FRT for the rights and interests of children and young persons (those aged less than 18) are discussed in a number of places in this report. Children and young persons, as human beings, are rights-holders, and should receive the same minimum standards of human rights protections as adults. Nonetheless, children and young persons have a specialized human rights treaty (the United Nations Convention on the Rights of the Child[60]) which recognises the particular vulnerabilities and characteristics of children and young persons.

54 *Tavita v Minister of Immigration* [1994] 2 NZLR 257 (CA) at 266.

55 *New Zealand Air Line Pilots' Association Inc v Attorney-General* [1997] 3 NZLR 269 (CA) at 289.

56 *Second Periodic Report of New Zealand to the Committee on the Rights of the Child* CRC/C/93/Add.4 (2003) at [123].

57 Legislation Design and Advisory Committee *Legislation Guidelines: 2018 Edition* (March 2018) at [9.2].

58 International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49.

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

60 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.

New Zealand has not formally incorporated the Convention on the Rights of the Child (CRC) into domestic law.[61] The CRC has been regularly cited in argument in the New Zealand courts, principally in family law,[62] youth justice[63] and immigration law[64] cases but also other spheres such as freedom of expression.[65]

Some key principles of the CRC may be summarised thus:[66]

- Best interests: the best interests of the child or young person are a primary consideration in all decisions;
- Participation: the child or young person's effective participation is promoted in matters affecting them, and their views are taken into account in any decisions made;
- Non-discrimination: the state does not further perpetrate discrimination, and is cognisant of the needs and particular characteristics of groups such as ethnic minorities, indigenous peoples and children with disabilities.

The most relevant rights are probably those related to children in the criminal justice system (in terms of surveillance in relation to alleged offending or use as evidence), but children involved in protest movements and children in educational settings could also be affected by use of FRT. For any use in criminal justice and by police, international standards for children's rights require that there is a:[67]

- Reintegrative focus: any outcomes and processes must aim to reintegrate the young person so that they may take part in society, and avoid punitive and stigmatising processes and sanctions.

The rights of the child in the digital environment is an issue of contemporary importance,[68] with human rights bodies expressing concern about the impact of emerging technologies and surveillance the impact on the child's right to privacy and the right to freedom of expression.[69]

The new General Comment on children's rights in relation to the digital environment (in draft format) as of March 2019 provides commentary on children's rights in these environments.[70] The draft general comment emphasises the importance of the principle of non-discrimination – for particular children, particularly minority, indigenous, refugee and migrant children, LGBQTI and other vulnerable children, the digital environment may be more risky.[71] Ethics, privacy and safety in the digital environment must be respected by

61 There has been some incorporation in the Care of Children Act 2004. For more detail on the relationship between international law and domestic law in New Zealand, see the Law Commission *A New Zealand Guide to International Law and its Sources* (NZLC R34, 1996).

62 *Re the W Children* (1994) 12 FRNZ 548 (FC); *H v F* (1993) 10 FRNZ 486 (HC); and *Hemmes v Young* [2005] NZSC 47, [2006] 2 NZLR 1. See also cases cited in New Zealand's second periodic report to the United Nations Committee on the Rights of the Child due in 2000, discussed in the UN Committee on the Rights of the Child *Consideration of Reports Submitted by States Parties Under Article 44 of the Convention: New Zealand* CRC/C/93/Add.4 (2003) at [127]–[132].

63 *Whitcombe v Police* [2018] NZHC 1409, *DP v R* [2015] NZCA 476. See also lower court decisions: *Police v Ponniah* [2014] DCR 75 (DC) (delay); *Police v ET* [2015] NZYC 412 (delay). *HX v Police* [2019] NZYC 548

64 *Tavita v Minister of Immigration* [1994] 2 NZLR 257 (CA); *Jiang v Chief Executive of the Ministry of Business, Innovation and Employment* [2020] NZHC 1439; *Huang v Minister of Immigration* [2020] NZHC 956; *Ochibulu v Immigration and Protection Tribunal* [2020] NZHC 792; *Zhang v Minister of Immigration* [2020] NZHC 568; *Re AP (Vietnam)* [2020] NZIPT 504805; *Norman v Attorney-General* [2020] NZHC 336.

65 *Moonen v Film and Literature Board of Review* [2002] 2 NZLR 754 (CA); and *Child Youth and Family Services v Television New Zealand Ltd* (2005) 24 FRNZ 857 (HC).

66 Children's Convention Monitoring Group, *Getting It Right – Building Blocks - Building The Foundations For Implementing The Children's Convention In Aotearoa*, April 2018: Retrieved from https://www.occ.org.nz/assets/Uploads/Getting-It-Right-Building-Blocks-Apr-2018.pdf

67 United Nations Committee on the Rights of the Child, *General Comment No. 24 (2019) on children's rights in the child justice system* (CRC/C/GC/24, 18 September 2019). See also Liz Campbell and Nessa Lynch. "Competing paradigms? The use of DNA powers in youth justice." *Youth Justice* 12, no. 1 (2012): 3-18.

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

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

70 UN Committee on the Rights of the Child *Draft General Comment No. 25 (202x): Children's rights in relation to the digital environment* CRC/C/GC/25 (13 August 2020).

71 UN Committee on the Rights of the Child *Draft General Comment No. 25 (202x): Children's rights in relation to the digital environment* CRC/C/GC/25 (13 August 2020) at [12].

the business sector.[72] The collection and use of biometric data is considered a risk to children's right to privacy.[73]

2.6.4 International Human Rights Protections for Indigenous Peoples

Any discussion of human rights in the bi-cultural constitutional context of New Zealand must consider the rights of indigenous peoples.[74] While indigenous peoples, like all individual, are protected by the general human rights framework, there are also specific rights for indigenous people.[75]

The United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP)[76] was adopted by the United Nations General Assembly, September 2007. Settler states such as New Zealand, Australia, the United States and Canada initially voted against, but have now reversed that position.[77] UNDRIP is a non-binding declaration of the General Assembly. It provides a framework that individual states can adopt in their relationship with indigenous peoples and can guide them in the development of domestic law and policy.[78] Some of its content gathers together binding international legal principles set out in other instruments (such as freedom from discrimination[79]), others demonstrate evolving consensus of international norms.

UNDRIP's emphasis on self-determination in articles 3–4 provides international support for the recognition of indigenous peoples' control over their own data. In addition, s 31 of UNDRIP imposes a duty on States to assist in the protection of indigenous resources including their "cultural heritage", "traditional knowledge" and "human and genetic resources". Indigenous data sovereignty is the idea that indigenous peoples have sovereignty over their own data[80] – which would include databases of facial images. Te Mana Raraunga (the Māori data sovereignty network) have recently cautioned about the particular implications of the new all-of-government biometrics contract: "the proposed processing of large-scale biometric data by an overseas agency (DXC Technology via its subsidiary) represents clear and significant risks to Māori Data Sovereignty and the wider community in Aotearoa".[81]

2.7 APPLICATION OF HUMAN RIGHTS STANDARDS TO THE PRIVATE SECTOR

Much of the literature on human rights considers how the framework applies to state actions. Increasingly, there is recognition of the importance of human rights to the corporate sector.[82] This has relevance to FRT as many of the systems involve partnerships or transmission of information between the state and the private sector.

The United Nations has established a set of guidelines for the application of human rights standards to businesses:[83]

72 UN Committee on the Rights of the Child *Draft General Comment No. 25 (202x): Children's rights in relation to the digital environment* CRC/C/GC/25 (13 August 2020) at [39].

73 UN Committee on the Rights of the Child *Draft General Comment No. 25 (202x): Children's rights in relation to the digital environment* CRC/C/GC/25 (13 August 2020) at [70].

74 Māmari Stephens "Fires Still Burning? Māori Jurisprudence and Human Rights Protection in Aotearoa New Zealand" in Kris Gledhill, Margaret Bedggood and Ian McIntosh (eds) International Human Rights Law in Aotearoa New Zealand (Thomson Reuters, Wellington, 2017), 99

75 James S Anaya *International Human Rights and Indigenous Peoples* (Aspen Publishers, New York, 2009).

76 *United Nations Declaration on the Rights of Indigenous Peoples* GA Res 61/295 (2007).

77 United Nations "United Nations Declaration on the Rights of Indigenous Peoples" www.un.org.

78 Felipe Gómez Isa "The UNDRIP: an increasingly robust legal parameter" (2019) 23 Int J Hum Right 7.

79 *United Nations Declaration on the Rights of Indigenous Peoples* GA Res 61/295 (2007), art 2.

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

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

82 Claire Methven O'Brien and Jolyon Ford "Business and Human Rights: From Domestic Institutionalisation to Transnational Governance and Back Again" (2019) 37 Nord J Hum rights 216; and Sally Wheeler "Committing to human rights in Australia's corporate sector" [2019] Griffith LR 1.

83 UN Committee on Economic, Social and Cultural Rights *General Comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities* E/C.12/GC/24 (10 August 2017).

> "States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication."[84]
>
> "States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations."

The United Nations Committee on Economic, Social and Cultural Rights has emphasised that corporates must guard against discrimination: "States parties must therefore adopt measures, which should include legislation, to ensure that individuals and entities in the private sphere do not discriminate on prohibited grounds."[85]

2.8 CONCLUDING REMARKS

The human rights framework is the primary lens through which we will examine FRT. FRT may pose risks to a range of human rights, particularly freedom of expression, right to be free from discrimination, right of peaceful protest, and the minimum standards of criminal procedure.

The human rights framework protects general human rights and protects the rights of specific groups such as children and indigenous peoples.

People in Aotearoa New Zealand have more limited options to pursue human rights complaints against the state. In other jurisdictions, e.g. England and Wales, people have taken actions for breach of rights – e.g. in the case of *Bridges*.

This will have relevance in shaping our discussion around recommendations.

84 United Nations *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (United Nations Human Rights Office of the High Commissioner, New York and Geneva, 2011).

85 UN Committee on Economic, Social and Cultural Rights *General Comment No. 20: Non-discrimination in economic, social and cultural rights (art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights)* E/C.12/GC/20 (2 July 2009) at [11].

SECTION 3

VALUES, ATTITUDES, ETHICS AND SOCIAL LICENCE

3.1 INTRODUCTION

The overarching goal of this report is to establish a legal and ethical framework for the use of FRT in New Zealand.

The previous section considered the human rights and legislative frameworks which are relevant to FRT. The human rights framework constrains state power and to a certain extent constrains the actions of private individuals and businesses. But there are a range of other standards, guidelines and constraints on the use of emerging technologies and algorithms such as FRT. This can range from government standards on the ethical use of algorithms to more nebulous constraints such as the acceptance of use-cases of technology by members of the public.

This section reviews the literature on ethical standards, public attitudes and social licence in relation to FRT and related technology.

3.2 ETHICAL STANDARDS AND GUIDELINES

The previous section set out the human rights framework in Aotearoa. What are the attributes of ethics as opposed to human rights? Human rights are derived from law. As Carillo notes law is mandatory and enforceable.[1] Legal norms are common and uniform – arising from agreements between states or by enactment through the domestic legal process. In contrast, ethics is generally voluntary. The human rights framework provides "a ready-made, internationally tested and legitimate framework of civil, political, economic, cultural and social values, addressing both individual and collective concerns."[2]

Here, we discuss the different types of ethical standards that are in place in Aotearoa and comparable jurisdictions. Some apply to algorithms and data use generally, others are more specific to biometrics.

3.2.1 New Zealand Ethical Standards

This section reviews the existing ethical standards relating to use of FRT and similar technologies. This discussion frames recommendations made in the final section.

3.2.1.1 The Algorithm Charter

A review of the New Zealand government's use of algorithms in 2018 identified a range of uses for algorithms.[3] Amongst the risks identified were privacy, bias and data quality.[4] As a result of this, work was undertaken on an algorithm charter. New Zealand claims to be the first jurisdiction in the world to have a government commitment to a set of standards for the use of algorithms by the public service.[5] This Charter now sets principles for public sector agencies using algorithms for the basis of, or to guide, decision-making. Government agencies who sign up agree to several

1 Margarita Robles Carrillo "Artificial intelligence: from ethics to law" (2020) 44 Telecomm Policy.

2 AI Forum New Zealand *Trustworthy AI in Aotearoa: AI Principles* (March 2020) at 2.

3 Stats NZ *Algorithm Assessment Report* (October 2018).

4 Joy Liddicoat, Colin Gavaghan, Alistair Knott, James Maclaurin and John Zerilli "The use of algorithms in the New Zealand public sector" [2019] NZLJ 26.

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

principles to guide use of algorithms.[6] The term algorithm is not specifically defined in the Charter, noting that it is the effect of the particular algorithm rather than the complexity, that must be considered. The key principles of the Charter are:[7]

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

Not all agencies have signed up to the charter. This is a voluntary set of guidelines, and how an individual can query improper use and seek redress is unclear. It may also be noted that the Government Chief Data Steward has convened an independent group that is available to assist public sector agencies with data ethics issues, particularly relating to algorithms.[8]

3.2.1.2 Principles for the Safe and Effective Use of Data and Analytics

The Government Chief Data Steward and the Privacy Commissioner have developed a set of principles to guide safe and effective use of data and analytics:[9]

- Deliver clear public benefit – it is essential government agencies consider, and can demonstrate, positive public benefits from collecting and using public data.
- Maintain transparency – transparency is essential for accountability. It supports collaboration, partnership, and shared responsibility.
- Understand the limitations – while data is a powerful tool, all analytical processes have inherent limitations in their ability to predict and describe outcomes.
- Retain human oversight – analytical processes are a tool to inform human decision-making and should never entirely replace human oversight.

---

6 As of October 2020, the following agencies had signed up:
Te Ara Poutama Aotearoa — The Department of Corrections
Te Tāhuhu o Te Mātauranga — The Ministry of Education
Te Manatū Mō Te Taiao — The Ministry for the Environment
The Ministry of Housing and Urban Development
Te Tari Taake — Inland Revenue Department
Te Tāhū o te Ture — The Ministry of Justice
Toitū Te Whenua — Land Information New Zealand
Te Puni Kōkiri — The Ministry of Māori Development
Oranga Tamariki - The Ministry for Children
The Ministry for Pacific Peoples
Te Manatū Whakahiato Ora — The Ministry of Social Development
Te Tatauranga Aotearoa — Statistics New Zealand
Te Manatū Waka — The Ministry of Transport
Te Kāhui Whakamana Rua Tekau mā Iwa—Pike River Recovery Agency
Te Minitatanga mō ngā Wāhine — The Ministry for Women
Te Hau Tāngata — Social Wellbeing Agency
Te Ope Kātua o Aotearoa — New Zealand Defence Force
Te Kaporeihana Āwhina Hunga Whara — Accident Compensation Corporation
Te Tari Taiwhenua — Department of Internal Affairs
Te Arawhiti — The Office for Māori Crown Relations
Waka Kotahi — The New Zealand Transport Agency
Te Tari Arotake Matauranga — The Education Review Office
Hīkina Whakatutuki — The Ministry of Business, Innovation, and Employment
Manatū Aorere — The Ministry of Foreign Affairs and Trade
Manatū Hauora — The Ministry of Health
Nga Pirihimana O Aotearoa — New Zealand Police

7 Stats NZ *Algorithm Charter for Aotearoa New Zealand* (July 2020).

8 More information including membership and terms of reference may be found here: Data.govt.nz "Data Ethics Advisory Group" www.data.govt.nz. One of the authors of this report (Lynch) is a member of this Group. Any views expressed here are her own.

9 Privacy Commissioner and Stats NZ *Principles for the safe and effective use of data and analytics* (May 2018).

- Ensure data is fit for purpose – using the right data in the right context can substantially improve decision-making and analytical models, and will avoid generating potentially harmful outcomes.
- Focus on people – keep in mind the people behind the data and how to protect them against misuse of information.

3.2.1.3 Guiding Principles for the Use of Biometric Technologies for Government Agencies

In 2009, the government had a set of guiding principles for biometric technologies,[10] which emphasised a set of principles including justified use, lawful and authorised use, collaboration, consultation, fit for purpose and meeting domestic and international obligations. These guidelines and an accompanying Group appear to have been overtaken by other sets of standards. An Official Information request to DIA confirms this:[11]

> The Cross Government Biometrics Group was last operational in 2010.The group has been superseded by other forums including the Biometrics Sector Governance Group. The Department also participates in several international forums, including the Biometrics Institute and the National Institute of Standards.

3.2.1.4 Trustworthy AI in Aotearoa – AI Principles

These standards have been developed by the non-governmental organisation, the Artificial Intelligence (AI) Forum.[12] The Principles recommend that Designers, developers and users of AI systems (AI stakeholders) must respect:

- Applicable laws in New Zealand and other relevant jurisdictions,
- Human rights recognised under domestic and international law,
- Rights of Māori articulated in Te Tiriti o Waitangi,
- Democratic values including the electoral process and informed public debate,
- Principles of equality and fairness so that AI systems do not unjustly harm, exclude, disempower or discriminate against individuals or particular groups.

Other important standards are:

- Reliability, security and privacy,
- Transparency,
- Human rights and accountability,
- Well-being.

3.2.1.5 Principles of Māori Data Sovereignty

Te Mana Raraunga (The Māori Data Sovereignty Network) has developed a document which sets out an overview of key concepts in Māori Data Sovereignty:[13]

- **Rangatiratanga | Authority –** the inherent right to control and make decisions about data,
- **Whakapapa | Relationships** – data has a whakapapa (genealogy); data should be collected and coded using categories that prioritize Māori needs and aspirations; any use must protect against future harm,
- **Kotahitanga | Collective benefit** – individual and collective rights must be balanced; there must be accountability to those from which the data is derived; data systems must be designed to benefit Māori; build capacity and connect in support of common goals,
- **Manaakitanga | Reciprocity** – collection, use and interpretation will uphold dignity and avoid stigmatisation and blame; free, prior and informed consent shall underpin the collection and use of data,
- **Kaitiakitanga | Guardianship –** Māori data shall be stored and transferred so that Māori can exercise kaitiakitanga over their data; tikanga, kawa and mātauranga will underpin governance, and Māori will decide whether access is controlled or open.

10 Cross Government Biometrics Group *Guiding Principles for the Use of Biometric Technologies for Government Agencies* (Department of Internal Affairs, April 2009).

11 Official Information Request to Department of Internal Affairs (17 November 2020).

12 AI Forum New Zealand *Trustworthy AI in Aotearoa: AI Principles* (March 2020).

13 Te Mana Raraunga, Principles of Māori Data Sovereignty (Brief #1, October 2018) available at www.temanararaunga.maori.nz/nga-rauemi.

3.2.2 International Ethics Standards

Recent years have seen the proliferation of ethical standards for algorithm and data use.[14] Most of these are centred around similar concepts; privacy, transparency, accountability, bias and discrimination and equality:

- United Kingdom Government's seven principles for ethical data use,[15]
- Canadian Government's 'guiding principles' for AI,[16]
- Australian Government's AI ethics principles,[17]
- European Commission's ethics guidelines for Trustworthy AI,[18]
- The Toronto Declaration.[19]

Some of these are discussed in more detail in the sections on existing regulation, comparative models of regulation and in our recommendations sections.

3.3 PUBLIC COMFORT WITH FRT

A potential constraint on expansion of surveillance through FRT is the views of the public.[20] In New Zealand, the Police Commissioner has spoken of the importance of policing by consent.[21]

No specific research has been done in New Zealand, though the Digital Council are currently engaged in some work around citizens' trust in automated decision-making.[22]

Research studies in comparable jurisdictions give insight into people's level of comfort with the use of FRT. Most people surveyed in studies in the US, UK and Australia[23] were comfortable with the police or government using FRT for law enforcement purposes. However, the surveys indicated that most people would want regulations in place to control this power. Further, in the UK study, most people believed that there should be the option to opt out of FRT (46% thought this option should be available, 28% did not and the rest were unsure).

Moving to the private sector usage, most people in the US and UK studies felt uncomfortable with advertisers, retailers, stadiums, employers, apartment building landlords and other private parties using FRT. Only 15-36% of people in the US study and 4-7% of people in the UK were comfortable with it. The UK survey indicated that this comes from lack of trust in private parties to use the technology responsibly.

Levels of trust in the use of FRT also varied between different demographics in both the US and UK

14 Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Christopher Nagy and Madhulika Srikumar *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* (Berkman Klein Center for Internet & Society, January 2020).

15 Government Digital Service *Data Ethics Framework* (2020).

16 Government of Canada "Responsible use of artificial intelligence (AI)" www.canada.ca.

17 Australian Government: Department of Industry, Science, Energy and Resources "AI Ethics Principles" www.industry.gov.au.

18 Independent High-Level Expert Group on Artificial Intelligence *Ethics Guidelines for Trustworthy AI* (European Commission, April 2019) at 33-34.

19 Amnesty International and Access Now *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems* (May 2018).

20 Ben Bradford, Julia A Yesberg, Jonathan Jackson and Paul Dawson "Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology" (2020) 60 Br J Criminol 1502; and Anna Gurinskaya "Predicting citizen's support for surveillance cameras. Does police legitimacy matter?" (2020) 44 IJCACJ 63.

21 Jonathan Jackson, Ben Bradford, Mike Hough and Katherine Murray "Compliance with the law and policing by consent: notes on police and legal legitimacy" in Adam Crawford and Andrea Huckles (eds) *Legitimacy and Compliance in Criminal Justice* (Routledge, Abingdon, 2013) 29; and Sam Sherwood and Collette Devlin "Police Commissioner rules out bringing back Armed Response Teams" *Stuff* (online ed, New Zealand, 9 June 2020).

22 Digital Council *Trust and Automated Decision-Making: an interim report on the Digital Council's 2020 Research* (2020).

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

studies. Young people and ethnic minorities were less comfortable with police use of FRT.[24] However, this may be more of a reflection of levels of trust in law enforcement in general.

Both the UK and Australian data showed a general public concern over the normalisation of surveillance. However, both studies also showed recognition of the trade-off for public benefit such as security.

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

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

A report from the European Union relating to the use of FRT at the border notes that:[25]

> In a survey conducted by FRA in 2015 – involving 1,227 third-country nationals at seven border crossing points – 12 % of all respondents indicated feeling very uncomfortable when their facial image was used for crossing the border (see Figure 1); 18 % considered providing a facial image at a border very intrusive to their privacy; and 26 % said that doing so was humiliating. There are differences across nationalities, with Russians and citizens of the United States being less concerned, and Chinese citizens and people from other areas in the world being more concerned. No clear differences with respect to the level of feeling humiliated based on age and gender emerged from the survey. Results from such a survey might change rapidly over time given the fast development of the technology and that people are more often being exposed to such technology

A survey of people in China recently reported in Nature:[26]

> An online survey of more than 6,000 people in December 2019 by the Nandu Personal Information Protection Research Centre, a think tank affiliated with the *Southern Metropolis Daily* newspaper in Guangzhou, found that 80% of people worried about lax security in facial-recognition systems and 83% wanted more control over their face data, including the option to delete it.

3.4 SOCIAL LICENCE FOR TECHNOLOGY/STATE SURVEILLANCE IN NEW ZEALAND

The concept of 'social licence' was reportedly first used in the context of the mining industry.[27] Gulliver et al have defined social licence in the New Zealand data context as being: [28]

> …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.

It is our view that social licence can never override consent, human rights or privacy protections. Social licence may be relevant in considering the shape of legislative and policy reform. A salient question is also whether social licence for privacy and liberty restrictions in pursuit of collective safety/welfare has changed in the context of the 2020 global pandemic. Social licence can change rapidly – we have seen that before of course

24 Aaron Smith "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly" (5 September 2019) Pew Research Center www.pewresearch.org; and Information Commissioner's Office *ICO investigation into how the police use facial recognition technology in public places* (October 2019).

25 European Union Agency for Fundamental Rights *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Publications Office of the European Union, 21 November 2019) at 18.

26 Antoaneta Roussi "Resisting the Rise of Facial Recognition" (2020) 587 Nature 350.

27 Richard Parsons and Kieren Moffat "Constructing the meaning of social licence" (2014) 28 Soc Epistemol 340; and Gary Lynch-Wood and David Williamson "The social licence as a form of regulation for small and medium enterprise" (2007) 34 J Law Soc 321.

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

in relation to reactions to terrorist attacks such as the Christchurch mosque shooting,[29] but perhaps not as quickly.[30]

In section 1, we traced the increasing use of technologies including FRT in the response to Covid-19.[31] As one news report puts it: [32]

> [F]rom South Korea to Western Europe, democratically-elected governments are using digital tools to track the whereabouts of patients with coronavirus and monitor how effectively citizens are obeying social distancing measures. While such moves naturally spark immediate fears of political overreach from leaders, they also raise questions around what happens when this pandemic is over. The concern is that as the world comes to terms with its way of life, citizens become numb to what were initially extreme and extraordinary measures.

In a New Zealand context:[33]

> The Covid-19 pandemic has come at a time when we have unprecedented access to technology capable of collecting an unlimited amount of personal data. While this has been of huge benefit, it also poses serious threats to an individual's privacy and cybersecurity of the data that could enable mass surveillance and data breaches due to insufficient protection.

It is perhaps too early to assess whether the events of 2020 have altered individual and societal views on the acceptability of surveillance and tracking technology. It may also be that individuals are more aware of the importance of privacy and human rights, given the unprecedented restrictions on freedom of movement etc during the pandemic response. Key government initiatives such the Covid-19 app have probably raised awareness of consent in relation to location-based apps and similar technologies.

Research is needed on this specific question in New Zealand, and particularly there needs to be consultation with groups who are disproportionately affected by state surveillance.

3.5 CONCLUDING REMARKS

This section reviewed the various ethical standards in place in New Zealand and comparable jurisdictions. It may be seen that there has been a proliferation of ethical standards and guidelines amongst government in Aotearoa and in comparable jurisdictions. Public trust and social licence were also reviewed. There has been little specific research or consultation on state surveillance and tracking technology in a New Zealand context.

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

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

31 See also Jack Shenker "Cities after coronavirus: how Covid-19 could radically alter urban life" *The Guardian* (online ed, United Kingdom, 26 March 2020).

32 Luke McGee "Power-hungry leaders are itching to exploit the coronavirus" *CNN* (online ed, United States, 1 Apri 2020).

33 Rizwan Asghar "Covid-19 and the privacy trade-off" *Newsroom* (online ed, New Zealand, 22 May 2020).

SECTION 4

HUMAN RIGHTS IMPLICATIONS OF USING FRT

4.1 INTRODUCTION

This section maps some of the threats that FRT might pose to societal interests and the rights of individuals. It considers issues in the development and deployment of the technology, from a fundamental human rights perspective. As has been discussed, the technology is on the rise, and new uses continue to be found for FRT. These developments raise pressing questions concerning the accuracy of the technology, the level of public support it enjoys, and the impact the technology has on individual rights, and society more broadly. This section provides an overview of these issues, which forms the basis of discussion for how this technology can, and indeed *should*, be regulated.

4.2 THE ACCURACY AND EFFICACY OF FRT

The National Institute of Standards and Technology (NIST), a subgroup of the US Federal Department of Commerce, has provided technical evaluation of over 100 commercially available facial recognition algorithms as part of its 'Facial Recognition Vendor Tests' (FRVT). They measure the accuracy of facial recognition software algorithms in 'one-to one' (image verification) and 'one-to-many' (database search) contexts. Its FRVTs have shown that the technology is far more accurate than it was a decade ago, and these gains have been attributed to the confluence of growing computational power, increases in image data volume, and improvements in machine learning algorithms.[1] FRT is only likely to improve in future. However, recognition error rates remain significantly above zero, particularly where photography of faces is difficult or when stringent confidence thresholds are applied to reduce false positives.[2] The performance of FRT systems and algorithms vary depending on the task they are performing, and how 'success' is defined.[3] An FRT system may be set at a particularly high sensitivity level to maximise the number of identifications (with full awareness that this will also increase the number of false positive matches). Conversely, a low sensitivity level might be used, so that matches are only returned by the system where there is a particularly strong match between the scanned image and a watchlist image.

The performance of FRT systems can vary relative to the gender, ethnicity and age of the individuals targeted.[4] NIST's FRVT Part 3 focused specifically on demographic effects on the performance of most 189 commercially available facial recognition algorithms. It found that many of the algorithms varied in performance across different demographic groups, and that the part of the world in which the algorithm was developed could have a significant impact on its performance.[5] For example, algorithms developed in the United States tend to have the high false positive rates for West and East African and East Asian people in one-to-one matching, whereas for a number of algorithms developed in China this effect is reversed, with low false positive rates on East Asian faces.[6]

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

In the specific context of Aotearoa/New Zealand, the implementation of algorithms trained on overseas data sets of faces raises concern about lack of accuracy for

1 Patrick Grother, Mei Ngan and Kayee Hanaoka *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* (NISTIR 8238, November 2018).

2 "FRVT Quality Assessment" NIST www.pages.nist.gov/frvt/html/frvt-quality.html.

3 Patrick Grother, Mei Ngan and Kayee Hanaoka *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* (NISTIR 8238, November 2018).

4 See Joy Buolamwini and Timnit Gebru *Gender Shades: Intersectional Accuracy Disparities in Commerical Gender Classification* (Conference on Fairness, Accountability, and Transparency, 2018) 2; and Joy Buolamwini "Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces" (25 January 2019) Medium www.medium.com.

5 Patrick Grother, Mei Ngan and Kayee Hanaoka *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280, December 2019).

6 Patrick Grother, Mei Ngan and Kayee Hanaoka *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280, December 2019) at 2.

people in New Zealand, particularly those of Māori descent. For example, a study has found that facial tattoos may disrupt face recognition.[7] One commentator cautions that "my concern is we're going to see an increase in false arrests with Māori ... I'm also concerned the system wouldn't have been trained on tā moko, moko kauae so we have no idea how the system will react to that."[8]

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

Even where concerns about the accuracy of a system can be sufficiently mitigated, a broader assessment of its efficacy in a particular context may be needed. For example, when assessing the utility of FRT, consideration of the risk that a FRT system can be 'spoofed'[9] or avoided through the use of masks, baseball caps or other face coverings may be needed.[10]

FRT might also have a detrimental impact on fundamental human rights. When FRT is deployed, several human rights might be impacted. Again, the particular constellation of human rights impacts will vary depending on the features of the particular FRT system that is used, the context in which it is used, the manner of this use, the safeguards that are in place to regulate a particular deployment, and other factors. What follows is a discussion of human rights that have potentially been impacted and why FRT surveillance may threaten the enjoyment of these particular human rights.[11]

4.3 PROCEDURAL FAIRNESS IN THE CRIMINAL JUSTICE SYSTEM

The use of facial images as identification evidence has been used by police and at trial for many years. This is a spectrum from longstanding investigative and evidential techniques such as showing witnesses 'mugshots' of suspects or defendants, technological advances such as expert opinion based on image comparison techniques, to 'facial mapping' and now automated FRT.[12] Crawford notes that "no peer-reviewed studies have shown convincing data that the technology has sufficient accuracy to meet the United States constitutional standards of due process, probable cause and equal protection that are required for searches and arrests."[13]

Inaccurate FRT matching could have particularly serious repercussions in the context of criminal proceedings. In the course of a criminal investigation, the police may seek to identify individuals in a 'probe image'.

Example 1: Using FRT to verify the identity of an arrestee. A suspect is arrested, but refuses to provide his name to police. Police could take a 'probe image' of the individual's face. Facial recognition software could then be used to verify the individual's identity by comparing the probe image against a database of images that the police control, or to which the police have access.

Example 2: Using FRT to identify a suspect etc. CCTV footage shows a suspected burglar leaving a property. A still of the suspect's face is used as a probe image and compared with a database of custody images (commonly

7 Heather Buttle and Julie East "Traditional facial tattoos disrupt face recognition processes" (2010) 39 Perception 1672.

8 Karaitiana Taiuru quoted in Meriana Johnsen "Police facial recognition discrimination against Māori a matter of time – expert" *RNZ* (online ed, New Zealand, 2 September 2020).

9 This is where an FRT system is tricked by the use of an image of a face. For eg, an individual could use the image of the face of a smartphone owner to trick the FRT software on the phone into unlocking the device. See Aleksandr Parkin and Oleg Grinchuk *Recognizing Multi-Modal Face Spoofing with Face Recognition Networks* (CVPR Workshop Paper, 2019).

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

11 This section draws from, and expands upon, a context-specific discussion in Joe Purshouse and Liz Campbell "Privacy, Crime Control and Police Use of Automated Facial Recognition Technology" (2019) 3 Crim Law Rev 188.

12 Ioana Macoveciuc, Carolyn J Rando and Hervé Borrion "Forensic Gait Analysis and Recognition: Standards of Evidence Admissibility"(2019) 64 J Forensic Sci 1294.

13 Kate Crawford "Regulate facial-recognition technology" (2019) 572 Nature 565.

known as 'mugshots'). The facial recognition software generates a shortlist list of possible matches, and police arrest a suspect based on his place of residence being close to the crime scene and the strength of the FRT 'match'.

Example 3: Using FRT as evidence of identity. Following on from example 2, the suspect is charged but contests that he is not the person in the probe image. The prosecution present evidence that the suspect was identified through the use of facial recognition software at trial, which suggested that his stored custody image was a 'likely match' to the probe image taken from a CCTV feed.

As discussed in detail in Section 1, New Zealand Police now reportedly have an image management system which has the capability of verifying identity (as in example 1) and matching a probe image to an existing identity (as in example 2). There are considerable risks to using FRT to assist with identification in this way, and some of these have been discussed above. The accuracy of the FRT system in place is one consideration, but even if a system is very accurate, risks of misidentification may still arise owing to the ways in which probe images are obtained and processed by the authorities. In a detailed study of the New York Police Department's use of facial recognition to generate investigative leads (as in example 2), Garvie noted numerous problematic practices from officers submitting probe photos for facial recognition analysis, including the submission of: (i) images of celebrities that were said to resemble a suspect; (ii) composite sketches of suspects (iii) heavily doctored images, sometimes combining images of multiple faces to form a single probe image; and (iv) the use of poor quality or obscured facial images.[14]

Garvie summarised the inherent risks in these sorts of practices:

> During a face recognition search on an edited photo, the algorithm doesn't distinguish between the parts of the face that were in the original evidence—the probe photo—and the parts that were either computer generated or added in by a detective, often from photos of different people unrelated to the crime. This means that the original photo could represent 60 percent of a suspect's face, and yet the algorithm could return a possible match assigned a 95 percent confidence rating, suggesting a high probability of a match to the detective running the search.[15]

Garvie called for an end to these sorts of practices, and her study underlines the need for clear rules and guidance for law enforcement officers on appropriate and inappropriate uses of algorithmic technologies, such as FRT.

Such standards have been developed for the collection and use of CCTV images. In 2014, the Australia New Zealand Policing Advisory Agency (ANZPAA) published a document setting out recommendations for the use of CCTV systems for policing purposes,[16] This document provides guiding recommendations designed to ensure the reliability and efficiency of CCTV systems used for policing purposes. It emphasises that CCTV systems should be designed to achieve clear and particular goals, and be designed so they are fit for this purpose. It also makes technical recommendations on the operation, export functionality, software and resolution particulars. Any such guidance or regulations for FRT should also ensure that the use of such FRT is limited and transparent. This is particularly important for cases such as in example 3, where FRT is used as evidence of identity at trial. If an individual's fair trial rights are to be respected, then, at a minimum, the means by which a defendant has been identified should be disclosed to the defence. This includes, but is not limited to, the disclosure of the original probe image; any edits made to the probe image; information regarding disregarded 'matches', error rates and uncertainties of the system itself.[17]

One subsidiary issue here relates to the construction of police databases, and other databases of images to which the police can gain access for the purposes of running a facial recognition search. In the United States, police forces in numerous States can access not only custody images, but also driver's license and passport photos. In 2016, Garvie et al estimated that law enforcement agencies could potentially access over 116,000,000 American adults through cross searching a complex

14 Clare Garvie "Garbage In, Garbage Out: Face Recognition on Flawed Data" (16 May 2019) Flawed Face Data www.flawedfacedata.com.

15 Clare Garvie "Garbage In, Garbage Out: Face Recognition on Flawed Data" (16 May 2019) Flawed Face Data www.flawedfacedata.com.

16 PANZPAA *Australia New Zealand Police Recommendations for CCTV Systems* (2014).

17 Clare Garvie "Garbage In, Garbage Out: Face Recognition on Flawed Data" (16 May 2019) Flawed Face Data www.flawedfacedata.com; and Kyriakos N Kotsoglou and Marion Oswald "The Long Arm of the Algorithm? Automated Facial Recognition as Evidence and Trigger for Police Intervention" (2020) 2 FSI Synergy 86 at 88.

network of facial image databases.[18]

Recently released documents discussed in Section 1 demonstrate that "police already have 1.5 million images of 800,000 people, having first set up the existing image management system in 2009."[19] A request for proposals for a new database system released in mid-2018 shows that Police have an existing image management system called 'Photo Manager' with some FRT capability.[20] Further sources discussed in Section 1 reveal that the image management system has a single repository for all identification images including formal prisoner photographs, Firearms Licence holders images, suspect images and missing persons images.

As we discuss in the recommendations section, this large collection of images coupled with an ability to utilise live AFR or use FRT on already collected CCTV footage, represents a significant potential source of mass and/or targeted surveillance.

The potential that police forces could work with private companies to cross reference privately held images is also being realised. In January 2020, the New York Times reported that a small FRT start-up company, Clearview AI, had sold its FRT tool to over 600 law enforcement agencies around the world. The tool is described as follows, 'You take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared. The system — whose backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites — goes far beyond anything ever constructed by the United States government or Silicon Valley giants.'[21]

In February 2020, Buzzfeed reported that numerous police forces, public authorities and private organisations had run searches on Clearview AI's facial recognition app. Many of these clients had not previously disclosed their use of the app to the public, and had no internal guidance or policies regulating the circumstances in which they might use the app. As was discussed in detail in Section 1, in May 2020, it was revealed that the New Zealand Police had used the Clearview system without consulting the Police Commissioner or Privacy Commissioner.[22] Betkier, argues that the New Zealand Privacy Act 1993 does not adequately control or remediate privacy intrusions by developers such as Clearview AI, who give law enforcement agencies access to their databases before legislators are even aware that such surveillance is being used.[23]

4.4 SEARCH AND SURVEILLANCE – LAWFULNESS AND REASONABLENESS

The case of *Bridges* which will be discussed in more detail below involved a person in southern Wales who sought judicial review of a police trial of FRT surveillance in public spaces, on the grounds that this use breached human rights legislation and data protection legislation. As discussed in Section 2, in New Zealand, it would not be possible for a person to take a judicial review of this nature due to the constitutional structure of the jurisdiction. (It was noted that in the future, if FRT was empowered by an enactment and if the *Declaration of Inconsistency Bill* passes into law, a Court could make a declaration of inconsistency with the *New Zealand Bill of Rights Act*. This is not yet possible.)

The most likely contemporary scenario where the courts could consider the lawfulness and human rights impact of the use of FRT would be in the context of an admissibility of evidence case. This would occur if the police used FRT to obtain evidence against a defendant and the admissibility of the evidence was contended by the defence. Questions of lawfulness, human rights compliance and reasonableness might then arise.

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

19 Phil Pennington "Police setting up $9m facial recognition system which can identify people from CCTV feed" *RNZ* (online ed, New Zealand, 31 August 2020).

20 New Zealand Police *Request for Proposals ABIS 2 (Automated Biometric Identification Solution)* (TN 18/03, RFP released 15 January 2018) (copy on file with authors).

21 Kashmir Hill "The Secretive Company That Might End Privacy as We Know It" *The New York Times* (online ed, New York, 18 January 2020).

22 Mackenzie Smith "Police 'stocktake' surveillance tech after Clearview AI facial recognition trial" *RNZ* (online ed, New Zealand, 18 May 2020).

23 Marcin Betkier "Clearview AI exposes our regulatory shortcomings" (28 February 2020) Privacy Foundation www.privacyfoundation.nz.

4.4.1 Are the New Zealand Police permitted to use FRT in surveillance?

As noted, there is no specific legislative empowerment of the use of FRT, neither is there a prohibition (this mirrors the situation in the United Kingdom). There are no specific New Zealand cases on the lawfulness and/or admissibility of FR equipped surveillance, but analogies may be drawn with the law on admissibility of other forms of video surveillance.

Pre- *Hamed v R*[24] the law was understood as being that video surveillance by the Police was not unlawful because it was not forbidden by statutory or common law.[25] This position was confirmed in *Ngan*, *Fraser* and *Gardiner*.[26] Thus, police officers are entitled to do anything that can be lawfully done by a citizen unless there is a common law or statutory prohibition. This view was confirmed by the majority in *Hamed*. This is also the general position in the *Search and Surveillance Act 2012* – surveillance in a public place where no trespass has occurred is lawful and does not require a warrant.[27] The Court of Appeal in *Lorigan* found that covert surveillance with a night vision equipped camera was lawful as there was "no statutory or common-law prohibition and it would not have been unlawful for a citizen to do the same thing".[28]

Elias CJ in *Hamed* took the view that video surveillance in that case was unlawful, whether there was a trespass or not.[29] Elias CJ would have held that public officials are different to private citizens and cannot do something unless they have lawful authority (whereas private citizens have the freedom to do anything that they are not prohibited from doing). In our view, this is the preferred interpretation, but this was a minority view in this case.

4.4.2 Would use of a FR enabled camera be considered a 'search'?

Even if the legal framework was updated to prevent secret FRT identifications by law enforcement, under s.30 of the Evidence Act 2006, trial judges would not necessarily be required to exclude evidence of identity derived from a match obtained through, for example, the search of a probe image against Clearview AI's app. Instead, s. 30(2) requires exclusion only in circumstances where a judge finds: (a) on the balance of probabilities, that the evidence was improperly obtained; and, (b) determines that exclusion of the evidence is proportionate to the impropriety giving account of the need for an effective and credible justice system.[30] This means that the judge has a discretion to exclude evidence that is obtained in breach of the defendant's NZBORA rights, or otherwise unfairly, but that such evidence may still be admissible.

An important pre-cursor question in assessing admissibility is whether the use of a FR equipped camera by the police or other enforcement agency is a 'search' in terms of s. 21 of the NZBOR Act. The Court in *Bridges* did not engage with this point in the context of English law merely noting that a FR enabled camera was more intrusive than regular CCTV.[31]

Several New Zealand cases have discussed whether various forms of camera surveillance constitute a 'search'. In *Lorigan v R*,[32] the appellant argued that surveillance evidence gathered by the police in a drug offending case was inadmissible. The police had set up a video camera (with the permission of the landowner) and then subsequently a second camera with night-vision capabilities. The extent of the cameras' view was that

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

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

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

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

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

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

30 Evidence Act 2006, s 30.

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

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

which was in plain sight of any person who walked down the street.

As to the question of whether covert video surveillance was a search, counsel for the Crown accepted that covert video surveillance in this context was a 'search' for the purposes of s. 21 of the NZBOR Act.. This view was supported by two out of three Supreme Court Judges from the case of *Hamed*.[33] In *Hamed*, Blanchard J did not regard surveillance in a public place as being a search because there was no state intrusion into reasonable expectations of privacy. Nonetheless, he did mention that the situation may be different where the "surveillance of the public place involved the use of equipment that captured images that were not able to be seen by the naked eye, such as the use of infra-red imaging"[34] [This would be analogous to FR capability as well.] Tipping J in *Hamed* defined "search" as being able to include watching people by technical means. This is highly relevant to the use of live FRT as the system is processing biometric data.

The Court in *Lorigan* considered that the test was "whether the surveillance by the police involves state intrusion into reasonable expectations of privacy" relying on *Ngan*[35] and *Hamed*.[36] However, the Court in *Lorigan* did not consider the "regular" video surveillance to be a search because it did not involve trespass and there was no or minimal intrusion into the privacy rights of those in the area under surveillance.[37] But, in relation to the camera with the night-vision capability – the Court found it was a search as "the images it could capture were such that they could not be seen by the naked eye".[38]

The use of the covert video surveillance was found to be reasonable, because there was "no statutory or common-law prohibition and it would not have been unlawful for a citizen to do the same thing".[39] It was also relevant that it was a public road – so that there no reasonable expectation of privacy.

4.4.3 Implications

New Zealand case-law indicates that the Police do not need specific legislative authorisation to use a FR- equipped camera in a public place. It is likely that it would be considered a 'search' in terms of s. 21 of the NZBOR Act as it would involve a process not possible by means of simple human observation – following from the Court's comments in *Lorigan* in relation to the use of 'night-vision' equipped camera surveillance.

It is difficult to make substantive conclusions regarding reasonableness or the operation of s. 30 in individual circumstances of individual cases. However, the fact that FRT matches could be admissible at trial underlines the need for robust regulation and transparent usage by law enforcement. Such guidance will aid the trial judge's assessment of whether such evidence has been improperly obtained.

4.5 PRIVACY AND INFORMATION RIGHTS

Like fingerprint scanning and DNA profiling, FRT involves the processing of biometric information about the individual. The technology allows the police to go further in monitoring and tracing individuals than ordinary observation or CCTV monitoring would. The FRT process 'involves the creation of informational equivalents of body parts that exist outside their owner and are used and controlled by others.'[40] For Brey, through this process the individual loses full ownership of the geometric features of his or her face as these features acquire new meanings that the individual does not understand, and new uses realised outside of his or her own body.[41]

33 *Lorigan v R* [2012] NZCA 264 at [15]-[16].

34 *Lorigan v R* [2012] NZCA 264 at [17]; and *Hamed v R* [2011] NZSC 101, [2012] NZLR 305 at [167].

35 *R v Ngan* [2007] NZSC 105, [2008] 2 NZLR 48.

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

37 *Lorigan v R* [2012] NZCA 264 at [23].

38 *Lorigan v R* [2012] NZCA 264 at [25].

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

40 Philip Brey "Ethical Aspects of Facial Recognition Systems in Public Places" (2004) 2 JICES 97 at 107.

41 Philip Brey "Ethical Aspects of Facial Recognition Systems in Public Places" (2004) 2 JICES 97 at 107.

Conceptions of privacy depend on culture, age, history and personal experience.[42] Community perception will influence privacy expectations. Considering this, any regulation of FRT in New Zealand will have to account for the different understandings of privacy as recognised by Māori and Pākehā. Any benefits accruing from FRT may come at the cost of individual privacy, which is experienced differently depending on the person's context and heritage.[43]

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

- Informational privacy – the right to control over collection and use of personal information or data;[44] and
- Spatial privacy – the right to physical inaccessibility to the person or other designated private spaces.

Informational privacy has the potential to be impacted by FRT. Faces are inherently unique to a person and so the information relating to their structural geometry is clearly personal information. The New Zealand Supreme Court has recognised that a person should be protected from intrusion by the state into personal space that is recognised as private in accordance with human dignity.[45] 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.

The collection of DNA or even fingerprint data often requires physical contact, whereas FRT scans typically do not. Blanchard J stated in *Hamed* that a DNA test (buccal swab) is a manifest physical intrusion.[46] In *R. (Bridges) v Chief Constable of South Wales Police*[47] – where a campaigner from Cardiff failed to convince the High Court of Justice for England and Wales that his human rights had been violated after his face was scanned on two occasions by the South Wales Police - the Court viewed this distinction as significant. Haddon-Cave LJ and Swift J observed that there is an important distinction between 'intrusive' and 'non-intrusive' methods of gathering personal information. Live FRT was the latter and only the former fell outside the general common law powers of the police. The High Court ruled that the distinction turned on whether there was a physical intrusion with a person's rights vis-à-vis his or her home or interference with his or her bodily integrity.[48] It held that only these forms of 'physical' intrusion require a statutory legal basis. Whilst there are significant differences between different forms of biometric data processing technology, we submit that the physical/informational intrusion distinction drawn by the Court is too blunt to serve as a useful gauge for the extent to which a particular technology such as FRT should be regulated.

Whilst the deployment of FRT may not require an operator to come into physical contact with those scanned, this does not necessarily make FRT a less serious privacy intrusion. Indeed, in some ways, owing to the secrecy with which this surveillance can be undertaken, the use of FRT may be more intrusive than the collection of a fingerprint. Live FRT enmeshes physical and informational forms of surveillance by collecting information from the physical body of the person and breaking this down into an information structure, which can then be processed. The High Court's distinction for fleshing out the scope of the common law powers of the police, between physical and informational intrusions, seems unfit to capture the nuances of how FRT can intrude into the privacy of the individual from a distance.[49] In August 2020, the Court of Appeal allowed the claimant's appeal on the grounds that the South Wales Police's use of AFR was unlawful as it was not "in accordance with law" for the purposes of Article 8(2) ECHR, and the SWP had failed to carry out a proper Data Protection Impact Assessment ("DPIA"). The SWP also failed to comply with the public sector equality duty (PSED).

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

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

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

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

46 *Hamed v R* [2011] NZSC 101 at [165].

47 [2019] EWHC 2341 (Admin).

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

49 For an expanded discussion of this decision see J Purshouse "Facial Recognition Technology, the Metropolitan Police and the Law" (19 January 2020) Policing Law Blog www.policing.law.blog.

Despite its absence from NZBORA, privacy is a broad concept that is recognised in New Zealand both judicially and under the Privacy Act 1993. Privacy is inherently linked to freedom from search and seizure.[50] The courts have accepted that a search involves an intrusion into a reasonable expectation of privacy. A scan using FRT is not an intrusion in the physical sense. However, as discussed in the previous section, the fundamental considerations regarding expectations of privacy are likely still the same when determining whether use of FRT amounts to a 'search' and whether that search was unreasonable. The Supreme Court has asserted that the protections under s. 21 apply 'not only to acts of physical trespass' and extends to covert surveillance.[51] The courts have yet to determine whether s. 21 applies to FRT. This will turn on whether the use of FRT in a public space breaches the expectation of privacy. The question of whether the unreasonableness requirement extends to a particular deployment would then be a question of fact depending on the circumstances of the deployment.

A further issue pertains to the convergence of privately owned, yet publicly accessible spaces.[52] The deployment of FRT by private companies in publicly accessible spaces raises unique problems for regulators as private entities are generally not subject to the same safeguards or transparency requirements as state agencies. There are also risks here that police departments may develop working relationships with private organisations or individuals who are not subject to public oversight or - through the exercise of the vast discretion and power that FRT may provide - private organisations can subvert the criminal justice system altogether. For example, in the United Kingdom, Facewatch - a provider of FRT systems to retail companies - has, through the work of its retailer clients uploading images of suspected shoplifters to its central database, developed a watchlist of images of 'subjects of interest'. Each retailer with a Facewatch FRT system can scan customers' faces as they enter the premises and cross check the image collected against the Facewatch's watchlist. If there is a match, then Facewatch sends an alert to the store manager, who can ask the individual to leave the store.[53] This system has the potential to produce discriminatory or disproportionate outcomes as retailers have vast discretion over the images they upload to the Facewatch database. Individuals could potentially be denied from entry to large swathes of publicly accessibly space, particularly in shopping centres that can form the hub of a local community, despite never being convicted for any acquisitive crime.[54] Despite doubts over its compliance with GDPR, Facewatch has successfully developed working relationships with police forces in the United Kingdom whereby Facewatch and state law enforcement can share access to images of 'subjects of interest' and retailers can upload images of such persons for further investigation by the authorities.[55]

4.6 FREE EXPRESSION AND ASSEMBLY

The use of overt surveillance raises broader principled concerns, other than the impact that it will have on an individual's privacy. Overt surveillance can have a 'chilling effect' on public assemblies, freedom of expression, and the general use of public space by certain communities and demographics.

Where FRT is used technology to transcend social norms of acceptable observation and scrutiny in public it is not difficult to see how this might have a moderating effect on behaviour. As Benn puts it, sustained observation of an individual can be objectifying: "Finding oneself an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes."[56] The use of FRT surveillance to monitor public spaces can be distinguished not only from being subject to the fleeting observations one might be subject to by a stranger in public space, but also from prolonged surveillance by police personnel, and the use of CCTV surveillance, which cannot limit the personal autonomy of the individual to the same extent.

50 Law Commission *Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012* (NZLC R141, 2017) at [2.17].

51 *Hamed v R* [2011] NZSC 101 at [161].

52 Dan Sabbagh "Regulator looking at use of facial recognition at King's Cross site" *The Guardian* (online ed, United Kingdom, 12 August 2019).

53 Tom Chivers "Facial recognition...coming to a supermarket near you" *The Guardian* (online ed, United Kingdom, 4 August 2019).

54 IPVM "UK Facewatch GDPR Compliance Questioned" (27 August 2019) www.ipvm.com.

55 Isaac Ashe "Face database to catch shoplifters in Leicestershire" The Hinckley Times (online ed, Leicestershire, 21 May 2016).

56 Stanley Benn "Privacy, Freedom, and Respect for Persons" in J Roland Pennock and John W Chapman (eds) *Privacy: Nomos XIII* (Atherton Press, New York, 1971) at 7.

Though there is limited data on public attitudes to facial recognition surveillance, one study of over 4000 UK residents found that, whilst there was broad public support of the use of FRT, this support is by no means universal or unconditional. In some limited contexts, with appropriate safeguards, a majority of the public were supportive of the use of FRT. For example, the public supported police use of FRT *if* it was effective in reducing crime, targeted and specifically regulated.[57] In some contexts, such as in schools or on public transport, the majority of participants did not support the use of FRT. Of those surveyed who were less supportive of FRT, one of the primary reasons provided was discomfort and the fear of the surveillance becoming normalised.[58]

In certain contexts, the inhibiting impact of overt surveillance technologies, such as FRT, may be particularly pronounced. In a detailed empirical study of the use of surveillance cameras and Body Worn Video in the policing of football matches in Scotland, Hamilton-Smith et al. found that the targeting and intensity of such surveillance could not only be intimidating and oppressive to football fans, but also counter-productive:

> 'The perceived consequences of focussing surveillance on sections of the stadium where younger fan groups were located was not only generating a collective sense of grievance and unfairness, but also potentially provoking the very acts of offensive gestures, speech and song that officialdom were looking to find…'

'At certain games teams of officers with cameras would generally direct their attentions towards sections of fans that were considered to be 'high risk'. This strategy was viewed as provocative and intimidatory by targeted fans. The strategy was also seen as prone to highly inconsistent enforcement outcomes, where fans at home matches may unfairly get away with songs and gestures en masse that might be more readily picked upon when captured amongst smaller fan groups in away sections.'[59]

In the United Kingdom, football fans have responded to the use of live FRT at a number of matches by wearing face coverings or holding up signage to protest its use. When South Wales Police used live facial recognition at a football match between Cardiff City and Swansea City in January 2020, this prompted condemnation from football supporters' groups and civil liberties campaigners who argued that its use on football fans was unduly stigmatising.[60]

Overt surveillance can damage legitimate political mobilisations in public space by undermining the perceived legitimacy of protest groups and limiting their access to resources.[61] These findings, which are supported by empirical research from the United States,[62] suggest that the presence of visible surveillance at meetings and other political gatherings will reduce perceptions of legitimacy, and harm the efforts of such groups to be taken seriously and attract support from their target audiences.[63] The reputational hit that political groups may take when they are subject to surveillance can also have a knock-on effect on resources and networks.[64]

The use of FRT in the private sector may also impact on these interests, while not directly engaged by NZBORA.[65] Extensive use of the technology by companies under the guise of 'public safety and to ensure that everyone who visits has the best possible experience'[66] may have an intimidatory or chilling effect on behaviour. Notably, the Ada Lovelace survey on public attitudes to

57 Ada Lovelace Institute *Beyond face value: public attitudes to facial recognition technology* (September 2019) at 10-11.

58 Ada Lovelace Institute *Beyond face value: public attitudes to facial recognition technology* (September 2019) at 9.

59 Niall Hamilton-Smith, Maureen McBride and Colin Atkinson "Lights, camera, provocation? Exploring experiences of surveillance in the policing of Scottish football" (2019) Polic Soc at 8.

60 Football Supporters Europe "FSE Opposes Fans Being Used as Test Subjects for Facial Recognition Technology" www.fanseurope.org.

61 Valerie Aston "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protestor perspectives" (2017) 8 EJLT 1 at 10.

62 Amory Starr, Luis A Fernandez, Randall Amster, Lesley J Wood and Manuel J Caro "The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis" (2008) 31 Qual Sociol 251 at 261.

63 Valerie Aston "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protestor perspectives" (2017) 8 EJLT 1 at 10.

64 Amory Starr, Luis A Fernandez, Randall Amster, Lesley J Wood and Manuel J Caro "The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis" (2008) 31 Qual Sociol 251 at 258-259.

65 New Zealand Bill of Rights Act 1990, s 3.

66 Dan Sabbagh "Regulator looking at use of facial recognition at King's Cross site" *The Guardian* (online ed, United Kingdom, 12 August 2019).

FRT indicated that support for the use of FRT in public spaces plummeted in hypothetical scenarios where the technology was being deployed by a private company.

4.7 DISCRIMINATION AND BIAS

FRT might, through selective targeting and its relative inaccuracy as applied to different demographic groups, lead to members of some groups being subject to disproportionate targeting and, thus, violate one's right to be free from discrimination. In China's Xinjiang region, FRT surveillance is assisting the Chinese Communist Party to assert control over and 'ethnically sort' the region's Uyghur Muslim minority.[67] Discriminatory practices in the targeting of FRT surveillance are not the preserve of autocracies though. More subtle forms of discriminatory targeting may arise in liberal democracies where, for example, watch lists are disproportionately populated with ethnic minorities, or deployments are unduly targeted towards minority communities.

One of the purported advantages of FRT surveillance is that it can bring objectivity to the exercise of identifying suspects or 'persons of interest' in real time. Unlike the human eye, the software "does not see race, sex, orientation or age."[68] However, this truism masks the danger that this technology can reflect, produce and maintain biases in policing and security outcomes. In particular, as discussed above, the limited independent testing and research into FRT technology indicates that numerous FRT systems misidentify ethnic minorities and women at higher rates than the rest of the population.[69]

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.

There are residual concerns that the use of FRT may damage the legitimacy of state agencies, particularly if its use is not transparent or consensual. The 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.[70] 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. Police Commissioner Andrew Coster's recent comments, when announcing that the NZ Police would not use Armed Response Teams following a trial and consultation period, indicate that the NZ Police recognise the importance of public support to successful policing: 'It is clear to me that these response teams do not align with the style of policing that New Zealanders expect... How the public feels is important - we police with the consent of the public, and that is a privilege.'[71] If surveillance technology is perceived to produce unfair or discriminatory outcomes, or is used excessively in the absence of a prescribed legal framework, there is a risk that this will corrode the legitimacy of the police. When subject to automated surveillance, it is important that the body politic can assess that any intrusion occasioned is lawful and justifiable.

The algorithms and systems that power state FRT surveillance are often proprietary in nature, and this can place further barriers in the way of their availability for scrutiny.[72] Moreover, private organisations could deploy FRT surveillance on land that is ostensibly public, and may set up partnerships with state agencies to

67 James Leiblold "Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement" (2020) 29 J Contemp China 46.

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

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

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

71 "Police ending Armed Response Teams after trial – Commissioner" *RNZ* (online ed, New Zealand, 9 June 2020).

72 Michael Vale *Algorithms in the Criminal Justice System* (Law Society of England and Wales, 2019) at 21.

share matches.[73] This has the potential to exacerbate the opacity of how FRT is being deployed, as private companies may be able to circumvent regulatory requirements on public authorities to limit their use of FRT and inform the public of how this technology is being used. There are risks that the biases of those deploying FRT may be imported into how watchlists of images are curated, and locations for public surveillance are selected. These are risks to which regulators should be alert and should manage accordingly.

4.8 PARTICULAR CONSIDERATIONS FOR DISCRIMINATION AGAINST MĀORI

Building on our more general comments about discrimination and bias, specific considerations in Aotearoa must be highlighted. The Treaty's principles requires that the impact of decisions and policies on Māori must be considered.[74] Māori are over-represented in the New Zealand criminal justice system, and this disproportionate effect is observed at all stages from apprehension to custody. "Māori are 38% of people proceeded against by Police, 42% of people convicted, and 51% of people in prison."[75]This is despite Māori making up only approximately 16% of the New Zealand population. A range of factors influence this disproportionality from the effects of colonialism,[76] the largely mono-cultural nature of the justice system, bias in decision-making, and the higher rate of adverse life events amongst Māori.[77]

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

As we expand upon in the recommendations section, the Treaty partnership requires recognition of the Treaty principles of active protection, equity, rangatiratanga and partnership, and supports the notion that Māori should have an active role in all governance decisions.

4.9 CHILDREN AND YOUNG PERSONS

As noted, children and young persons have the same general human rights protection as adults, but have certain extra rights based on their status as children. The particular impact of FRT and similar types of surveillance on children and young persons is a subject which will be explored in more detail by a number of us in a planned publication.

In general terms, UNICEF warns that biometric systems such as FRT have been primarily designed for use with adults and error rates may be larger when applied to children. Further, children may lack the capacity and agency to consent to the use of FRT. Children's rights to effective and meaningful participation are guaranteed under Article 12 of the Convention on the Rights of the Child. Children are "at the forefront of the 'big data' revolution, and this increases their likelihood of being exposed to lifelong data risks, including privacy and security concerns".[78]

Like adults, children and young persons have the right to protest and peacefully assemble.[79] Recent youth movements such as the school strike for climate have

73 In London, the use of FRT surveillance by property developer, Argent, on its publicly accessible land in the Kings Cross area of the city prompted public disquiet and an investigation by the Information Commissioner's Office. See Madhumita Murgia "London's King's Cross uses facial recognition in security cameras" *Financial Times* (online ed, London, 13 August 2019). See also: Alexander R Cuthbert and Keith G McKinnell "Ambiguous space, ambiguous rights – corporate power and social control in Hong Kong" (1997) 14 Cities 295.

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

75 Hāpaitia te Oranga Tangata: Safe and Effective Justice "Our justice system needs to change" (14 May 2019) www.safeandeffectivejustice.govt.nz.

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

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

78 UNICEF *Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes* (July 2019) at 19.

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

demonstrated the power of children's participation in the public space.[80] The use of FRT to monitor protests in public spaces may have a similar 'chilling' effect on children's freedom of expression.

In the education sphere, UNICEF notes that biometric technologies such as FRT can be used to register attendance and reduce the instances of fraud.[81] Contemporary schools have been described as being under surveillance.[82] The use of CCTV is widespread, with reports of 'function creep' starting with security and access control, evolving to a means of monitoring breaches of discipline and now to surveillance of both children and teachers. Thus, "a means justified as caring for children turns into a tool for monitoring teachers".[83] These effects are amplified where FRT is implemented or added to existing surveillance tools.

In the context of youth justice, as well as the threats to general human rights represented by the use of FRT by police, international standards require special consideration for children and young people, based on their vulnerability and lesser capacities.[84] This requires an emphasis on reintegration and should guide police decisions to retain images of children for later comparison. It is appropriate to note that Māori children and young persons are over-represented and thus will bear the brunt of FRT surveillance if implemented.[85]

4.10 CONCLUDING REMARKS

Our research indicates that, whatever the operational benefits of FRT, its use in a security or policing context is likely to be beset by multifaceted risks to human rights that require careful management or may, in certain circumstances, serve as a legal or ethical barrier to its use. Where Police intend to introduce FRT in future, the impact of this use must be fully assessed, including its operational utility, and its impact on equality, privacy, data protection, and free assembly.

80 Shelley Bouillaine ""School Strike for climate": Social Media and the International Youth Protest on Climate Change" (2020) 8 Media Commun 208; and Amanda Thomas, Raven Cretney and Bronwyn Hayward "Student Strike 4 Climate: Justice, Emergency, and Citizenship" (2019) 75 N Z Geog 96.

81 UNICEF *Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes* (July 2019).

82 Torin Monahan and Rodolfo D Torres (eds) *Schools under surveillance: Cultures of control in public education* (Rutgers University Press, United States, 2009); and Michael Gallagher "Are Schools Panoptic?" (2010) 7 Surveill Soc 262.

83 Lotem Perry-Hazan and Michael Birnhack. "Caught on camera: Teachers' surveillance in schools" (2019) 70 Teach Edu 193 at 203.

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

85 Ministry of Justice *Youth Justice Indicators Summary Report August 2019* (2019).

SECTION 5

EXISTING REGULATION OF FRT

5.1 INTRODUCTION

This section will consider how existing law and regulations in New Zealand and the European Union apply to FRT. This and the next section (considering models of law and regulation from comparable jurisdictions) provides context for our recommendations section.

There is currently no regulation in New Zealand that directly regulates FRT, although there are existing regulations that apply. The most important is the *Privacy Act 1993* which will be substituted on 1 December 2020 by the *Privacy Act 2020*. The *Privacy Act 1993* regulates the collection, storage, use and disclosure and use of personal information (collectively named personal information/data processing[1]), where personal information is information about an identifiable individual. Facial images used to identify individuals are personal information, therefore every processing of personal information, such as capturing and processing images or CCTV footage, falls under the *Privacy Act*. Thus, most of this section will be focused on data privacy laws.

It is also worth mentioning about other existing elements of statute which are relevant to FRT. As foreshadowed in Section 1, probably the most important is the *Immigration Act 2009* which specifies when the biometric information could be collected for the purposes related to immigration,[2] defines some specific uses of biometric information,[3] and contains the general rule that biometric information has to be dealt with accordance with the *Privacy Act*.[4] Other relevant statutory mechanisms are those which enable exchange of information between state agencies that may be necessary for their use of FRT . Some of those mechanisms are based directly on the *Privacy Act 1993* (Approved Information Sharing Agreements), and some are only controlled under the *Privacy Act*, but enabled in other statutory provisions and covered under broad term 'information matching'.[5] They will be described in more detail below.

5.2 RESPONSES TO HIGHER LEVEL OF RISK CAUSED BY FRT

FRT activities may introduce a high level of risk for the individual. That additional risk for a person is usually correlated in data privacy literature with profiling.[6] Profiling is processing of personal data to make detailed conclusions about certain aspects of a person.[7] The better the profile of the individual (described in data), the more impact on the individual due to the use of that profile. In other words, the more insight about individuals provided by data the more harm could be inflicted. The use of FRT may greatly enhance the profiles of those individuals by adding data identifying them as engaging in certain activities. For example, it may identify the person spotted in the street (e.g. during a protest or entering a sex shop) with the already existing online profile of that person. In such a way, it will be much harder for those individuals to keep some activities away from the scrutiny and judgment of the state or other members of society. In this respect, FRT increases the scope of data used for profiling and links them together.

The use of personal data for profiling has long been recognised in the European Union law as a factor exacerbating the potential risks and as a measure of

1 'Data processing' will be used as a catch-all term including any operation on personal data, so, e.g. collection, recording, organisation, alteration, use, or disclosure. Note that this term is not defined in New Zealand law, but it is a legal term in Europe, see Article 4(2) of the GDPR.

2 See ss 60, 100 and 111.

3 See e.g. s 28 about automatic decision making or s 32 about the obligatory privacy impact assessment.

4 Section 31.

5 See e.g. s 280(2) of the Accident Compensation Act 2001, or s 39 of the Electronic Identity Verification Act 2012; more information on Office of the Privacy Commissioner "Information matching provisions" www.privacy.org.nz>.

6 See the special role of profiling in the jurisprudence of the European Court of Justice explained by its President, Koen Lenaerts "Accountability in a digitalised world: the Court's role in enhancing data protection in the European Union" (speech to the General Data Protection Regulation five months on – 40th International Conference of Data Protection and Privacy Commissioners, 25 October 2018) at 1:30:00; Bart Schermer "Risks of Profiling and the Limits of Data Protection Law" in Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky (eds) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer, Berlin, 2013) 137; or Mireille Hildebrandt "Who is Profiling Who? Invisible Visibility" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer Netherlands, Dordrecht, 2009) 239.

7 See, e.g. definition in GDPR art 4(4).

intrusion into individual rights.[8] Although the expression 'profiling' does not appear in New Zealand's *Privacy Act 1993* (nor its successor), it is intrinsically linked with adverse consequences on the individual that are described in s 66(1)(b) of the Act (s 69(1)(b) of the *Privacy Act 2020*) and that are in many cases necessary to find the breach of privacy actionable.[9] Also, the measure of harm is taken into account by the Human Rights Review Tribunal when assessing damages.[10] In other words, New Zealand law addresses those potential risks when they have already eventuated.

Profiling by means of FRT is also particularly risky for individuals because FRT uses biometric (facial) data that cannot be changed by those individuals[11] and are used for the purposes of identifying them with high level of certainty. That increased risk might be mitigated by special treatment of biometric data that involves, for instance, more protective procedures and increased security measures. That would address the risks before they eventuate into harms.

However, New Zealand's *Privacy Act* currently offers only one level of protection for all personal information without explicitly distinguishing categories of information that create higher level of risk. Biometric information is defined in the Act only for the purposes of enabling schemes related to identification of individuals. It is worth noting that the European Union has a different approach. The General Data Protection Regulation (GDPR) defines special ('sensitive') categories of data that demand some special rules and more protection. That is the function of Article 9 of the GDPR which covers, among other types of data, biometric data used 'for the purpose of uniquely identifying a natural person'. It seems that the example of provisions of the *Immigration Act 2009* presented above shows that such approach imposing different regulations to different categories of information may also be adopted in New Zealand.

Similar effect could also be achieved by issuing a code of practice under s 46 of the *Privacy Act 1993* (s 32 of the *Privacy Act 2020*) that may introduce special rules related, for example, to a class of information.

Finally, the additional risk caused by the FRT systems may come from making decisions about individuals automatically (by the means of 'algorithms'), that is, without or with little human involvement. Such use may generate errors that are not possible to detect by humans which may rise concerns of 'being ruled by computers/robots'. Such concerns have been historically raised and resulted in the European Union in regulations against 'automatic decision making' (e.g. Art 22 of the GDPR). New Zealand does not have similar provision in the *Privacy Act* but has some experience in this area. For example, the provisions of the *Immigration Act 2009* clearly describe the scope of automatic decision making (ss 28-29A), limit the use of biometric information in decision making (s 30), and make sure that in particular circumstances decisions made automatically must for all purposes be treated as a decision of a person (see s 28(7) and s 29A(3)). This is much higher level of scrutiny than in Art 22 of the GDPR, but in much more limited scope (only particular decisions in the immigration process). Also, in New Zealand individuals have two important rights against public sector agencies under ss 22 and 23 of the *Official Information Act 1982*: right of access to internal rules affecting decisions, and right of access by person to reasons for decisions affecting that person. These could potentially be used in the context of categorisation made by the means of FRT.

It is also worth noting, that the use of algorithms by many government agencies in New Zealand is regulated by a self-adhered set of principles called the 'Algorithm Charter' which was adopted in July 2020. An FRT system that matches individuals based on their facial scans should be treated as an algorithm and also self-regulated under the Algorithm Charter.[12] That, in specific terms, may mean increased obligations as to transparency of those systems and their oversight, review and assessment for unintended consequences.

8 Koen Lenaerts, President European Court of Justice "Accountability in a digitalised world: the Court's role in enhancing data protection in the European Union" (speech to the General Data Protection Regulation five months on – 40th International Conference of Data Protection and Privacy Commissioners, 25 October 2018).

9 With the exception of breaches of privacy principle 6 or 7 described in s 66(2) of Privacy Act 1993 (s 69(2) in Privacy Act 2020).

10 See Privacy Act 1993, s 88 (Privacy Act 2020, s 103).

11 Without changing the characteristics of person's face which potentially may be achieved in a way of a major surgery.

12 "Algorithm charter for Aotearoa New Zealand" (July 2020) data.govt.nz www.data.govt.nz>.

5.3 DATA PRIVACY/DATA PROTECTION REGULATIONS

The existing regulations that apply to FRT are related to processing of personal information (or personal data).[13] Personal information (or data) is defined as information (data) that relates to an identified or identifiable natural person (individual or data subject).[14] It is widely acknowledged that images of individuals collected by surveillance systems is personal data.[15] In the case of FRT the goal of the technology is to (at least) recognise the individual, so there should be no doubt as to identifiability of data being an input to FRT process (collected images, face templates). Obviously, data that is the output of the FRT process are personal as well, as they describe particular, identified individuals and their characteristics.

The *Privacy Act 1993* (the *Privacy Act 2020* from 1 December 2020) regulates the processing of personal information by private and public sector 'agencies' in New Zealand.[16] Its provisions will also be contrasted below with the provisions of data protection regulations in the European Union:

- Regulation 2016/679 (The General Data Protection Regulation, GDPR)[17] which deals with processing of personal data in the EU in general, and
- Directive 2016/680 (The Law Enforcement Directive, LED)[18] which applies to the processing of personal data for the purposes of law enforcement by 'competent authorities' (so, Law Enforcement Agencies, LEAs).

As the EU data protection regime is the most advanced one,[19] such a comparison will allow us to consider possible ways of developing the New Zealand law to cover FRT technology.

5.4 PRIVACY ACT 1993 (AND PRIVACY ACT 2020)

The *Privacy Act 1993* is a flexible tool that permits almost all personal data activities but puts them under the limitations of the privacy principles (Informational Privacy Principles or IPPs)[20] and under the 'jurisdiction' of the Privacy Commissioner. This regulation is a much more permissive model than the European GDPR and, notably, was not changed a lot over the last 25 years. The applied model of regulation is in principle untouched by the *Privacy Act 2020* that enters into force on 1 December 2020. This is because the new Act does not aim for any more radical changes; it only introduces some amendments proposed by the Law Commission in 2011.[21] Unless specifically distinguished, both enactments will be referred below collectively as *Privacy Act*.

Deploying an FRT system either by private companies or by public authorities is legal under the Privacy Act 1993, as long as it complies with IPPs.[22] Those principles require: stating a lawful purpose (IPP1), collection of information directly from individuals (IPP2), notifying individuals (IPP3),[23] collection in a manner that is not unfair or unreasonably intrusive (IPP4), ensuring security of information (IPP5), allowing individuals access and correction of information (IPP6 and IPP7),

13 The term 'personal information' is used in New Zealand and 'personal data' is an equivalent term used in Europe. They are used in this report interchangeably.

14 GDPR, art 4(1); and Privacy Act 1993, s 21(1).

15 See e.g. C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů (Office for Personal Data Protection)* [2014] ECLI:EU:C:2014:2428; *Armfield v Naughton [2014]* NZHRRT 48; and *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin).

16 With some exceptions, for example media, Parliament, etc.

17 Article 4(1) of the GDPR; and Privacy Act 1993, s 21(1).

18 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

19 It was revised in 2016 and it contains several protections that are not accessible in any other data privacy/protection law, e.g. the right to erasure or the right not to be subject to a decision based solely on automated processing, including profiling.

20 See Privacy Act 1993, s 6 (Privacy Act 2020, s 22).

21 See more in Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123 2011).

22 Office of the Privacy Commissioner "Can I use facial recognition technology?" www.privacy.org.nz>.

23 A relatively broad exceptions to this principle apply 'to avoid prejudice to the maintenance of law … including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences', when 'compliance would prejudice the purposes of the collection', or even when 'compliance is not reasonably practicable in the circumstances of the particular case', see Privacy Act 1993, s 6 (Privacy Act 2020, s 22), IPP3, cl 4.

ensuring accurateness of information (IPP8), deleting it where it is no longer needed (IPP9), limiting the use and disclosure of information (IPP10 and IPP11),[24] and some special use of assigned unique identifiers (IPP12).[25] The new *Privacy Act 2020* contains an additional principle related to disclosure (or transfer) of information overseas (new IPP12).[26] None of these limitations is critical from the perspective of the implementation of FRT. Also, as mentioned above, neither the *Privacy Act 1993* nor *Privacy Act 2020* provide for specific, sensitive categories of data, such as biometric data that would require special protection. However, the Privacy Commissioner is clearly aware about the increased sensitivity of such information, hosting on the Commissioner's website a warning as to its security and risks for individuals associated with potential data breach.[27]

The *Privacy Act* does not provide individuals with the right to express (or deny) consent as to the information processing activities. Although IPP2 and IPP3 state that personal information (here, a facial image) needs to be collected directly from the individual and such individual needs to be informed before collection, this is not the same mechanism as consent in the European law, because such 'soft consent' need not to be clear, affirmative and explicit (as it is in the GDPR) and, importantly, cannot be revoked by the individual. This is not necessarily negative for the individual in every circumstances, as there are reasons to believe that often consent given by the individuals is not ethically or legally meaningful.[28] That is, people do not read privacy policies, even if they read them they do not understand them, they face information asymmetry and their decision are subject to a number of cognitive and structural problems with exercising their autonomy through consent.[29] In short, such consent is likely to be either not informed or not intentional and may be easily manipulated.[30] Despite these problems, the European regulation is more focused on consent. Also, despite these problems consent remains the best known legal 'tool' that enables individuals to exercise autonomy over their data. The more revealing the personal data could be, the more important is to have authorisation for collecting and using that data from the individual described. The public availability of consent notices also enables public scrutiny of data practices in relation to the use of personal information by private sector agencies.

That role in relation to processing of personal information in public sector could be performed by Privacy Impact Assessments (PIAs). Consent cannot be an appropriate method of authorisation for processing personal information by public authorities, as they need personal information to perform their tasks that are justified by some public interest. So, the only way to control their actions with personal information is through increased transparency and oversight. Those could be increased by the means of a PIA. It is an evaluation of some new product or project from the perspective of its impact on privacy that is performed by the agency and often publicly available.[31] Interestingly, the concept of a PIA is not covered at all in the *Privacy Act*. So, those evaluations are an informal way of proceeding with public projects that may have impact on privacy, like recently with the Covid App.[32] As exemplified by the *Immigration Act 2009*, the requirement of undertaking the PIA may also be expressed in the statute.[33]

24 Those principles have a very similar set of exceptions as IPP3, described above.

25 A facial template decoded from someone's face could be considered a 'unique identifier' of the individual under the Privacy Act 1993 (and, even more readily, under Privacy Act 2020). That would mean serious limitations to the use of FRT because according to IPP12 (IPP13 in the new Act) no agency could assign to the individual unique identifier that has already been assigned by another agency. Such interpretation, however, seems to be unlikely because of the current understanding and use of that term (for identifying numbers, e.g. IRD, passport, or driving licence number), and because the facial template seems to not be 'assigned' by the agency, but naturally belongs to the individual (like a fingerprint).

26 Current IPP12 has been renumbered to IPP13, see Privacy Act 2020, s 22.

27 Office of the Privacy Commissioner "Can we collect biometric information" www.privacy.org.nz>.

28 See e.g. Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880.

29 Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880 at 1882-1993A similarly, Bart W Schermer, Bart Custers and Simone van der Hof "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 Ethics Inf Technol 171 at 176–179.

30 Ruth R Faden and Tom L Beauchamp *A History and Theory of Informed Consent* (Oxford University Press, New York, 1986) at 238; also, Tom L Beauchamp and James F Childress *Principles of Biomedical Ethics* (7th ed, Oxford University Press, New York, 2013) at 104; similarly, Gerald Dworkin *The Theory and Practice of Autonomy* (Cambridge University Press, Cambridge, New York, 1988) at 81.Cambridge, New York, 1988.

31 See e.g. Office of the Privacy Commissioner "Privacy Impact Assessment Handbook" www.privacy.org.nz>.

32 See the PIA of the Covid App: Ministry of Health *COVID-19 Contract Tracing Application: Privacy Impact Assessment* (9 September 2020).

33 See Immigration Act 2009, s 32.

As the concept of the PIA is not formally defined in the law, there is currently no requirement as to its form. In the New Zealand context, the Privacy Commissioner offers informative guidelines as to the methodology of carrying it out.[34] According to the Commissioner, a PIA comprises collecting all necessary information about the project, checking it against privacy principles from the *Privacy Act*, identifying real privacy risks and the methods of their mitigation,[35] producing the report and taking action towards those risks. That process may be reinforced by additional external expertise, stakeholder involvement (consultation), improving data governance or corresponding contracts with third parties that have access to data and, finally, publication of the PIA.[36] Similarly simple PIA process comprising mainly assessing privacy risks and privacy compliance can be found in other common law jurisdictions – Australia and Canada.[37] More sophisticated and detailed PIA processes can be found in the privacy literature,[38] and in the EU, where the GDPR contains a legal obligation to perform a 'Data Protection Impact Assessment' (essentially a PIA) when personal data processing 'is likely to result in a higher risk to the rights and freedoms of a natural person may be a source of further ideas and more detailed guidance in that respect'.[39] It seems that a PIA may be an interesting procedural method to mitigate the privacy risks of using FRT.

Further, there are existing mechanisms in the *Privacy Act* that enable flexible adjustment of privacy rules to particular information, agency, activity, or class/classes of information, agency or activity. In this respect, the Privacy Commissioner can issue a code of practice under s 46 of the *Privacy Act 1993* (s 32 of the *Privacy Act 2020*) which can modify important elements of the application of the *Privacy Act*, such as, adding, changing or exempting some action from IPP. The code is a disallowable instrument, which means that it has to be presented to the House of Representatives and can be disallowed by its resolution.[40] Such code of practice is used, for example, for processing health information by health agencies.[41] Also, one such code automatically enters into force when state of national emergency is declared, which happened in April 2020 during the Covid-19 response.[42]

A privacy code of practice could be a convenient method to regulate FRT. Such regulation can be envisaged, for example, as a set of additional rules that apply to particular classes of information (facial biometric information), particular agencies (law enforcement agencies) or particular activities (remote biometric identification[43]). This would be in line with the current practice in relation to, for example, health information. It is also worth noting that the Law Commission recommended in their 2011 report that '[t]he Privacy Commissioner should consider whether it is timely

34 Office of the Privacy Commissioner "Privacy Impact Assessment Handbook" www.privacy.org.nz>

35 'A "privacy risk" is the risk that a proposal will fail to meet individuals' reasonable expectations of privacy – for instance because it breaches the Privacy Act, or unreasonably intrudes into their personal space and personal affairs, or runs contrary to what your relationship with your clients suggests should happen.', . See Privacy Commissioner *Privacy Impact Assessment Toolkit – Part 2: How to do a Privacy Impact Assessment (PIA)* (July 2015) at 12.

36 Privacy Commissioner *Privacy Impact Assessment Toolkit – Part 2: How to do a Privacy Impact Assessment (PIA)* (July 2015) at 16-17.

37 Office of the Privacy Commissioner of Canada "Privacy Impact Assessments (PIAs)" www.priv.gc.ca>; and Office of the Australian Information Commissioner "Guide to undertaking privacy impact assessments" www.oaic.gov.au>.

38 See e.g. Silvia Venier, Emilio Mordini and Michael Friedewald A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies Final Report (European Commission EC FP7-SIS; 244779; PRESCIENT 2013 See e.g. Silvia Venier, Emilio Mordini and Michael Friedewald *A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies Final Report* (European Commission EC FP7-SIS 244779; PRESCIENT, 2013); and Dariusz Kloza, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals* (d.pia.lab Policy Brief No. 1/2017, 2017).

39 See Art 35 of the GDPR; also Article 29 Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (European Commission, WP 248 rev.01, 2017); incompleteness of the PIA (called DPIA) was a ground for successful appeal in *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [145]-[154]; Information Commissioner's Office "Data protection impact assessments" (24 June 2019) www.ico.org.uk>; and Dariusz Kloza, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals* (d.pia.lab Policy Brief No. 1/2017, 2017).

40 See Privacy Act 1993, s 50 (Privacy Act 2020, s 36) and Legislation Act 2012, s 42.

41 Health Information Privacy Code 1994 replaced on 1 December 2020 by the Health Information Privacy Code 2020.

42 Civil Defence National Emergencies (Information Sharing) Code 2013 replaced on 1 December 2020 by the Civil Defence National Emergencies (Information Sharing) Code 2020.

43 Cf. distinguishing remote biometric identification from a regular biometric authentication, as activity creating particularly high risk for individuals, European Commission *White Paper on Artificial Intelligence - A European approach to excellence and trust* (COM(2020) 65 final, February 2020) at 18.

to issue a code of practice or guidance covering biometrics'.[44] Therefore, it seems that issuing such code of practice would be a natural way to deal with the increased risk created by FRT.

The *Privacy Act* contains mechanisms that enable or control the exchange of personal information between state authorities. They may be necessary for the use of FRT by state agencies, for example, when FRT is used on existing database of personal information. Those mechanisms are:

- Approved Information Sharing Agreements (AISAs) – an open framework for enabling new information exchanges across the government. See Part 9A of the *Privacy Act 1993* (Part 7 subpart 1 of Privacy Act 2020);
- Information matching – a mechanism of comparison of personal information held by different state authorities for the purpose of producing or verifying information. It is enabled by different statutory provisions, but controlled under the *Privacy Act* (Part 10 of *Privacy Act 1993*, Part 7 subpart 4 of the *Privacy Act 2020*);
- Identity information exchange – a mechanism of verification of individual identity on the basis of data held by another agency (Part 10A *Privacy Act 1993*, Part 7 subpart 2 *Privacy Act 2020*;
- Law enforcement information exchange - enables access of specified agencies to particular law enforcement information held by particular agencies (Part 11 *Privacy Act 1993* and Schedule 5, Part 7 subpart 3 *Privacy Act 2020* and Schedule 4).

Those mechanisms do not regulate FRT but regulate the exchange of personal information necessary for many uses of that technology. They are under the oversight of the Privacy Commissioner with the notable exceptions of law enforcement information exchange and identity information exchange introduced by the *Enhancing Identity Verification and Border Processes Legislation Act 2017*. Those two mechanisms appear to enable a very broad access to facial image databases. For example, as listed in Schedule 4A of the *Privacy Act 1993* (Schedule 3 of the *Privacy Act 2020*) Police has access to identity information held by the Department of Internal Affairs (passport photos) and the New Zealand Transport Agency (driver licence photos). That enables Police (subject to the technical arrangements of their access)[45] to perform a general search of those image databases in a way which is limited only by the purposes of such access listed in the *Privacy Act*. Currently Police can perform such a search to verify the identity of a person in a custody, for summons,[46] returning offender or to prevent a person to leave New Zealand to breach a condition of a sentence.[47] All those purposes can be verified only internally by Police.

As described in Section 1, there are also two statutory mechanisms enabling electronic identity verification: *Electronic Identity Verification Act 2012* and *Identity Information Confirmation Act 2012*). They enable RealMe identification service and governmentbased identity services for e-Government (or 'igovt'). The use of both of those instruments remains under the supervision of the Privacy Commissioner.[48]

5.5 THE GENERAL DATA PROTECTION REGULATION

The GDPR applies to data processing activities of entities in the EU and, in some scenarios, also outside the EU.[49] It does not apply to activities of law enforcement agencies that are performed for the purposes of law enforcement that are covered by the Law Enforcement Directive and described below. Unlike the New Zealand *Privacy Act*, under the GDPR, biometric data is explicitly defined in Article 9 which describes treatment of so-called 'special categories of data' (sensitive data). According to Art 9(1), the processing of biometric data for the purpose of uniquely identifying a natural person shall be prohibited unless special circumstances described in the following sections apply. The definition of biometric

44 See recommendation 106, Law Commission, above n 21, at 273.

45 We requested this information under the Official Information Act, but a response was not received within the timeframe for publication.

46 The Policing Act 2008, ss 32-33.

47 Privacy Act 2020, schedule 3.

48 See ss 14-16 of the Identity Information Confirmation Act 2012, and ss 7-7 of the Electronic Identity Verification Act 2012.

49 GDPR, art 3.

data explicitly refers to 'facial images',[50] so there is little doubt that every FRT system that at least identifies individuals should be treated as processing sensitive data.[51] Processing of such data is possible only under one of the exemptions defined in Article 9(2). For the purposes of FRT used by private entities for live deployment of FRT for commercial purposes those are in most cases limited to consent.[52] Such consent needs to meet several requirements. That is, it needs to be: freely given, specific, informed, unambiguous, given by a statement or clear affirmative action, explicit, possible to withdraw and not be a condition sine qua non to a service when it is not strictly necessary for provision of that service. All of this needs to be demonstrated by the data controller (agency).[53]

The fact that consent is practically obligatory for commercial FRT operations may have serious consequences for the service design. That means that a person whose face may potentially be scanned needs to consent to such data processing before it happens. According to the Guidelines of the European Data Protection Board (EDPB), a biometric system (under the GDPR) should always be run in a 'controlled environment', i.e. in an environment in which it can be used only by persons that have previously consented to such a use, or under some other appropriate exception listed in Art 9(2).[54] An environment can be put under control, for example, by deploying the system in a space which can be accessed after collection of consent, or redesigning the system to request prior affirmative action from its users (e.g. scanning the face after pushing a button).[55] Also, private data controllers need to provide individuals with a parallel, non-biometric procedure without restraints or additional costs. This is because only such a choice can allow them to freely consent to FRT. Interestingly, the pre-GDPR approach to facial recognition allowed the initial scanning of faces before their comparison to have a separate legitimate basis, 'the legitimate interest of data controller to comply with data protection rules', provided that data processed during that phase would only be processed to verify the user's consent.[56]

Such a strong emphasis on consent in commercial applications may be considered as a hurdle in many FRT scenarios. However, it ought to be noted that the GDPR also permits the EU Member States to introduce in their national laws 'further conditions including limitations' to the processing of biometric data. That was used by some member states to introduce less strict rules to FRT systems on a national level. For example, the Netherlands relaxed rules for authentication or security purposes, while Croatia did so for surveillance security systems.[57]

The GDPR contains also in Article 35 a requirement to carry out a Data Protection Impact Assessment (the equivalent of PIA). It is necessary '[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons…'. It is worth noting that this requirement is mandatory, pre-emptive as to the processing and introduces a broad assessment of different mandatory risk-related factors that have to be evaluated against the increase of the risk to the individual rights and freedoms.[58] Such a DPIA is required in particular when the systemic and extensive processing leads to decisions that significantly affect the natural persons, or processing includes the use of sensitive data on large scale or monitoring of public places on large scale.[59] These conditions may specifically fit the deployment of the FRT systems.

50 GDPR, art 4(14).

51 *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at [132]-[133].

52 European Data Protection Board *Guidelines 3/2019 on processing of personal data through video devices* (3/2019 v 2.1, 2020) at 18.

53 The GDPR distinguishes different roles in data processing. 'Controller' determines the purposes and means of the processing of personal data, while 'processor' only processes personal data on behalf of the controller. Both of those roles are covered in New Zealand law under the term 'agency'.

54 European Data Protection Board, above n 53, at 18–21. European Data Protection Board *Guidelines 3/2019 on processing of personal data through video devices* (3/2019 v 2.1, 2020) at 18-21.

55 See also other examples At 19–20. See also other examples at 19-20.

56 Article 29 Working Party *Opinion 02/2012 on facial recognition in online and mobile services* (European Commission, WP 192, 2012) at 5.

57 Michael Whitener and Raquel Aragon "How should we regulate facial-recognition technology?" (29 January 2019) IAPP www.iapp.org>.

58 Note, that the concept of "a risk to a right" appears to mix the logic of risk-management with legal rights and can be criticised, see e.g. Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit "A risk to a right? Beyond data protection risk assessments" (2016) 32 Computer Law & Security Review 286.

59 Article 35(3).

According to the GDPR, a DPIA should contain a systematic description of the envisaged processing operations, the assessment of their necessity and proportionality in relation to the purposes of processing, the assessment of the risks to the rights and freedoms of individuals, and the measures envisaged to address those risks.[60] The requirement to address the risks to rights and freedoms is notably broader than in the New Zealand PIA practice. Similarly, the requirement to assess necessity and proportionality of the processing operations impose more restrictions on the controller carrying out the DPIA than on the agency carrying out PIA in New Zealand. The GDPR contains also an invitation to seek the views of individuals themselves on the intended data processing,[61] which seems to go towards increasing individual participation and transparency. All these requirements give some insight as to the potential scope of mandating PIA of FRT systems which will be recommended in the following section.

5.6 THE LAW ENFORCEMENT DIRECTIVE

The Law Enforcement Directive (LED) was introduced in parallel to the GDPR to create a unified panEuropean set of rules that protect personal data of individuals during processing for law enforcement purposes. LED lays down the rules relating to processing of personal data by 'competent authorities' for a set of purposes related to law enforcement.[62] That set of purposes comprises 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (material scope). The competent authorities (personal scope) are the Member States law enforcement agencies (LEAs) that are entrusted by law to exercise public authority for the purposes listed in the material scope.[63] It is worth noting that the same LEAs may process data under the GDPR and under the LED depending on the purposes of processing (material scope).[64]

FRT, where deployed for the purposes of preventing threat to public security or detection of crimes, will be regulated in the EU by the LED. This regulation is slightly different and more permissive than that of the GDPR. Notably, the data minimisation principle, as stated in Article 4(1)(c) of the LED, allows to collect more data than its equivalent under the GDPR. This is because according to LED data processing cannot be excessive which is a lower threshold than 'limitation to what is necessary' defined in the GDPR.[65] The second crucial difference is lack of the requirement to consent (or option to use consent) under Article 10 of the LED which regulates processing of special categories of data (the equivalent of Article 9 of the GDPR). These rules are slightly different because the sole legal basis for FRT activities can be the performance of a task carried out by a competent authority in the public interest defined by the law. In this context, a consent requirement would not make sense.

Instead of consent, LED specifies additional obligations of the data controller that processes biometrical data. The processing of such data for the purposes of uniquely identifying a natural person is permissible where it is strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. Additionally, data processing should be explicitly authorised by law, or performed to protect the vital interests of the data subject or of another natural person, or such processing may be related to data which is manifestly made public (Article 10).

This requires LEA to prove the 'strict necessity' of FRT activities and the existence of appropriate safeguards and legitimate goal of protecting vital interests of people. For example, in the United Kingdom transposition of the Directive (Part 3 of the *Data Protection Act 2018*) a data controller has to have an appropriate policy document in place to demonstrate compliance of its safeguards and processes (s 42). That was tested by the English High Court in *Bridges* (a case which we examined in more

60 Article 35(7).

61 Article 35(9).

62 LED, art 1(1).

63 LED, art 3(7).

64 There are also other regulations that may apply here, for example processing data by Union institutions falls under Regulation 2018/1725, while Europol activities are under Regulation 2016/794. It is also possible that no European regulation applies if data processing falls outside to the Union law at all (e.g. some intelligence activities of Member States).

65 See Art 5(1)(c).

depth in the previous section) where it was determined that the police deployment of FRT was strictly necessary and according to the policy document.[66] The court seemingly had some doubts as to the appropriateness of the written policy, as it found it 'brief and lacking in detail narrative', but did not decide against the Police activities on that basis.[67] According to the Information Commissioner's Office, such 'appropriate policy' must explain procedures for complying with the data protection principles and the policy for the retention and erasure of personal data.[68] In the second instance, the Court of Appeal found additionally that the legal framework (which the policy is a part of) should specify who can be on the watchlist and where the FRT could be deployed.[69] That could be understood as necessary to fulfil the requirements of the Article 10 of the LED.

It should be noted that the Police deployment of FRT for purposes going further than uniquely identifying a natural person and strictly necessary for that goal may lack appropriate basis under the LED. This may be, for example, the case of the uses of FRT for recognising psychological characteristics.

Also, Article 27 of LED imposes the obligation of performing Data Protection Impact Assessment (so, PIA) which is stated in exactly the same words as in the GDPR.[70] Similarly, such assessment should contain at least: 'a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance [with LED] (…), taking into account the rights and legitimate interests of the data subjects and other persons concerned'.[71] Failure to meet that requirement was a ground for successful appeal in *Bridges*.[72]

Further, the LED imposes on a data controller the obligation to provide data subjects with a set of information about processing specified in Article 13. This information set is similar to the GDPR. In the case of FRT it boils down to displaying detailed information in a way in which it could be noticed before entering the FRT zone. In *Bridges*, Police went much further than that, using social media to reach out to people before the FRT was deployed at a given site, and even handing out postcard-sized notices in the vicinity.[73] That was found by the Court as 'striking the fair balance and not disproportionate'.[74]

The problem with informing individuals about using FRT for law enforcement is that sometimes it goes against the very motive for using FRT and puts LEAs in the position of conflict of interest. That is visible when Police is obliged to advertise the fact of searching for suspects to all the members of the public including those suspects. Such advertising not only undermines the goal of their activities but may also impact the effectiveness of the regulation. It is hard to assume that Police will be striving to achieve high level of individual awareness of their activities when achieving such a level frustrates achieving their goals. That tension is well documented in the ICO's documentation from control of the FRT activities of Police forces in the United Kingdom.[75] Most of the vehicles used for FRT deployment were either unmarked or only partially marked; similarly, the deployed signage did not guarantee that the members of the public see it before their faces were scanned.

The LED lays down many obligations for LEAs, but it seems that the basic function of identification of individuals for the purposes of law enforcement can be performed by the means of FRT in that regime. However, some of those obligations (like provision of information) are impractical for law enforcement and, also, the use of FRT that goes further than identification

66 *Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019)* [135]–[141]; this is nothing unusual, a similar conclusion as to the use of biometrics (fingerprints) in passports was reached by the CJEU in *Schecke v Land Hessen* [2010] ECLI:EU:C:2010:662.

67 *Bridges, R (On Application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) (04 September 2019)* [139].

68 Information Commissioner's Office "Guide to Law Enforcement Processing" (13 September 2019) www.https://ico.org.uk>; also, Information Commissioner's Office *The use of live facial recognition technology by law enforcement in public places* (1/2019 2019) at 11."plainCitation":"Information Commissioner's Office "Guide to Law Enforcement Processing" (13 September 2019

69 *Bridges, R (On the Application Of) v South Wales Police* [2020] EWCA Civ 1058 (EWCA Civ) [91].

70 LED, art 27(1).

71 LED, art 27(2).

72 *R (on the application of Bridges) v Chief Constable of New South Wales* [2020] EWCA Civ 1058 at [145]-[154].

73 *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at [39].

74 *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at [101].

75 Information Commissioner's Office *ICO investigation into how the police use facial recognition technology in public places* (2019) at 26–29.

(e.g. behaviour detection) most probably could not be based on this regulation.

5.7 CONCLUDING REMARKS

There are a number of potential takeaways from the comparison of the current legal obligations in New Zealand law with the requirements that are embedded in the European legislation. First, the private sector deployment of FRT is almost always authorised in the European Union by the consent of the individual. This tool is absent in the New Zealand legislation, which leaves individuals to some extent unprotected against private actors. Also, partly because of that, the New Zealand law does not give the individuals the same level of control over their personal data that may be used by the companies using FRT. The *Privacy Act 2020*, despite requests from Privacy Commissioner[76] and NGOs,[77] did not introduce any rights that would increase that control, such as right to erasure, or right to personal information portability.

Second, the use of FRT for policing by public authorities is under many limitations in the European Union. Most importantly, the purposes of processing should be set by the law, and the use of FRT must be 'strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject'. This is a test which requires assessment of the particular use against particular intrusion into rights of the individuals and of the general public. This is sensible, as the way the FRT is deployed and its goals may be different. For example, a form of general preventive surveillance of the society (e.g. enabling FRT of all passers-by on the streets of Wellington or Auckland to pick up all people from the police watchlist) seems to be a huge intrusion into public and individual privacy interest that is not justified by the broad goal. In turn, targeted approach against preventing particular people increasing the risk for the public (e.g. people that were arrested at the previous event of the same type[78]) from accessing a particular event would be probably less intrusive and easier to justify.[79] It seems, that this balancing process needs to be put into the New Zealand law to enable a pragmatic and proportionate response and prevent the public actors from, even benevolent, overreaching intrusions into the s 21 rights of New Zealanders and into the public interest in privacy. That balancing exercise could possibly be performed as a compulsory Privacy Impact Assessment and such requirement could possibly be introduced by the relevant code of conduct under the Privacy Act related to remote biometric identification. Both those measures could work in a more pre-emptive way than the current legal rules; they could help to mitigate the risks arising from FRT before they eventuate.

Third, there is some inherent tension in informational requirements for policing purposes which are present in the European law which seems to be impossible to avoid. If FRT is designed for particular, narrow purpose of catching wanted persons, there may be no point in informing them about it in advance. This seems to be avoided in New Zealand law by the current exceptions to IPP3 that enables agencies to not inform individuals when that would prejudice the purposes of the collection. But, this exception should be treated narrowly and if FRT is used by LEAs for other objectives (e.g. intelligence gathering) or used by the private actors for commercial purposes, the requirement to inform the individual about the use of that technology could be of a critical importance.

76 Privacy Commissioner *Privacy Commissioner's Submission on the Privacy Bill to the Justice and Electoral Select Committee* (2018).

77 Privacy Foundation New Zealand *Submission to the Justice Committee of Parliament about Privacy Bill* (2018).

78 Like in *R (on the application of Bridges) v Chief Constable of New South Wales* [2020] EWCA Civ 1058 at [29].

79 See also a "narrowly defined purpose" in Information Commissioner's Office, above n 66, at 15.

SECTION 6

POTENTIAL REGULATION OF FRT - COMPARATIVE MODELS

6.1 INTRODUCTION

The previous section considered how existing New Zealand law and regulation applies to FRT. This section analyses and reviews models of regulation from comparable jurisdictions.

The potential regulation of FRT centres on a number of questions: (how) should we limit/govern this technology? Should this be through specific rules on FRT or generic rules relating to biometrics/algorithms overall? Who or what should have oversight? Due to rights concerns, should we ban FRT completely, issue a moratorium until these are resolved, or otherwise restrict its use? A spectrum of options from several comparable jurisdictions is surveyed here, and then the next section will propose a specific set of recommendations for the New Zealand context.

6.2 BAN OR MORATORIUM ON FRT

One possible, if unlikely, approach would be to issue a ban or moratorium on FRT. This has occurred in certain public and private settings in the United States, with some other comparative examples also.

6.2.1 The United States

Just a single US state, Massachusetts, has passed a law that places comprehensive limits on law enforcement use of FRT,[1] though some cities have done so, and sector-specific limitations exist also. For instance, Oregon and New Hampshire barred the use of facial recognition searches of police body worn camera recorded footage;[2] Maine and Vermont restricted the use of facial recognition on footage collected by police drones,[3] and Michigan requires the destruction of facial recognition data from people who are arrested but never charged, or are acquitted.[4] In 2019, authorities in San Francisco banned the use of facial recognition technology, or information received from external systems that use the technology, by the police and other city agencies.[5] This was followed by the City of Oakland and the City of Berkeley.[6] Most recently the Portland City Council banned the public and private use of facial recognition technology in September 2020.[7] 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.[8] 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.[9]

1 See Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 35. This report observes that "Not a single state has passed a law that places comprehensive limits on law enforcement use of face recognition technology", though this predates the Massachusetts State Senate Bill.

2 Or Rev Stat § 133.741(1)(b)(D); and NH Rev Stat Ann § 105-D:2(XII).

3 Me Rev Stat Ann, title 25 § 4501(5)(D); and Vt Stat Ann, title 20 § 4622(d)(2).

4 Mich Comp Laws Ann § 28.243(7)-(8). See Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 35.

5 SF Admin Code § 19B.2(d); and Kate Conger, Richard Fausset and Serge F Kovaleski "San Fransisco Bans Facial Recognition Technology" *The New York Times* (online ed, New York, 14 May 2019).

6 Oakland Mun Code § 9.64.045; Edwin Chau *Resolution opposing California State Assembly Bill No. 2261* (City and County of San Fransisco, Res No 217-20, 12 May 2020) at 1; and Berkley Mun Code § 2.99.030(5).

7 Portland.gov "City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces" (press release, 9 September 2020); https://cdn.vox-cdn.com/uploads/chorus_asset/file/21868276/703_Sep_9_2TC_TW_E_Ord_BPS_1.pdf.

8 Connor Hoffman "State Sentate to vote on facial recognition moratorium bill" *Niagra Gazette* (online ed, Niagra Falls, 21 July 2020).

9 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.

6.2.2 The European Union

At the start of 2020, in a leaked draft white paper from the European Commission, the European Union signalled it would pass a moratorium of 3-5 years banning FRT.[10] However, later it decided not to implement a ban, stating instead that there should be "'clear criteria' in future mass-scale deployment of biometric identification systems in the EU."[11]

6.2.3 Scotland

Currently Scotland has a moratorium on law enforcement use of FRT, in contrast to the rest of the United Kingdom. While Police Scotland's 10-year strategy, Policing 2026, included a proposal to use of facial recognition technology,[12] a parliamentary committee was highly critical of this. The Justice Sub-Committee on Policing found that live facial recognition software is known to discriminate against women, and those from black, Asian and ethnic minority communities, that there is no justifiable basis for Police Scotland to invest in this technology; that prior to any decision to introduce FRT a robust and transparent assessment of its necessity and accuracy should be undertaken, and that the potential impacts on people and communities are understood, and that the use of live facial recognition technology would be a radical departure from the fundamental principle of policing by consent.[13] A subsequent response from Police Scotland responded that the force currently does not use live facial recognition technology, nor has plans to do so at this time, that it would ensure safeguards are in place prior to introducing the use of this technology, and agreed that the impact of its use should be understood fully before it is introduced.[14]

6.2.4 Morocco

On September 2 2019, Morocco placed a 7-month moratorium on the use of facial recognition technology for public or private use.[15] In April 2020, this moratorium was extended to the end of 2020. However certain trials and deployments of the technology can be used in specific situations, particularly technology that has the purpose of reducing health risks during the COVID-19 pandemic.[16]

6.2.5 Corporations that have halted development/ provision of FRT

In addition to public action by states in the context of law enforcement, some corporations have taken action. In June 2020, Amazon, IBM and Microsoft all stated that they would not sell any facial recognition technology to US police forces, amid increasing concerns about racial injustice in the US and the racial bias that has been found in facial recognition software. Amazon announced that it would stop providing facial recognition software to police force for one year, with the hope that the temporary pause would give US Congress time to "implement appropriate rules" around police use of the technology.[17] IBM's CEO wrote a letter to US law makers, stating that it will stop making general purpose facial recognition software altogether. The letter stressed that "now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies."[18] Similarly, Microsoft announced that it would not sell any FRT to the police until there was federal regulation around police use of the technology.[19]

10 Luana Pascu "EU considers 5-year facial recognition ban for public spaces" (17 January 2020) Biometric Update www.biometricupdate.com

11 Luana Pascu "EU no longer considering facial recognition ban in public spaces" (30 January 2020) Biometric Update wwww.biometricupdate.com

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

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

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

15 Chris Burt "Morocco places moratorium on facial recognition, California limits police use" (12 September 2019) Biometric Update www.biometricupdate.com

16 Chris Burt "Morocco extends facial recognition moratorium to year-end, proposes biometric authentication service" (9 April 2020) Biometric Update www.biometricupdate.com.

17 "We are implementing a one-year moratorium on police use of Rekognition" (10 June 2020) The Amazon blog blog.aboutamazon.com.

18 IBM "IBM CEO's Letter to Congress on Racial Justice Reform" (8 June 2020) www.ibm.com.

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

That said, it should be noted that these companies are not the top suppliers of facial recognition software to police departments in the US. Leading companies like Clearview AI, NEC, Ayonix, Cognitec and iOmnisicent all intend to continue their relationships with United States police forces.[20]

6.3 RETENTION OF THE STATUS QUO

Another option is retention of the status quo, with no specific legislation, operating with the existing legal and ethical framework, for both public as well as private use. This is the approach adopted in England & Wales, where the existing framework is regarded as sufficient. That said, the absence of specific legislation will not guard against legal challenge and it may run the risk of an overly liberal situation whereby the police may be captured by the lure and prospect of new technology, and thus push the boundaries of what is permitted and later wait for a reaction.

6.3.1 England and Wales

6.3.1.1 No specific legislative basis

England and Wales have been at the vanguard of the use of FRT, with South Wales Police[21] the London Metropolitan Police[22] and various quasi-private schemes[23] using it for policing and security purposes for several years. This is despite "the lack of a clear legislative framework for the technology".[24] Indeed, the *Protection of Freedoms Act 2012* provides a legal framework for two types of biometrics, DNA and fingerprints, but does not apply to other biometrics such as facial images, gait, or voice. No jurisdiction in the United Kingdom has introduced any specific laws relating to FRT; this situation has prompted much commentary as well as an ongoing legal challenge. A number of academic commentators, including some of this paper's authors, suggested that police deployment of FRT in England and Wales may be held unlawful due to the absence of domestic legal authorisation.[25] Moreover, the Law Society for England and Wales suggested that it is highly unclear whether facial recognition at scale can meet a test of strict necessity as required under the *Data Protection Act 2018* (DPA 2018), particularly given issues of accuracy and its "highly unproven nature".[26] The police response to this was that the legal basis regulating its proper operational limits is adequate and lies in the DPA 2018; the Surveillance Camera Code of Practice; and relevant common law and human rights principles.

Though none of these regimes provides guidelines or rules specifically regulating the police use of FRT, a recent challenge to the legality of South Wales Police's (SWP) use of FRT was dismissed on all grounds at first instance but succeeded in part on appeal. This was the first ever legal challenge to the use of FRT in the United Kingdom.

In September 2019 a Divisional Court in *R v Bridges* refused an application for judicial review challenging the legality of SWP's use of FRT.[27] SWP is the national lead on FRT in England and Wales, having received a £2.6 million government grant to test the technology. Mr Bridges had challenged the legality of SWP's use of a particular application of FRT on the grounds that its use was contrary to the *Human Rights Act 1998*, data protection legislation, and that the decision to implement it had not been taken in accordance with the *Equality Act 2010*.

It is worth highlighting some of the dimensions of the SWP initiative to illuminate the reasons behind the Court's refusal of judicial review. In April 2017, SWP began a trial of automatic FRT with subsequent national rollout in mind. The trial (which is still ongoing) comprises two pilots, once of which is known as AFR Locate and

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

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

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

23 Dan Sabbagh "Facial recognition technology scrapped at King's Cross site" *The Guardian* (online ed, United Kingdom, 2 September 2019).

24 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 29.

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

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

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

the other known as AFR Identify. The judicial review proceedings concerned AFR Locate. This involves the processing of digital images of members of the public taken from live CCTV feeds, and the comparison of this with biometric information of individuals on a watch-list compiled specifically for the deployment of FRT. The SWP takes steps to inform members of the public that AFR Locate is being used at an event or area.

In terms of human rights, the Divisional Court concluded that while the use of AFR Locate engaged the ECHR Article 8 (privacy) rights of the members of the public whose images were taken and processed, its use was in accordance with the law. FRT use was deemed to be within the police's common law powers so that there is currently no need to legislate to permit its use, at least as currently practised in the SWP pilots. Moreover, those actions were subject to adequate legal controls, contained in Data Protection legislation, statutory codes of practice, and SWP's policies. The pilots were legally justified; AFR Locate was deployed for a limited time only, for specific and limited purposes. Furthermore, unless someone's image matched that on the watchlist, all data were deleted immediately after having been processed. The CCTV feed is retained for 31 days in accordance with the standard CCTV retention period, and data associated with a match is retained within AFR Locate for up to 24 hours.

As for the data protection claims, the Court determined that the collection and processing by SWP of images of members of the public constituted collecting and processing of their personal data, notwithstanding that they might not be identifiable by name. Such processing of personal data was deemed to be lawful and to comply with the conditions in the DPA2018. The Court was also satisfied that SWP had complied with the requirements of the public sector equality duty.

Mr Bridges sought leave to appeal on a number of grounds.

The Court of Appeal ruled that the Divisional Court erred in its finding that the measures were 'in accordance with the law'. The Court analysed whether the framework governing the use of live AFR was reasonably accessible and predictable in application, and sufficient to guard against 'overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights'.[28] While statutory authorisation was not deemed to be required, the Court of Appeal was not satisfied that the SWP's use of live AFR was sufficiently regulated by the combination of the DPA 2018, the Surveillance Camera Code of Practice and SWP's local policies, as this left too much discretion in terms of who was to be placed on the watchlist, and where AFR could be deployed.[29] This is a significant finding, as it means that more detailed and circumscribed polices would address these issues and thus satisfy the 'in accordance with the law' component of Article 8(2).

The Court held that the SWP's use of AFR was a proportionate interference with Article 8 rights under Article 8(2). In addition, the Court held the Divisional Court erred in finding that SWP provided an adequate 'data protection impact assessment' (DPIA) as required by the DPA 2018. Finally, the Court of Appeal held that the SWP 'never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex.'[30]

6.3.1.2 Implications of *Bridges* for existing and proposed regulation

Bridges is a pyrrhic victory for civil libertarians. It seems to limit police powers, but as noted, some tweaks to policy, such as including more precision as to who is on police watchlists and why, and where and why AFR is deployed, should render them human rights compliant. Moreover, it is telling that SWP is not appealing.

In addition, there are several (co/pre-existing) guidance documents, such as from the Home Office Biometrics and Forensics Ethics Group (2018), and the Surveillance Camera Commissioner (2019),[31] which seek to steer police practice in this area. Though these guidance documents may be cited in court, they do not provide actionable grounds for an individual to make a complaint. Moreover, non-compliance would not impact on the admissibility of any material gleaned.

28 *Beghal v Director of Public Prosecutions* [2015] UKSC 49, [2016] AC 88 at [31] and [32] per Lord Hughes.

29 *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [96].

30 *R (on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [199].

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

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

- "Carry out a data protection impact assessment and update this for each deployment - because of the sensitive nature of the processing involved in LFR, the volume of people affected, and the intrusion that can arise. Law enforcement organisations are advised to submit data protection impact assessments to the ICO for consideration, with a view to early discussions about mitigating risk.

- Produce a bespoke 'appropriate policy document' to cover the deployments - it should set out why, where, when and how the technology is being used.

- Ensure the algorithms within the software do not treat the race or sex of individuals unfairly."[32]

In terms of any future police trials of FRT and other technologies, the London Policing Ethics Panel has proposed a framework to support analysis of the ethical issues raised field trials of policing technologies, grouping suggested inquiries into four domains: serving the public; robust trial design; respect for equality, dignity and human rights; and addressing concerns and outcomes.[33]

As will be discussed more thoroughly in the next section, we endorse the recommendation of the House of Commons Science and Technology Committee from July 2019, reiterating its recommendation from a 2018 Report, that FRT should not be deployed until concerns over the technology's effectiveness and potential bias have been fully resolved. We echo the Committee's call on to issue a moratorium until a legislative framework has been introduced and an oversight and evaluation system has been established.[34] This conclusion is relevant to New Zealand.

The House of Commons Science and Technology Committee Report also highlighted the recommendations of the Surveillance Camera Commissioner (SCC), Microsoft, and the Information Commissioner's Office regarding the need for legislation regarding biometrics such as automatic facial recognition.[35] Microsoft's involvement in this context is notable, and strategically very adept. By calling for tighter regulation it immediately reframes the debate as one around the nature and scope of laws, rather than on whether the technology should be used at all. [36]

In terms of regulatory bodies, the oversight setup in the United Kingdom relating to FRT (and indeed biometrics and forensic material more broadly) is complex and not necessarily one to replicate.[37]

Biometrics Commissioner[38]

- Statutory in nature,[39]

- Function is to keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints. FRT not within remit, though the Commissioner has been consistently critical of FRT.[40]

Forensic Science Regulator

- Non-statutory in nature,

- Role is to advise Government and the Criminal Justice System on quality standards in the provision of forensic science.[41]

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

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

34 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].

35 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].

36 Ben Wagner "Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?" in Emre Bayamlioğlu, Irina Baraliuc, Liisa Janssens and Mireille Hildebrandt (eds) *Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen* (Amsterdam University Press, Amsterdam, 2018) 84.

37 See Law Commission *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara* (NZLC IP43, 2018) at chapter 15.

38 "Office of the Biometrics Commissioner: About Us" GOV.UK www.gov.uk.

39 Protection of Freedoms Act 2012 (UK), s 20.

40 "Automated facial recognition" (10 September 2019) GOV.UK www.gov.uk. See also Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020) at 68.

41 "Forensic Science Regulator" GOV.UK www.gov.uk.

Biometrics and Forensics Ethics Group

- Non-statutory in nature,
- Role is in the consideration of the ethical impact on society, groups and individuals of the capture, retention and use of human samples and biometric identifiers for purposes which fall within the purview of the Home Office, including the differentiation between, or identification of, individuals.[42]

Information Commissioner's Office

- An independent national body responsible for upholding information rights in the public interest, covering legislation such as DPA2018, FOI2000, GDPR[43]

That said, had the guidance issued by each of these bodies been issued/considered/followed prior to police rollout of the FRT pilots the landscape would look rather different!

6.3.2 Australia

FRT is used by a number of states and agencies in Australia, though empirical evidence about the extent of use is patchy. For instance, police and city councils in Perth and Melbourne use FRT to identify individuals, but there is no indication of specific guidance or statistics linked to this.[44] Face recognition is used to access certain government services online, and the federal government in September 2020 announced plans to pour $256 million additional funding to upgrade and expand its opt-in 'digital ID' system.[45]

6.3.2.1 Identity Matching Services

At the federal level an Intergovernmental Agreement on Identity Matching Services was reached in 2017 between the Prime Minister and the first ministers of all states and territories.[46] This agreement hinged on retention or creation of legislation to support the sharing of facial images and related identity information, via a set of "identity-matching services", for a range of national security, law enforcement, community safety and related purposes.

The Identity Matching Services include the Document Verification Service (DVS); Face Verification Service (FVS), which involves one-to-one matching to help verify the identity of a known person; Face Identification Service (FIS), one-to-many or one-to-few matching to identify an known person or where a person may hold multiple identities; One Person One Licence Service (OPOLS), "a narrowly focused check, on a constrained one-to-many basis, of facial images within the National Driver Licence Facial Recognition Solution"; Facial Recognition Analysis Utility Service (FRAUS), enabling each state or territory Road Agency or licencing authority to conduct biometric matching using its own data; and the Identity Data Sharing Service (IDSS).[47]

Certain technical systems enable the operation of the Identity Matching Services, by providing the mechanisms for data sharing between Agencies.[48] The "Interoperability Hub" is a technical system that facilitates secure transmission of facial images and related identity information between Agencies and Organisations participating in the Face Matching Services.[49]

The Intergovernmental Agreement sets out several guiding principles in regard to the operation and development of identity matching services:

- Privacy by design,
- Best practice security,
- Data providers maintain access controls,
- Data quality,
- Non-evidentiary system, in that the results of

42 "Biometrics and Forensics Ethics Group: About Us" GOV.UK www.gov.uk.

43 Information Commissioner's Office "About the ICO" www.ico.org.uk.

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

45 Prime Minister of Australia "Digital Business Plan to Drive Australia's Economic Recovery" (press release, 29 September 2020).

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

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

48 Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017) at [6.1].

49 Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017) at [6.6].

identity matching are not to be the sole basis for identifying a person,

- Robust accountability.[50]

Agencies with access to the Face Identification Service may use the service for a list of specified purposes only, which centring quite an expansive interpretation of safety and security.[51] Private sector access currently is not allowed for any FRT services under the National Facial Biometric Matching Capability, though there is provision to make Facial Verification Services available to the private sector for one-to-one matching in accordance with the agreement.[52] No other FRT related services will be made available to the private sector.[53]

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

There is a memo of understanding between the Office of the Australian Information Commissioner and the Attorney General's Department on the National Facial Biometric Matching Capability,[54] setting out the role of the OAIC in relation to its role of assessing and advising the AGD in relation to FRT. While the primary focus appears to be in relation to funding the purpose of the 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".[55] Beyond this, each agency must enter into a separate agreement on data sharing and a separate MoU with the Attorney-General's Department, setting out the terms and safeguards.

6.3.2.2 Proposed federal legislation

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

While the political claim was this Bill would maintain robust privacy safeguards, the response was almost uniformly critical. The Parliamentary Joint Committee on Human Rights questioned whether the identity matching services which would be facilitated by the Interoperability Hub (the Hub) and the National Driver Licence Facial Recognition Solution (NDLFRS) were a proportionate limitation on the right to privacy and requested the advice of the Minister for Home Affairs as to whether the limitations on the right to privacy contained in the Bill are reasonable and proportionate measures to achieve the stated objective.[56] Numerous submissions to the Parliamentary Joint Committee on Intelligence and Security inquiry emphasised the definitional imprecision of the Bills, the limited oversight, the powers given to non-state entities, and the limited timeframe for review.[57] This inquiry lapsed with the dissolution of the House of Representatives in April 2019. The *Identity Matching Services Bill 2019* was reintroduced in 2019 and went before the Parliamentary

50 Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017), part 2.

51 Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017) at [4.21].

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

53 Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017) at [5.5].

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

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

56 Parliamentary Joint Committee on Human Rights *Human rights scrutiny report: Report 3 of 2018* (Australia, 27 March 2018) at [1.151]-[1.152].

57 Parliament of Australia "Review of the Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018: Submissions received by the Committee" www.aph.gov.au.

Joint Committee on Intelligence and Security again.[58] The Committee recommended that the Identity-matching Services Bill 2019 be re-drafted, taking into account the following principles:

- the regime should be built around privacy, transparency and subject to robust safeguards,
- the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality,
- the regime should be one that requires annual reporting on the use of the identity-matching services, and
- the primary legislation should specifically require that there is a Participation Agreement that sets out the obligations of all parties participating in the identity-matching services in detail.[59]

At the time of publication (November 2020), no such amendments have been circulated.

Moreover, it has come to light that the Australian Federal Police and Victoria Police have been using Clearview AI, an Australian-founded start-up which develops facial recognition software and has found itself at the centre of a data privacy debate.[60] This revelation about law enforcement use was despite initial police denials. Clearview uses an algorithm to allow users to photo anyone in public, upload it, and access any public images of that person, such as on their public social media accounts.[61] As this case exemplifies, like in *Bridges* (and New Zealand), if Australian police forces are not banned from using FRT explicitly they do not need specific legislative authority to deploy it.

6.3.3 The European Union

Beyond the General Data Protection Regulation, it looks like some specific guidance on use of FRT will emerge from the EU soon. The President of the European Commission[62] has promised new legislation "for a coordinated European approach on the human and ethical implications of artificial intelligence".[63] The European Commission White Paper on Artificial Intelligence provides that "in accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards."[64]

6.4 DISCRETE REGULATION

A further possibility is the development of a separate and distinct regulatory framework. One such example was devised in the United States, focusing on police and national security, in a 2016 report of the Center on Privacy & Technology at Georgetown Law by Clare Garvie. This provides a very helpful overview of recommendations for "commonsense" and "comprehensive" regulation,[65] which while created with the US context and legal framework in mind, are of comparative value.

The most salient recommendations include:

- "Law enforcement face recognition searches should be conditioned on an individualized suspicion of criminal conduct."

58 Parliament of Australia "Review of Identity-Matching Services Bill 2019 and the Australian Passport Amendment (Identity-matching Services) Bill 2019" www.aph.gov.au; and Identity-matching Services Bill 2019 (Cth).

59 Parliamentary Joint Committee on Intelligence and Security *Advisory Report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* (PP 458/2019, Australia, 24 October 2019) at [5.7].

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

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

62 Von der Leyen had once her fingerprints taken by a hacker from a high-resolution photo on Ministry's website: Alex Hern "Hacker fakes German minister's fingerprints using photos of her hands" *The Guardian* (online ed, United Kingdom, 30 December 2020).

63 Ursula von der Leyen *A Union that strives for more - My agenda for Europe: political guidelines for the next European Commission 2019-2024* (European Commission, October 2019) at 13.

64 European Commission *White Paper on Artificial Intelligence - A European approach to excellence and trust* (COM(2020) 65 final, February 2020) at 22. See also European Union Agency for Fundamental Rights *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Publications Office of the European Union, 21 November 2019).

65 Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 62.

- "Mug shot databases used for face recognition should exclude people who were found innocent [sic] or who had charges against them dropped or dismissed."
- "Searches of driver's license and ID photos should occur only under a court order issued upon a showing of probable cause."
- "Limit searches of license photos—and after-the-fact investigative searches—to investigations of serious offenses."
- "Real-time video surveillance should only occur in life-threatening public emergencies under a court order backed by probable cause."
- "Use of face recognition to track people on the basis of their race, ethnicity, religious, or political views should be prohibited."
- "All law enforcement use of face recognition should be subject to public reporting requirements and internal audits."
- "State … financial assistance for face recognition should be conditioned on transparency, oversight, and accountability"

State and local law enforcement should:

- "Impose a moratorium on face recognition searches of state driver's license and ID photos until state legislatures regulate that access"
- "Adopt public face recognition use policies that have received legislative review and approval."
- "Use contracts and the contracting process to maximize accuracy"
- "Implement internal audits, tests for accuracy and racial bias, and the use of trained face examiners."[66]

6.5 CONCLUDING REMARKS

A survey of potential regulation models from comparable jurisdictions demonstrate a spectrum of responses from moratorium to regulation. Our final section draws together our conclusions and recommendations.

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

SECTION 7

CONCLUSIONS AND RECOMMENDATIONS

7.1 INTRODUCTION

This section draws together the conclusions and recommendations made throughout this report. Some are of general application and others are specific (mainly to the contexts of policing/law enforcement).

Our perspective and expertise are in the law and we do not make specific recommendations about the technical operations of FRT, other than supporting the concept that systems used and acquired by the state should be industry best practice and be designed to eliminate bias and discrimination and protect privacy.

The need for regulation of FRT is a pressing one, which has even been recognised by major technology suppliers. Microsoft CEO's Brad Smith commented last year:[1]

> We believe it's important for governments in 2019 to start adopting laws to regulate this technology. The facial recognition genie, so to speak, is just emerging from the bottle. Unless we act, we risk waking up five years from now to find that facial recognition services have spread in ways that exacerbate societal issues. By that time, these challenges will be much more difficult to bottle back up.

7.2 CROSS-CUTTING ISSUES

It is worth mentioning here two issues that fall beyond the scope of this report, but which increase the importance of considering specific regulation of FRT.

7.2.1 Lack of Pathways for Individual Human Rights Complaints

This report illustrated the potential threats which FRT can pose to individual and collective rights, such as privacy, freedom of expression and procedural fairness in criminal justice processes. In other jurisdictions, individuals may use domestic human rights legislation to advance a judicial review of the effect of a piece of legislation or policy affecting their rights. This has been the case in the *Bridges* decision in England and Wales. Here, Mr Bridges alleged that the use of an automated FRT system had breached his right to respect for private life.[2]

New Zealand's system does not allow the same pathways for an individual to seek recognition and redress for a breach of human rights through the courts. While civil complaints mechanisms are available through the Human Rights Review Tribunal exist, this is a relatively weak form of protection.

This is a larger question than cannot be addressed in our report, but it does increase the importance of other forms of law, regulation and remedy where an individual believes that his or her rights have been infringed by an FRT system.

7.2.2 Treaty Principles and Māori Data Sovereignty

As we discuss in sections 2 and 3, indigenous data sovereignty is an emerging area of international human rights law and domestic human rights advocacy. We also highlighted in section 4 that Māori are disproportionally affected by the operation of the criminal justice system, including a disproportionate presence in databases of biometrics held by the Police.

We highlighted that the police documents released under the *Official Information Act 1982* show little evidence of consideration of Treaty principles or potential disproportionate impact on Māori.

Commentators have suggested that facial image data represents individual and collective whakapapa.[3]

We believe there may be an impact where a person has a moko or moko kauae, which may make the facial image of particular importance in revealing personal information.

1 Brad Smith "Facial recognition: It's time for action" (6 December 2018) Microsoft blogs.microsoft.com.

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

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

Consultation with Māori scholars and community representatives should be undertaken to explore the cultural issues embodied in the collection, retention and comparison of facial images. Māori scholars and advocates have expressed concern over data sovereignty in the context of FRT,[4] particularly where suppliers are from other jurisdictions.

Police data (including facial images) has been gathered through a system in which Māori are over-represented in apprehension, arrest and conviction. Independent oversight mechanisms that include Māori voices and apply appropriate ethical frameworks are essential.[5]

7.3 SPECTRUM OF IMPACT ON HUMAN RIGHTS

The first section of this report described the spectrum of existing uses of FRT in Aotearoa and other jurisdictions and the potential use-cases. Use by both the private and public sectors is growing exponentially. Our focus in this report is on state use of FRT, but this necessarily involves some consideration of private sector use.

The basic operational aspects of collection, retention and comparison of facial images are used in a range of contexts, not all of which are problematic and creating risks. The technology patently has many uses and potential uses which, consequently, create a spectrum of risk in terms of impact on human rights. Here, we give a broad overview of the potential risk factors. Such factors could be, for example:[6]

- Amount of personal information involved; (data minimisation, privacy by design);
- Size of the population impacted;
- Duration, or permanence, of the program or activity;
- Existence of a systemic monitoring or tracking of individuals;
- Whether the affected population is a vulnerable population;
- Profiling (and its level) or behavioural predictions;
- Data matching (linking unconnected personal information).
- Sensitivity of the personal information involved;
- Sensitivity of the context in which the program or activity will operate;
- Affecting Māori data sovereignty;
- Sharing personal information outside of the institution;
- Potential for use of the information by unauthorised third parties, value of the information for the third parties, and impact on individuals in case of such access (e.g. hacking);
- Purposes of the FRT activities, the type of potential impact on individuals and the gravity of that impact;
- The level of awareness of individuals (the use of notice and consent);
- The level of control over personal information the individuals will have;
- The existence of effective and efficient complaint system which could be used by individuals;
- The existence of oversight of an independent agency with necessary expertise;
- The transparency of FRT activities against individuals and supervising institutions;
- Using personal information for secondary purposes (also, potential for function creep);
- Use of automated or quasi-automated decision-making; (human out of the loop, human on the loop);
- High-level of outsourcing by state sector agencies the systems to suppliers from the private sector (data control by the agency);
- Transfer of data outside the jurisdiction;
- Necessary arrangements (technological, legal, contractual) against losing control over data.

The list above is not an exhaustive one. Those factors above may determine the likelihood and severity of risks

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

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

6 Prepared on the base of Office of the Privacy Commissioner of Canada "Privacy Impact Assessments (PIAs)" www.priv.gc.ca, also Office of the Australian Information Commissioner "Guide to undertaking privacy impact assessments" www.oaic.gov.au.

of FRT operations. For example, a small scale, voluntary/consent-based service which is comparing one image to another where the individual is clearly informed and provided with an alternative path of achieving the same effect without FRT would probably create a low level of risk. A scenario which involves information sharing between the agencies, which would be compulsory for a large part of the population, the service is outsourced to a third party overseas, and the information that is collected is highly valuable for third parties, would create a high risk for the individual.

Attributes of Lower- Risk FRT Activities

Consent-based FRT activities or services:

- The consent should be opt-in rather than opt-out,
- The individual clearly consents to and understands the storage and comparison of their facial image. However, we note that consent may be somewhat illusory,[7]
- An alternative path must be provided (consent without alternative means does not make sense),
- 'Isolated' uses at particular place and time ('controlled environment') with data minimisation and privacy built into design (only the necessary amount of data collected, data deleted straight afterwards),
- The use of FRT for decisions that have little gravity at an individual level (e.g. a quicker access to a service),
- Use of the application not required by the state and with alternatives that are available e.g. using another system for verification.

One to One Verification

- FRT used for comparing one image to another image.

Attributes of Medium-Risk FRT Activities

- 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,
- Activities that are quasi-compulsory, for instance where FRT comparison is required to be enrolled in passport or driving licence scheme,
- Private sector suppliers are involved, but this may be mitigated by a high degree of transparency and accountability in the contractual arrangements.

Attributes of High-Risk FRT Activities

- Compulsory to access state services,
- Decisions have grave consequences, such as identification in criminal proceedings, determination of eligibility for public services or benefits,
- Particularly wide deployments that may affect people en masse,
- Activities that could be used to track individuals, build or contribute/link to their detailed profile, discriminate against, recognise the person from the distance,
- Profiling when FRT is analysing mood/emotion/or psychographic characteristics,
- Systems that are highly automatized (human out of the loop, human on the loop),
- Systems completely controlled by the suppliers from the private sector,
- Systems which transfer data overseas without necessary contractual arrangements (against losing control over data),
- Activities that may affect Māori data sovereignty and require consultation.

Our recommendations listed below go towards elimination or mitigation of some of the risks caused by FRT. This can be done by introducing regulatory measures that should work in a systemic way (for example, by introducing regulations or appointing some overseeing institution) or by mandating the organisations that plan to use FRT to carry out the necessary analysis of, and mitigation of the risk before they start their activities (for example, high-quality Privacy Impact Assessments). The overarching goal of those recommendations is to change the New Zealand regulatory system to address and mitigate the risks of using FRT in an earlier phase, before they are eventuated.

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

7.4 GENERAL RECOMMENDATIONS

In this section, we provide general recommendations about regulation and oversight of FRT which are applicable to a range of uses of the technology.

Recommendation 1: Create a new category of personal information for biometric information

We recommend the creation of a legislative category of special sensitive personal information to cover biometric information, including facial images.

New Zealand's *Privacy Act 2020* offers currently only one level of protection for all personal information without explicitly distinguishing categories of information that create higher levels of risk. Biometric information is defined in the Act only for the purposes of enabling schemes related to identification of individuals.

It is worth noting that the European Union has a different approach. The General Data Protection Regulation (GDPR) defines special ('sensitive') categories of data that demand some special rules and more protection.

A potential definition of biometric information is that used by Scotland: "biometric data" means 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 (whether or not biometric data), to establish the identity of an individual."[8]

The increased risk that this type of information represents could be mitigated by special treatment of a new legislative category of biometric information that involves, for instance, more protective procedures and increased security measures.

Recommendation 2: Provide individuals with additional control over personal information

We recommend that New Zealand introduce additional mechanisms in the *Privacy Act 2020* that enable individuals to have a more participatory role in information processing and additional control over their information. This will improve the potential to increase accountability and trust in data handling, especially in the private sector. Such mechanisms would not require changing our flexible model of information privacy principles, but introducing into that model additional requirements related to:

- Right to object,
- Right to erasure of personal information,
- Right to personal information portability.

The *Privacy Act 2020*, despite requests from Privacy Commissioner[9] and NGOs,[10] did not introduce any rights that would increase that control.

It is worth noting, that this could help New Zealand to achieve better alignment with quickly progressing international standards for privacy legislation, that can be observed in the European's Union General Data Processing Regulation and the Council of Europe's modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data.[11] It is also worth noting that Canadian government recently introduced the Bill proposing new *Consumer Privacy Protection Act (CPPA)* that intends to give Canadians more control over their personal information by giving them possibility to withdraw the consent, disposal (permanent deletion) of information at the individual's request and disclosing the information to another organisation designated by the individual.[12] Those proposals go exactly in the direction of this recommendation.

Recommendation 3: Establish a Biometrics Commissioner or other oversight mechanism

Following the recommendation to recognise biometrics as a specific and special category of information, we recommend consideration of establishing a role of 'biometrics commissioner' to oversee collection,

8 Scottish Biometrics Commissioner Act 2020, s 23(1) and (2).

9 Privacy Commissioner *Privacy Commissioner's Submission on the Privacy Bill to the Justice and Electoral Select Committee* (2018) at 2.

10 Privacy Foundation New Zealand *Submission to the Justice Committee of Parliament about Privacy Bill* (2018).

11 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Council of Europe 108 European Treaty Series (adopted 17–18 May 2018).

12 See ss 17, 55 and 72 of Parliament of Canada "House Government Bill C-11 (43-2)" www.parl.ca.

retention, use and destruction of biometrics by state agencies.

Several Law Commission reports have flagged this as a desirable oversight mechanism. The Law Commission's review of search and surveillance noted that "a consistent approach to all biometric information may be considered desirable", but recognised that DNA contains much more personal information than other forms of biometrics.[13]

The Law Commission's Issues Paper on DNA in Criminal Investigations had as a preliminary recommendation that a new Commissioner/Regulator could be established to have oversight of matters such as:[14]

> "(a) the use of all forensic sciences in criminal investigations (in addition to DNA analysis) including the use of fingerprint, blood pattern, hair, ballistic and footprint analysis;
>
> (b) the use of biometrics generally by the State (which would include the collection and retention of digital images, fingerprints and iris scans by agencies such as the Department of Corrections, the New Zealand Customs Service and Immigration New Zealand as well as Police); and/or
>
> (c) the use of any new technologies by Police that enables some form of public surveillance (which would include use of the DNA profile databanks but also practices such as CCTV and social media monitoring)."

The recently released Law Commission Final Report on DNA states:[15]

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

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

The Scottish legislative scheme defines biometric data as "…information about an individual's physical, biological, physiological or behavioural characteristics which is capable of being used, on its own or in combination with other information (whether or not biometric data), to establish the identity of an individual."[16]

This Commissioner:[17]

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

In a New Zealand context, a potential role description could also include oversight of Māori data sovereignty issues and the operation of the Treaty partnership. The role could be potentially be operated out of the Privacy Commissioner's office or as part of his/her role.

This officeholder could also have a role in ensuring that Police adhere to statutory requirements to destroy and delete facial images and photographs where the person has not been convicted or accepts a diversion. At present, there is no independent oversight of this *Policing Act* requirement. This is the database which will be used for FRT comparisons.

Such an office-holder could also have oversight of the issue of what images should be retained and under what conditions comparisons may be made. As discussed, the

13 At para 2.38

14 Law Commission *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara* (NZLC IP43, 2018) at [15.104].

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

16 Scottish Biometrics Commissioner Act 2020, s 23(1) and (2).

17 Scottish Biometrics Commissioner Act 2020, s 2(3).

Police's ABIS database appears to contain facial images which have been collected for non-criminal regulatory purpose (firearms licencing) but which are apparently intended to be included in wider searching.

Recommendation 4: Implement high-quality Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a useful tool that may contribute towards agencies making better quality decisions, where decisions involve the assessment of risks for the individuals and protection from risks for the agency. A PIA is a systematic assessment of a project that identifies its impact on the individuals, and sets out recommendations for managing (minimising, eliminating) risks it might involve.

Our analysis of the practice of the use of that tool by government sector agencies in relation to FRT shows that it is necessary to state clearly some rules around that use to avoid treating PIAs only as a necessary burden and delay in the project. There is a precedent for setting such rules in s 32 of the *Immigration Act 2009* and the authors believe that similar provisions should be used more often, and they could be enhanced according to the description below.

PIAs should be mandatory and consider both the impact on individuals and society

The law should clearly define when it is mandatory to perform a full PIA. That level should be set at least at the threshold where there is a high-level risk for individual and/or societal values. Because of that risk and the fact that individuals have little choice in interaction with government agencies we think that it is appropriate to impose on those agencies the requirement to assess and reduce the risk. That could be expressed in a statute or in privacy code of practice (see Recommendation 6). It may be an extension of the Law Commission's recommendation to adopt such general policy in a Cabinet Office circular.[18]

Importantly, it should be explicitly stated that the role of the PIA is to define and eliminate the impact on *individuals and society*. This is because, as evidenced by some of the reviewed PIAs, the agencies have tendency to analyse the impact of their projects on their systems or on themselves.

Further, impact on the individual and collective privacy interests should be interpreted widely. That is, that impact should not be limited to analysis of privacy principles defined in the Privacy Act, but should include impact on both the privacy right and the rights protected by privacy (like freedom from discrimination, freedom of expression, assembly, association, thought, religion), and potential harms such as revelation of personal information, harms to dignity and autonomy of individuals and their social effects (e.g. chilling effects).[19] In this respect it is worth noting that current Privacy Commissioner's PIA Handbook already recommends assessment of the 'privacy risks' that are defined as risks of the failures of the project to meet individuals' reasonable expectations of privacy.[20] The PIA should be evaluated every time high risk is involved, although the systems are only 'upgraded'[21] or replaced with a new system with changed functionality. Also, 'the replacement nature' of the new system[22] should not by itself prevent the agency from preparing a PIA. This is because the new ways of processing personal information by new software and hardware components and possibly new ways of transferring them between agencies are a source of new risks that must be properly assessed and mitigated. Ideally, a PIA should be treated as a 'living instrument',[23] not a 'report', but an ongoing 'activity'[24] that continues throughout the life cycle of the designed IT process or system and is revisited when needed.

18 Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123 2011) at 262–263.

19 See section 4 for a discussion of the human rights implications.

20 Privacy Commissioner *Privacy Impact Assessment Toolkit Part 2: How to do a privacy impact assessment (PIA)* (2015) at 12.

21 This argument was made by Police in relation to the upgrade of the ABIS system.

22 This argument was made by the Department of Internal Affairs to the question why the PIA was not carried out when they were replacing the current Passport Facial Recognition System.

23 See the first best practice in Dariusz Kloza and others "Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals" (2017) 1 d.pia.lab Policy Brief at 2."plainCitation":"See the first best practice in Dariusz Kloza and others "Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals" (2017

24 Last comment from the floor in Stewart Blair "PIAs—an early warning system" (1996) 3 Privacy Law & Policy Reporter 134.

Additionally, the law could define particular risk factors that should be assessed to determine the level of the risk for individuals and trigger a PIA. Such factors could be, for example, those mentioned in section 3, above.

The practice of performing PIAs should adhere to some general guidance defined by the law

The law should define the role and goals of carrying out PIAs in relation to FRT and ways of achieving them. That, in our view, could be achieved by defining the following 5 goals which could be complemented by specific guidelines issued by a supervisory authority (e.g. a Biometrics Commissioner, see Recommendation 3).

First, there should be a requirement of presenting the envisaged project and information flows:

> (1) Presenting a thorough, systematic description of the project and information flows.[25]

Such description was clearly missing in some of the PIAs considered during this research.

The current PIA guidelines of the Privacy Commissioner and the *Immigration Act 2009* define two main roles for the PIA,[26] which could be adapted as below:

> (2) Identifying the potential effects that the proposal may have upon personal privacy *and the corresponding interests of society*,
>
> (3) Examining how any *of those* detrimental effects on privacy might be lessened.

Further, we believe that the law should provide for some general principles to ameliorate the privacy risks, which could be found in necessity and proportionality.[27] That could be summarised as:

> (4) Showing that the organisation and design of the proposed project are necessary for legitimate purposes, and do not introduce measures that intrude into privacy and the corresponding interests of society to an extent that is not proportional to those purposes.

Such general guidance seems to be necessary to ensure that PIAs are not merely a tick-box exercise, but that they shape the systems and processes in a way which protect the interests of individuals and society.

We also believe that the law should provide some general guidance as to *ways* of ameliorating the privacy risks. This could be done for example by defining the following goal:

> (5) Showing that the proposal has considered and, if appropriate, minimised the collection and use of personal information, incorporated privacy into design and made use of privacy enhancing technologies.[28]

As mentioned above, this definition of goals of PIA may be complemented by a specific guidance issued by Biometric Commissioner (or/and Privacy Commissioner) and the template for conducting PIAs for FRT, similar to the one published by the United Kingdom's Surveillance Camera Commissioner and Information Commissioner.[29] Such regulation would be capable of achieving both certainty as to the defined goals and principles, and elasticity in light of technological advancement.

The law should define the standards for transparency and external engagement in defining PIAs

For the sake of accountability and public trust, PIAs for FRT systems should be well documented and transparent.[30] A PIA should be written with an expectation that it will be widely disseminated and

25 Office of the Privacy Commissioner of Canada, above n 5; Office of the Australian Information Commissioner, above n 5; Article 29 Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248rev01 2017) at 22; Step 2 in Information Commissioner's Office "Data Protection Impact Assessments (DPIAs)" (18 September 2020) https://ico.org.uk.

26 Office of the Privacy Commissioner of Canada, above n 5, also s 32 of the Immigration Act 2009.

27 Office of the Australian Information Commissioner, above n 6, also the GDPR Art 35(7)(b). Office of the Privacy Commissioner of Canada, above n 5.

28 Office of the Australian Information Commissioner, above n 6; Office of the Privacy Commissioner of Canada, above n 5.

29 Information Commissioner's Office and Surveillance Camera Commissioner *Data protection impact assessments for surveillance cameras* (2018).

30 See the best practice 8 in Kloza and others, above n 23, at 2; Office of the Privacy Commissioner of Canada, above n 5.above n 21, at 2; Office of the Privacy Commissioner of Canada, above n 5.

published.[31] That does not mean that the whole PIA must be published, but at least its summary and conclusions.[32] Such transparency may help ensure that the high-risk system is thoroughly examined from the perspective of its safety (as 'sunlight is the best disinfectant'[33]), and may also build trust amongst the individuals that the system will have impact on. For example, in Australia government agencies keep a register of PIAs on their website and the Australian Bureau of Statistics publishes all carried out PIAs.[34]

Further, the PIA should not be an isolated exercise. The law should prescribe that the agency implementing FRT systems should actively engage with external stakeholders, including the affected groups and, if appropriate, the general public. Also, the assessors should be independent from the assessed entity. They may be in-house or external but should not receive instructions from the assessed entity. For government agencies, this could ideally be, for example, the Government Chief Privacy Officer. Involvement of the Privacy Commissioner should be carefully considered, because of the Commissioner's quasijudicial, independent role in investigating privacy complaints. The potential for a conflict of interest should be balanced with gains from early involvement of the oversight body.[35] Having said that, the Privacy Commissioner (or/and Biometrics Commissioner) should be the source of the detailed guidelines for PIAs.[36] The Privacy Commissioner should also be informed after the PIA is concluded which may enable him (or her) to issue a compliance notice under s 123 of the *Privacy Act 2020* if a breach of the Privacy Act or a privacy code of practice is found.

Recommendation 5: Add enforceability and oversight to Algorithm Charter

The use of algorithms by government agencies in New Zealand is regulated by a voluntary set of principles called the 'Algorithm Charter' which was adopted in July 2020. As was discussed in Section 3, signatories include the New Zealand Police, MBIE and a range of other agencies.

A FRT system that matches individuals on the basis of their facial scans should be treated as an algorithm and also self-regulated under the Algorithm Charter.[37] That, in specific terms, may mean increased obligations as to transparency of those systems and their oversight, review and assessment for unintended consequences.

The Principles of the Algorithm Charter were discussed in an earlier section and are in summary:

- Transparency,
- Partnership,
- People,
- Data,
- Privacy, ethics and human rights.

The Algorithm Charter is a useful standard that mirrors many other similar ethical standards in comparable jurisdictions. However, it does not have any enforceability mechanisms. It cites the best practice but does not have a remedy for non-compliance. It does not solve the issue of an individual who is concerned that state use of FRT may breach their human rights and wishes to ensure that their rights have been protected or raise awareness of a breach of human rights or privacy standards.

We recommend that consideration is given to oversight and audit mechanisms for the Algorithm Charter. The administering agency, Stats NZ are intending to review the Algorithm Charter one year after implementation.[38]

Some options for increasing oversight and audit of implementation of and compliance with the Charter could be:

31 Trilateral Research & Consulting *Privacy impact assessment and risk management—Report for the Information Commissioner Office* (2013) at 27.

32 Similarly Article 29 Working Party, above n 24, at 18; also, Office of the Privacy Commissioner of Canada, above n 5, see also s 32(4) of the Immigration Act 2008.

33 Attributed to J Louis Brandeis.

34 Australian Bureau of Statistics "ABS Privacy Impact Assessments" www.abs.gov.au/websitedbs/d3310114.nsf.

35 So, potential for greater effectiveness and efficiency, more in Blair Stewart "Privacy Impact Assessment: Optimising the Regulator's Role" in David Wright and Paul De Hert (eds) *Privacy Impact Assessment* (Springer Netherlands, Dordrecht, 2012) 437; John Edwards "Privacy Impact Assessment in New Zealand – A Practitioner's Perspective" in David Wright and Paul De Hert (eds) *Privacy Impact Assessment* (Springer Netherlands, Dordrecht, 2012) 187 at 199.Dordrecht, 2012

36 Cf. different approach in s 32(2)-(3) of the Immigration Act 2008.

37 "Algorithm charter for Aotearoa New Zealand—data.govt.nz" https://data.govt.nz.

38 Stats NZ *Report to the Minister of Statistics: Releasing the Algorithm Charter* (July 2020).

- The existing Data Ethics Advisory Group[39] could be empowered to oversee adherence to the Algorithm Charter,
- Agencies required to report annually on their compliance with the Algorithm Charter,[40]
- A requirement that policy proposals are assessed for compliance with the Algorithm Charter. This could involve an Algorithm Impact Assessment, a process akin to the Privacy Impact Assessment.[41]
- Creation of an individual complaint mechanism – perhaps to the Biometrics Commissioner?

Further, Gavaghan et al, in their review of the use of artificial intelligence by the New Zealand Government have recommended the creation of a regulatory agency to monitor algorithm use:[42]

> One possible role for such an agency in New Zealand would be in providing a pre-implementation "safety check" for government use of predictive algorithms. For example, technical experts could validate their accuracy and transparency, while legal and ethical members would consider potential human rights or privacy breaches.

Recommendation 6: Transparency in the use of FRT

The prevalence of current and planned use of FRT across state agencies and particularly by the Police and has only come to light through investigations by journalists and academic researchers.

We are of the view (and support similar recommendations made by others in relation to algorithms generally),[43] that state agencies are transparent about their use of FRT.

We also recommend that agencies are transparent in their processes around carrying out Privacy Impact Assessments (see also Recommendation 4), information sharing agreements (see also Recommendation 8), auditing and mitigation of error rates.

Recommendation 7: Implement a code of practice for biometric information

While we also recommend the consideration of a new role of biometrics commissioner, a parallel or preliminary exercise would be the establishment of a Code of Practice for Biometric Information.

We believe that the development of technology justifies the establishment by the Privacy Commissioner of a new privacy code of practice for biometric information under s. 32 of the *Privacy Act 2020*. Such a code would be capable of imposing tougher controls on the collection and handling of biometric information than those that apply to the collection and handling of personal information. Those tougher controls could involve, for example, an obligation related to FRT systems to carry out high-quality Privacy Impact Assessments. That would be in line with similar codes for health information[44] or credit reporting.[45] Also, it would be in line with the recommendation of the Law Commission from 2011 that 'that this is an area where greater certainty and guidance would be useful'.[46] The Law Commission recommended that the code should be developed on the base of the Australian Biometrics Institute Privacy Code. However, the Australian code, which was voluntary, was revoked in April 2012 due to the low number of subscribers.[47]

39 One of the authors (Lynch) is currently a member of this Group. These are personal views rather than the views of the Group.

40 We note that this would have significant resourcing implications.

41 Dr Andrew Chen has made this point in his submission on the Algorithm Charter. All submissions may be found here https://cdm20045.contentdm.oclc.org/digital/collection/p20045coll24/id/378/rec/1. The Canadian government has also been working on an algorithm impact assessment process: Government of Canada "Algorithmic Impact Assessment (AIA)" (28 July 2020) www.canada.ca.

42 The Law Foundation *Government Use of Artificial Intelligence in New Zealand* (2019) at [69].

43 The Law Foundation *Government Use of Artificial Intelligence in New Zealand* (2019).

44 Health Information Privacy Code 2020.

45 Credit Reporting Privacy Code 2020.

46 See recommendation 106 in Law Commission, above n 16, at 273.

47 "Privacy Act 1988 - Revocation of the Biometrics Institute Privacy Code - Explanatory Statement" (April 2012) www.legislation.gov.au.

Recommendation 8: Information sharing agreements for facial images must be appropriate and transparent

Experience from other jurisdictions shows the issues that may occur where databases of facial images are shared inappropriately between law enforcement and other state agencies for FRT comparison to be undertaken.[48]

As part of the research, we were interested in investigating whether New Zealand Police have access to existing databases of facial images such as the driving licence database and the passports database. Access to these databases 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.

Our overarching view is that it is inappropriate for law enforcement to have access to broad population level databases of facial images such as driver licensing and passport databases except in very clear situations involving a specific risk to public safety.

At the time of writing, the privacy legislation is in transition, with the new Privacy Act 2020 coming into force on 1 December 2020. The Privacy Act 2020 allows agencies a few different information exchange mechanisms. Police appear to have an identity information sharing agreement with several agencies (including DIA in its capacity as the administrator of the Citizenship and Passports Acts).

This was a set of agreements that are wider than the issue of FRT and collection of facial images.[49] We make comment here on the basis that this is a system which appears to empower large scale sharing of the passport database with frontline police officers, and thus has relevance in considering potential usage for FRT.

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

- of a person in lawful custody who has been detained for committing an offence whose identifying particulars (which includes facial images) have been taken,[50] or
- of someone whose particulars have been taken to send a summons, where the constable has good cause to suspect and intends to bring proceedings,[51] or
- of a returning offender[52] whose particulars have been taken.

This appears to have been put in place in response to the Philip Smith case, where an offender managed to obtain a passport and flee the jurisdiction.[53]

Police's own press release states the broad purposes of the system:[54]

> The system allows Police 24/7 access to passport and birth information, making it easier to identify a person police are taking enforcement action against. This is particularly valuable when police have arrested a person or suspect that a person has breached a court order. "This electronic access to passport and birth information improves Police's ability to better manage the identities of people entering the criminal justice system," says National Manager Criminal Investigations Tim Anderson. The improvements build on recent automated access for Police to driver licence images held by the NZ Transport Agency, as well as immigration data and photos from Immigration New Zealand (INZ). Police can send a subset of data back to INZ under certain conditions.

The mandatory reporting of the use of this agreement in the Police Annual Report suggests that this identity verification method was used over 250,000 times in less

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

49 For context see Treasury *Impact Summary: Improvements to the accuracy and timeliness of Police information regarding name changes, deaths and non-disclosure directions* (April 2019).

50 Policing Act 2008, s 32.

51 Policing Act 2008, s 33.

52 Returning Offenders (Management and Information) Act 2015.

53 Which initiated policy changes that were further enacted in Enhancing Identity Verification and Border Processes Legislation Act 2017.

54 New Zealand Police "Improvements to information sharing between DIA, the Registrar-General, Births, Deaths and Marriage and Police" (press release, 3 May 2019).

than 12 months.[55] The annual report reports queries made from Police to Immigration New Zealand: The Police on-duty mobile application was used to make 78,005 queries to the INZ system, including for suspects/offenders 45,118 times. 180,263 queries were made in total from the Police NIA desktop application.

While it is not possible for us to gain further information on the nature of these queries[56] and not all will involve transfers of biometric information such as facial images, it does suggest that the use of the interface has become a regular part of policing. This power, added to the increased functionalities of the ABIS system, creates the architecture for a significant surveillance system. These surveillance tools must be carefully regulated.[57]

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

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

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

By contrast Customs report that they accessed information from the Department of Corrections 362 times in the 2019 reporting period.[58]

Customs annual report states that:[59]

> In each instance where Customs accessed data held by the Department of Corrections (Corrections) it related to an alert created by Corrections (Customs' border management system electronically screens passenger information for matches, enabling Customs to notify Corrections if a person subject to an alert arrives at the border). Customs submitted a phone and email request to Corrections for offender images and supporting details to verify the identity of the person attempting to depart New Zealand – Corrections supplied an email response with an attached photograph.

It appears as if Customs usage is triggered by a very specific set of procedures, while Police use appears to be more widespread.

When this report was at the editing stage, a Official Information Act request was received back from MBIE, which had been an extension of time. This request revels a list of information sharing agreements relating to FRT. These include with other jurisdictions such as the Five Eyes partners, Crimestoppers and other NZ government agencies. There was not time to make another request for individual agreements, but the authors intend to pursue this line of enquiry. [60]

Recommendations:

- Information sharing agreements and identity verification access agreements must be clear and transparent,
- Police should not have the power to conduct general speculative searches across either the passport or driving licence databases, given the broad coverage of these databases,
- All information sharing mechanisms should have stringent and appropriate oversight to avoid scope creep.

55 New Zealand Police *Annual Report 2018/19* (November 2019) at 178.

56 We sought further information under the Official Information Act.

57 Privacy Commissioner *Privacy Commissioner's Submission to the Law and Order Commitee on the Enhancing Identity Verification and Border Processes Legislation Bill 147-1* (November 2016).

58 New Zealand Customs Services *Annual Report 2019* (B.24 AR, 2019) at 11.

59 New Zealand Customs Services *Annual Report 2019* (B.24 AR, 2019) at 11.

60 Source: Official Information Act Request DOIA 2021:0838, 27 November 2020.

7.5 POLICING

As we discuss throughout this report, the sphere of deployment where FRT represents the greatest potential threat to human rights is in the areas of policing and intelligence. That threat is posed by the disparity in power between the individual and the state, the consequences of the decisions which may impose criminal sanctions including the deprivation of liberty, and the potential for discriminatory use against individuals or groups.

A recent stocktake of Police use of technology released under the *Official Information Act 1982* reveals several existing and planned systems with FRT capability. Again, there is a spectrum of risk, with some lower-risk systems that involve searching of legally obtained evidence, but there are also systems with capability for targeted and mass surveillance activities that clearly pose high-risk.

As detailed in the first section, systems that are in place include:

- BriefCam – analysis of CCTV footage including facial images,
- NewX "Searches unstructured data and platforms for faces, guns, and body markings (tattoos)"
- Cellebrite – searches seized cell-phone for data. Includes FRT capability,
- ABIS (Automated Biometric Information Survey) -FRT capability.

Planned systems include: [61]

- Digital Information Management. ICTSC has indicated it will be running an RFI/RFP to look at systems that will store both evidential information and CCTV, social media and photographs. It is likely the tenders will list AI and potentially facial recognition as part of the requirements.

There is also discussion of drones, and CCTV feeds into a national command centre, both of which can relatively easily be equipped with FRT capability. The rapid pace of development of surveillance technology and systems involving FRT algorithms means that the July 2020 stocktake may quickly be out of date.

Police's overall view is that the public can be reassured that Police are not planning to use the various new capabilities; they also want to make sure that regulating the law enforcement use of FRT will not blunt our ability to respond quickly and effectively to threats to the safety.[62] However, even if some technologies become relatively widespread in the private sector, their use by police raises different issues, related to power imbalance and trust.[63]

As the Biometrics Commissioner for England and Wales has stated:[64]

Public trust in policing must be retained as new technologies are deployed. The mere fact that private companies are using many of the same technologies does not mean that in using the same technologies the police can assume public trust. The police will always be a special case because they embody the power of the state to sanction behaviour deemed unacceptable.

Recommendation 9: A moratorium on the use of live AFR by Police

As we have discussed throughout this report, we regard live automatic facial recognition technology (AFR) as the most problematic in terms of impact on individual and societal rights.

In a recent stocktake report on technology,[65] New Zealand Police have stated that they will not use this technology, but have the capability, and indeed recently concluded a deal to purchase a new system which has this capability. While the statement that Police have no plans to use the technology is welcome, there is currently no official position on this, and no legal or regulatory barrier to the police deployment of this technology.

Currently New Zealand, like many other jurisdictions, has a regulatory gap that can permit troublesome surveillance practices.

61 New Zealand Customs Services *Annual Report 2019* (B.24 AR, 2019) at 5.

62 Clare Garvie, Alvaro Bedoya and Jonathan Frankle *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy & Technology, 18 October 2016) at 72.

63 Ben Bradford, Julia A Yesberg, Jonathan Jackson and Paul Dawson "Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology" (2020) 60 Br J Criminol 1502; and Neil Selwyn, Beatriz Gallo Cordoba, Mark Andrejevic and Liz Campbell *AI for Social Good? Australian public attitudes towards AI and society* (Monash University, 2020).

64 Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020) at [63].

65 New Zealand Police *Assurance review of emergent technologies* (July 2020). Released under the Official Information Act.

The policy of non-deployment appears dependent on a current Police leadership position and the management lines within the police.

We do not consider that there is currently a case for live FRT public space monitoring as a legitimate and proportionate policing tool.

Our strong view is that there should be a formal moratorium on the use of AFR by police.

Recommendation 10: Consultation and consideration of legislation

Building on several the threads of the recommendations, a legislative regime for the use of FRT by the Police should be considered.

The need for legislative authorisation has been raised by the Biometrics Commissioner for England and Wales:[66]

The bigger question going forward is whether there should be new legislation that provides new rules for the police (and perhaps others) use of new biometrics, including LFR but also voice recognition, gait analysis, iris analysis or any other new biometric technologies as they emerge. The alternative is that we are likely to see further legal challenges to other biometric use by the police. In the absence of new legislation such challenges will be helpful in clarifying how the police may act but will mean that the police exploration of new biometrics will be slowed and rely on judge-made law, something that most of the judiciary do not like doing, preferring that if there needs to be a legal response to social and technological change that it should be through legislation made by Parliament.[67]

At present, the situation regarding the collection, retention, comparison and matching of facial images by Police is very complex, sitting across numerous pieces of legislation, regulation and policy. There remains a significant regulation gap. As discussed in the context of other recommendations, there are synergies with an recently finalised review of the DNA legislation by the Law Commission.

We recommend that consideration be given to

- A statute which would regulate the collection, retention and comparison of biometrics in a policing context;
- A clear legislative framework for the power to collect, retain and compare facial images across government agencies.

Recommendation 11: Review of collection and retention of facial images by Police

Matters to resolve when considering the appropriate parameters of a police power to use facial recognition technology include identifying where the facial images which populate a potential image database are derived from and the threshold to meet before the database of images may be searched.

Information sharing between agencies was discussed in an earlier recommendation, but here we will make some recommendations about a database of images held by Police. Documents obtained under the OIA show that the Police ABIS system contains around 2 million images.[68] While all of these are lawfully held, there may be questions as to whether it is legitimate to search these using FRT.

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

- A decision not to charge,
- Acquittal.

The images may be retained after the following events:[69]

- Diversion,
- Conviction,
- Section 283 (*Oranga Tamariki Act 1989*) orders in the Youth Court,

66 Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020) at [33].

67 Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020) at [43].

68 National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020) at 4.

69 Policing Act, s 34A.

- Discharged under s. 106 of the *Sentencing Act*.

Documents report that the new image management system holds 1.85 million images from 800,000 individuals in these categories and expecting to add 50,000 per annum.[70]

It also appears to hold some voluntarily provided images from children and young persons. Police also hold facial images of child sex offenders and returning offenders.

There is a general expectation that those persons whose offending has been proved must accept that there will be storage of data related to their offending.

Documents indicate that police intend to use their new system to create a suspect category where an officer can seek a facial comparison of an image of a suspect with a database:

> These images will be used for facial comparison purposes and searched against the known person databases (Offender, Voluntary, Customs, Child Sex Offenders, Returning Offenders, Firearms Licence holders and Missing Persons) to provide intelligence / identity of the individual featured in the Suspect image.

While the other categories involve persons whose offending have been proved, and there would be a case for inclusion and search of missing person images, the inclusion of firearms licence holders appears incongruous. Firearms licence holder images comprise around 250,000 images, which is a significant portion of the New Zealand population.[71]

There is a question as to the lawfulness of this retention and potential comparison. The privacy statement declares that the use of the photograph is for the purpose of the Arms Act 1983. There could be a case for comparison where a police officer believes that a potential licensee is committing fraud in applying for the licence (where banned from being licenced) but should not be used for general speculative searching .There may be considerable public concern about this given that collection and retention of facial images of firearm licence holders is a regulatory function of the Police, rather than a criminal investigation function.

Our recommendation is that Police:

- Review whether over 250,000 images of firearm licence holders are properly associated in a database with convicted persons, given that licensing is a regulatory power un-associated with investigation and prosecution of criminal offending. If the intention is to have separation, that should be a clear and public policy statement;
- Consider whether images of children and young persons should be retained given the different principles applying to the youth justice system;
- Consider whether indefinite retention aligns with other schemes for retention of biometrics (e.g. DNA retention periods, which are not uniformly indefinite);
- Consider whether retention policies align with the principles of the *Criminal Records (Clean Slate) Act 2004* legislation, which provides for reintegrative responses for less serious offending;
- Provide reporting on the ethnicity of those persons whose images are held (as with the DNA database) which then provides transparency for patterns in image collection practices.

Recommendation 12: Threshold before comparison can be made in Police's image system

Following on from the last recommendation, we recommend Police consider application a threshold of 'reasonable suspicion' or similar before FRT comparison can be done on already collected images. While the search of the database is not akin to live AFR, being able to carry out functions such as a search across large amounts of CCTV footage potentially allows Police to build a picture of a person's movement and link to their identity.

It may be that Police have procedures such as this already in place, and the stocktake document does discuss that there are oversight mechanisms, but a clear policy of a threshold linked to a standard of reasonable suspicion would reduce the risk of speculative searches or other scope creep.

70 National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020) at 4.

71 National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020) at 4.

Recommendation 13: Oversight of the Police's image database

As discussed in the previous recommendations, there are concerns about the range of images that are stored in the ABIS system and whether their retention and comparison is legitimate.

We recommend that the Police establish an oversight mechanism with independent representation to ensure that the image database (and any potential FRT or other matching proposals).

It would be appropriate if this group contained some independent members to provide assurance to the public. Māori representation is particularly important, given the over-representation in the criminal justice system. A proposed Biometrics Commissioner role would be at a level above this.[72]

Recommendation 14: Oversight of emerging technology such as FRT

As discussed, the controversial trial of Clearview by New Zealand Police earlier in 2020 sparked a review of the use of technology for police and the publication of a set of guidelines.

The stocktake recommended:[73]

- Centralised governance,
- A new policy,
- A comprehensive 'deep dive' into ethical and privacy implications.

Guidelines for trial of emerging technology were published recently.[74] Police are now required to:

- Seek advice from senior management even when responding to an offer from a technology company, even where the new technology would only be explored in a non-operational test setting,
- Approval for any trial must now be sought from the Police Security and Privacy Reference Group, and endorsed by the Organisational Capability Governance Group,
- Submissions for approval are expected to consider ethical and human rights considerations, including public expectations and legal obligations surrounding the right to privacy.

These are welcome developments, but, again, Police should have a clearer policy statement and independent oversight.

Police policy on emerging technology also seems to be guided purely by the *Privacy Act 2020* and the Principles for the Safe and Effective Use of Data and Analytics. While adherence to these standards is valid and important, missing aspects are:

- Principles of human rights law as defined in an earlier section (allowing broader consideration of principles such as the right to be free from discrimination, freedom of expression, right to peacefully protest),
- Principles of the Treaty of Waitangi.

It must be noted that the privacy impact assessment contains out of date information that the *Bridges* decision complied with human rights – this was not the case in the Court of Appeal finding.

Recommendation 15: Regulate surveillance using FRT in public places

In Recommendation 9 we recommended that a moratorium on the use of live AFR is put in place. Here, we foreshadow some broader recommendations around conditions giving rise to a lifting of a moratorium, building on our points above around specific regulation of biometrics made above.

As technology rapidly develops, state operated CCTV cameras will be able to be cheaply and easily fitted with FRT capability. This could involve Police operated surveillance but also cameras operated by local government and in precincts such as the parliamentary grounds.

72 We support the oversight model recommended by the Law Commission in their recently released report on DNA and consider that this type of oversight mechanism could also oversee biometrics. Law Commission *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara – Final Report (2020).*

73 National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020) at 11.

74 New Zealand Police *Police Proposals to test or trial the use of emergent technologies* (September 2020).

We believe that use of FRT in public places by the state should be carefully regulated, necessary, proportionate and restricted to limited circumstances involving serious crime or significant risks to public safety.

The New Zealand Law Commission's work on reviewing the *Search and Surveillance Act 2012* found that public surveillance is different from surveillance normally carried out under the this Act as it is usually not targeted at a particular person. As the Law Commission notes: [75]

> An argument could be made that the use of public surveillance for law enforcement purposes raises different considerations, in light of the significant resources and coercive powers available to the State. If surveillance becomes too frequently used in circumstances beyond the investigation of specific offences (where a reasonable belief threshold must be met), the general public may feel they are being treated as suspects. This could have a chilling effect on the exercise of rights such as freedom of expression.

The Law Commission's review proposed an option that the Act could require authorisation where: [76]

> Camera footage taken by a police officer in the street during an incident may be comparable to footage that could be taken by a member of the public, so would not require authorisation. However, systematic CCTV surveillance across a city would be substantially different in character, particularly if it could be: used to track an individual's movements; or linked with facial recognition software and cross-referenced against a police database to identify wanted people.

In New Zealand, the use CCTV has not been considered objectionable, but the Law Commission found that "modern technology allows this type of public information to be gathered in large volumes, aggregated and used in increasingly sophisticated ways";[77] facial recognition is one of these ways as it "… allow[s] video data to be quickly processed and matched against government databases to identify potential offenders in a way that was previously impossible."[78]

While covert video surveillance in a public place is not currently regarded as a search by New Zealand case-law, there is developing case-law in other jurisdictions on the subject.[79] As we discuss in section 4, there is a reasonable argument that use of FRT in a public place might be a considered a search for the purposes of s. 21 of the NZBORA.

We also support the Law Commission's recommendation that there be a policy statement on public surveillance in the *Search and Surveillance Act 2012*.[80]

We recommend that the following principles are mandated for any use of FRT in public places:

- Limited to serious crime;
- Limited to specific locations;
- There must be a reasonable suspicion;
- Independent oversight/authorisation of use.

7.6 CONCLUDING REMARKS

The risks of using FRT need to be properly managed. We recommend a set of general and particular requirements that aim at addressing those risks with necessary regulation and oversight mechanisms. Those mechanisms should also increase public trust.

Public trust is essential for state services and particularly in policing. Our overarching recommendation is for transparency and consultation.

Extensive media reporting has shown the level of public concern about the use of such technology. Minority groups and those affected disproportionately must be consulted on potential use and given opportunities to be involved in oversight.

We place the burden firmly on those who want to use FRT, particularly live FRT to demonstrate not only its utility as a surveillance tool, but also due appreciation of its broader social impact and the factoring of this into any assessment of use.

75 Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.125].

76 Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [2.118].

77 Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.115].

78 Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.116].

79 Douglas A. Fretty, "Face-recognition surveillance: A moment of truth for fourth amendment rights in public places." (2011): Va. JL & Tech. 16 430; Andrew Guthrie Ferguson, "The Smart Fourth Amendment." *Cornell L. Rev.* 102 (2016): 547.

80 Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016) at [3.129].

SECTION 8

SELECTED BIBLIOGRAPHY

8.1 CASES

8.1.1 New Zealand

Armfield v Naughton [2014] NZHRRT 48.

Attorney-General v Taylor [2018] NZSC 104.

Attorney-General v Udompun [2005] 3 NZLR 204.

Beagle v Attorney-General [2007] DCR 596.

Child Youth and Family Services v Television New Zealand Ltd (2005) 24 FRNZ 857 (HC).

Fensom v KME Services NZ Pty Limited [2019] NZERA Christchurch 728.

Flickinger v Crown Colony of Hong Kong [1991] 1 NZLR 439.

Greenwood v Attorney-General [2006] DCR 586.

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

Hemmes v Young [2005] NZSC 47, [2006] 2 NZLR 1.

H v F (1993) 10 FRNZ 486 (HC).

Lorigan v R [2012] NZCA 264.

Moonen v Film and Literature Board of Review [2000] 2 NZLR 9 (CA).

Moonen v Film and Literature Board of Review [2002] 2 NZLR 754 (CA).

New Zealand Air Line Pilots' Association Inc v Attorney-General [1997] 3 NZLR 269 (CA).

Puli'uvea v Removal Review Authority [1996] 3 NZLR 538 (CA).

Oosterman v Attorney-General DC Rotorua CIV-2006-063-384, 1 July 2008.

Quilter v Attorney General [1998] 1 NZLR 523 (CA).

Rajan v Minister of Immigration [1996] 3 NZLR 543 (CA).

Re the W Children (1994) 12 FRNZ 548 (FC).

R v Alsford [2017] NZSC 42.

R v Butcher [1992] 2 NZLR 257 (CA).

R v Fraser [1997] 2 NZLR 442 (CA).

R v Gardiner (1997) 15 CRNZ 13.

R v Goodwin [1993] 2 NZLR 153 (CA).

R v Ngan [2007] NZSC 105, [2008] 2 NZLR 48

R v Shaheed [2002] 2 NZLR 377 (CA).

Simpson v Attorney-General [Baigent's Case] [1994] 3 NZLR 667 (CA).

Taunoa v Attorney-General [2007] NZSC 70.

Tavita v Minister of Immigration [1994] 2 NZLR 257 (CA).

Taylor v Attorney-General [2015] NZLR 791.

Van Essen v Attorney-General [2013] NZHC 917, [2014] NZAR 809.

8.1.2 United Kingdom

Beghal v Director of Public Prosecutions [2015] UKSC 49, [2016] AC 88.

Malone v The United Kingdom [1984] ECHR 10.

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

RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012] EWHC 1681.

R (on the application of Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.

8.1.3 European Cases

C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů (Office for Personal Data Protection)* [2014] ECLI:EU:C:2014:2428.

8.2 BOOKS AND CHAPTERS IN BOOKS

James S Anaya *International Human Rights and Indigenous Peoples* (Aspen Publishers, New York, 2009).

Tom L Beauchamp and James F Childress *Principles of Biomedical Ethics* (7th ed, Oxford University Press, New York, 2013).

Gerald Dworkin *The Theory and Practice of Autonomy* (Cambridge University Press, Cambridge, New York, 1988).

Stanley Benn "Privacy, Freedom, and Respect for Persons" in J Roland Pennock and John W Chapman (eds) *Privacy: Nomos XIII* (Atherton Press, New York, 1971).

Andrew Butler and Geoffrey Palmer *Constitution for Aotearoa New Zealand* (Victoria University Press, Wellington, 2016).

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

Ruth R Faden and Tom L Beauchamp *A History and Theory of Informed Consent* (Oxford University Press, New York, 1986).

Kelly Gates *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, New York, 2011).

Janine Hayward '"Flowing from the Treaty's Words": The Principles of the Treaty of Waitangi', in Janine Hayward and Nicola R Wheen (eds) *The Waitangi Tribunal: Te Roopu Whakamana i te Tiriti o Waitangi* (Bridget Williams Books, Wellington, 2004) 29.

Mireille Hildebrandt "Who is Profiling Who? Invisible Visibility" in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds) *Reinventing Data Protection?* (Springer Netherlands, Dordrecht, 2009) 239.

Grant Huscroft "The Attorney-General's Reporting Duty" in Paul Rishworth, Grant Huscroft, Scott Optican and Richard Mahoney (eds) *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003).

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

Tahu Kukutai and John Taylor (eds) *Indigenous Data Sovereignty: Towards an Agenda* (ANU Press, Canberra, 2016).

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

Arthur R Miller *The Assault on Privacy: Computers, Data Banks, and Dossiers* (University of Michigan Press, Ann Arbor, 1971).

Torin Monahan and Rodolfo D Torres (eds) *Schools under surveillance: Cultures of control in public education* (Rutgers University Press, United States, 2009).

Matthew Palmer *The Treaty of Waitangi in New Zealand's Law and Constitution* (Victoria University Press, Wellington, 2008).

Paul Rishworth, Grant Huscroft, Scott Optician and Richard Mahoney *The New Zealand Bill of Rights* (Melbourne: Oxford University Press, 2003).

Bart Schermer "Risks of Profiling and the Limits of Data Protection Law" in Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky (eds) *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Springer, Berlin, 2013) 137.

Ben Wagner "Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?" in Emre Bayamlioğlu, Irina Baraliuc, Liisa Janssens and Mireille Hildebrandt (eds) *Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen* (Amsterdam University Press, Amsterdam, 2018) 84.

Alan F Westin *Privacy and Freedom* (Atheneum Press, New York, 1967).

Margaret Wilson *The Struggle for Sovereignty: New Zealand and Twenty-First Century Statehood* (Bridget Williams Books, Wellington, 2015).

8.3 JOURNAL ARTICLES

Sawsan Abuhammad, Omar F Khabour and Karem H Alzoubi "COVID-19 Contact-Tracing Technology: Acceptability and Ethical Issues of Use" (2020) 14 Patient Prefer Adherence 1639.

Mark Andrejevic and Neil Selwyn "Facial recognition technology in schools: critical questions and concerns" (2020) 45 Learn Media Technol 115.

Nur Diyanah Anwar and Cameron Sumpter "Societal resilience following terrorism: Community and coordination in Christchurch" [2020] Behav Sci Terrorism Polit Aggres 1.

Valerie Aston "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protestor perspectives" (2017) 8 EJLT 1.

Nila Bala "The danger of facial recognition in our children's classrooms" (2020) 18 DLTR 249.

Lindsey Barrett "Ban Facial Recognition Technologies for Children - And for Everyone Else" (2020) 26 JOSTL 223 at 258.

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

Ben Bradford, Julia A Yesberg, Jonathan Jackson and Paul Dawson "Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology" (2020) 60 Br J Criminol 1502.

Philip Brey "Ethical Aspects of Facial Recognition Systems in Public Places" (2004) 2 JICES 97.

Andrew Butler and Petra Butler "The Judicial Use of International Human Rights Law in New Zealand" (1999) 29 VUWLR 173.

Heather Buttle and Julie East "Traditional facial tattoos disrupt face recognition processes" (2010) 39 Perception 1672.

Margarita Robles Carrillo "Artificial intelligence: from ethics to law" (2020) 44 Telecomm Policy.

Kate Crawford "Regulate facial-recognition technology" (2019) 572 Nature 565.

Alexander R Cuthbert and Keith G McKinnell "Ambiguous space, ambiguous rights – corporate power and social control in Hong Kong" (1997) 14 Cities 295.

John Danaher "Could There Ever be an App for that? Consent Apps and the Problem of Sexual Assault" (2018) 12 Crim Law Philos 143.

Fiona de Londras "Dualism, Domestic Courts, and the Rule of International Law" in Mortimer Sellers and Tadeusz Tomaszewski (eds) *The Rule of Law in Comparative Perspective* (Springer, Dordrecht, 2010) 217.

Paula Donnolo and Kim K Azzarelli "Ignoring the Human Rights of Children: A Perspective on America's Failure to Ratify the United Nations Convention on the Rights of the Child" (1996) 5 JL & Pol'y 203.

S Every-Palmer, R Cunningham, M Jenkins and E Bell "The Christchurch mosque shooting, the media, and subsequent gun control reform in New Zealand: a descriptive analysis" [2020] Psychiatr Psychol Law 1.

"Facial-recognition research needs an ethical reckoning" (2020) 587 Nature 330.

Charles Fried "Privacy" (1968) 77 Yale LJ 475.

Michael Gallagher "Are Schools Panoptic?" (2010) 7 Surveill Soc 262.

Claudia Geiringer "The Dead Hand of the Bill of Rights? Is the New Zealand Bill of Rights Act 1990 a Substantive Legal Constraint on Parliament's Power to Legislate?" (2007) 11 OLR 389.

Claudia Geiringer "The Principle of Legality and the Bill of Rights Act: A Critical Examination of *R v Hansen*" (2008) 6 NZJPIL 59.

Claudia Geiringer "On a Road to Nowhere: Implied Declarations of Inconsistency and the New Zealand Bill Of Rights Act" (2009) 40 VUWLR 613.

Claudia Geiringer "Inaugural Lecture: Mr Bulwark and the Protection of Human Rights" (2014) 45 VUWLR 367.

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

Janneke Gerards "The fundamental rights challenges of algorithms" (2019) 37 NQHR 205.

Felipe Gómez Isa "The UNDRIP: an increasingly robust legal parameter" (2019) 23 Int J Hum Right 7.

Anna Gurinskaya "Predicting citizen's support for surveillance cameras. Does police legitimacy matter?" (2020) 44 IJCACJ 63.

Niall Hamilton-Smith, Maureen McBride and Colin Atkinson "Lights, camera, provocation? Exploring experiences of surveillance in the policing of Scottish football" (2019) Polic Soc.

Tom Hickman "Bill of Rights Reform and the Case for Going Beyond the Declaration of Incompatibility Model" [2015] NZ L Rev 35.

Janet L Hiebert "Rights-vetting in New Zealand and Canada: similar idea, different outcomes" (2005) 3 NZJPIL 63.

John Ip "Attorney-General v Taylor: A Constitutional Milestone?" [2020] NZ L Rev 35.

Jonathan Jackson, Ben Bradford, Mike Hough and Katherine Murray "Compliance with the law and policing by consent: notes on police and legal legitimacy" in Adam Crawford and Andrea Huckles (eds) *Legitimacy and Compliance in Criminal Justice* (Routledge, Abingdon, 2013) 29.

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

Kenneth J Keith '"Concerning Change": The Adoption and Implementation of the New Zealand Bill of Rights Act 1990" (2000) 31 VUWLR 37.

Paula King, Donna Cormack and Mark Kopua "Oranga Mokopuna-A tāngata whenua rights-based approach to health and wellbeing" (2018) 7 MAI Journal 187.

Brendan F Klare, Mark J Burge, Joshua C Klontz, Richard W Vorder Bruegge and Anil K Jain "Face Recognition Performance: Role of demographic information" (2012) 7 TIFS 1789.

Kyriakos N Kotsoglou and Marion Oswald "The Long Arm of the Algorithm? Automated Facial Recognition as Evidence and Trigger for Police Intervention" (2020) 2 FSI Synergy 86.

Chei Sian Lee, Dion Hoe-Lian Goh, Sei-Ching Joanna Sin, Hamzah Osop and Yin Leng Theng "Finding trafficked children through crowdsourcing" (2019) 55 Proceedings of the Association for Information Science and Technology 811.

James Leiblold "Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement" (2020) 29 J Contemp China 46.

Leslie Lenert and Brooke Yeager McSwain "Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic" (2020) 27 J Am Med Inform Assoc 963.

Joy Liddicoat, Colin Gavaghan, Alistair Knott, James Maclaurin and John Zerilli "The use of algorithms in the New Zealand public sector" [2019] NZLJ 26.

Steven Livingston and Mathias Risse "The future impact of artificial intelligence on humans and human rights" (2019) 33 Ethics Int Aff 141.

Jessica Long "Facial recognition trial at tertiary providers could lead to wider use in schools" *Stuff* (online ed, New Zealand, 26 February 2019).

Adam Lopatka "An Introduction to the United Nations Convention on the Rights of the Child" (1996) 6 TLCP 251.

Gary Lynch-Wood and David Williamson "The social licence as a form of regulation for small and medium enterprise" (2007) 34 J Law Soc 321.

Ioana Macoveciuc, Carolyn J Rando and Hervé Borrion "Forensic Gait Analysis and Recognition: Standards of Evidence Admissibility"(2019) 64 J Forensic Sci 1294.

Dominic McGoldrick "The United Nations Convention on the Rights of the Child" (1991) 5 IJLPF 132.

Lorna McGregor, Daragh Murray and Vivian Ng "International Human Rights Law as a Framework for Algorithmic Accountability" (2019) 68 ICLQ 309.

Janet McLean "Legislative invalidation, human rights protection and s 4 of the New Zealand Bill of Rights Act" (2001) NZL Rev 421.

Janet McLean "Crown Him with Many Crowns: The Crown and the Treaty of Waitangi." (2008) 6 NZJPIL 35.

Sharon Nakar and Dov Greenbaum "Now you see me. Now you still do: Facial Recognition Technology and the growing lack of privacy" (2020) 23 JOSTL 88.

Claire Methven O'Brien and Jolyon Ford "Business and Human Rights: From Domestic Institutionalisation to Transnational Governance and Back Again" (2019) 37 Nord J Hum rights 216.

Richard Parsons and Kieren Moffat "Constructing the meaning of social licence" (2014) 28 Soc Epistemol 340.

Nicholas Petrie "Indications of Inconsistency" (2019) 78 CLJ 612.

Arthur Piper "ABOUT FACE: The Risks and Challenges of Facial Recognition Technology" (2019) Risk Management 18.

Joe Purshouse and Liz Campbell "Privacy, Crime Control and Police Use of Automated Facial Recognition Technology" (2019) 3 Crim Law Rev 188.

Rebecca Rios-Kohn "The Convention on the Rights of the Child: Progress and Challenges" (1998) 5 Geo J Fighting Pov 139.

Paul Rishworth "Reflections on the Bill of Rights after Quilter v Attorney General" [1998] NZ L Rev 683.

Mathias Risse "Human rights and artificial intelligence: An urgently needed agenda" (2019) 41 HRQ 1.

Catherine Rodgers "A Comparative Analysis of Rights Scrutiny of Bills in New Zealand, Australia and the United Kingdom: Is New Zealand Lagging Behind its Peers?" (2012) 21 APR 4.

Antoaneta Roussi "Resisting the Rise of Facial Recognition" (2020) 587 Nature 350.

Bart W Schermer, Bart Custers and Simone van der Hof "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 Ethics Inf Technol 171.

Daniel J Solove "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880.

Amory Starr, Luis A Fernandez, Randall Amster, Lesley J Wood and Manuel J Caro "The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis" (2008) 31 Qual Sociol 251.

Nili Steinfeld "Situational user consent for access to personal information: Does purpose make any difference?" (2020) 48 Telemat Inform.

Amanda Thomas, Raven Cretney and Bronwyn Hayward "Student Strike 4 Climate: Justice, Emergency, and Citizenship" (2019) 75 N Z Geog 96.

Tom R Tyler "Enhancing Police Legitimacy" (2004) 593 Ann Am Acad Pol Soc Sci 84.

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

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

Sally Wheeler "Committing to human rights in Australia's corporate sector" [2019] Griffith LR 1.

8.4 REPORTS

Ada Lovelace Institute *Beyond face value: public attitudes to facial recognition technology* (September 2019).

AI Forum New Zealand *Trustworthy AI in Aotearoa: AI Principles* (March 2020).

ANZPAA *Australia New Zealand Police Recommendations for CCTV Systems* (2014).

Australian Government Department of Home Affairs *Privacy Impact Assessment: Law Enforcement, Crime and Anti-Corruption Agency Use of the Face Matching Services, NFBMC (v.1.0)* (Bainbridge Associates, March 2019).

Gabrielle Berman, Karen Carter, Manuel Garcia-Herranz and Vedran Sekara *Digital contact tracing and surveillance during COVID-19: General and child-specific ethical issues* (UNICEF, WP 2020-01, June 2020).

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

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

Joy Buolamwini and Timnit Gebru *Gender Shades: Intersectional Accuracy Disparities in Commerical Gender Classification* (Conference on Fairness, Accountability, and Transparency, 2018).

Centre for Data Ethics and Innovation *Snapshot Series: Facial Recognition Technology* (May 2020).

Council of Europe Commissioner for Human Rights *Unboxing Artificial Intelligence: 10 steps to protect Human Rights* (Council of Europe, May 2019).

Bethan Davies, Martin Innes and Andrew Dawson *An Evaluation of South Wales Police's Use of Automated Facial Recognition* (CUPSI, September 2018).

Digital Council *Trust and Automated Decision-Making: an interim report on the Digital Council's 2020 Research* (2020).

European Commission *White Paper on Artificial Intelligence - A European approach to excellence and trust* (COM(2020) 65 final, February 2020).

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

Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Christopher Nagy and Madhulika Srikumar *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* (Berkman Klein Center for Internet & Society, January 2020).

Pete Fussey and Daragh Murray *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (Human Rights Centre, July 2019).

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

Patrick Grother, Mei Ngan and Kayee Hanaoka *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* (NISTIR 8238, November 2018).

Patrick Grother, Mei Ngan and Kayee Hanaoka *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (NISTIR 8280, December 2019).

IEEE *Ethically Aligned Design – First Edition: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (EAD1e, 2019).

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

Independent High-Level Expert Group on Artificial Intelligence *Ethics Guidelines for Trustworthy AI* (European Commission, April 2019).

Information Commissioner's Office *ICO investigation into how the police use facial recognition technology in public places* (October 2019).

Lucas D Introna and Helen Nissenbaum *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (The Center for Catastrophe Preparedness and Response, July 2009).

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

Dariusz Kloza, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals* (d.pia.lab Policy Brief No. 1/2017, 2017).

The Law Foundation *Government Use of Artificial Intelligence in New Zealand* (2019).

Ministry of Business, Innovation and Employment *Privacy impact assessment report: Collection and handling of biometrics at the Ministry of Business, Innovation and Employment* (May 2016).

Ministry of Business, Innovation and Employment E*lectronic Travel Authority (ETA): Summary of Submissions Report* (August 2018).

Ministry of Health *COVID-19 Contract Tracing Application: Privacy Impact Assessment* (9 September 2020).

Ministry of Justice *Re-Evaluation of the Human Rights Protections in New Zealand* (2000).

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

National Biometric Information Office, the Assurance Group and New Zealand Police *IMS Photo Manager and ABIS 2 Project Privacy Impact Assessment* (October 2020).

New Zealand Customs Services *Annual Report 2019* (B.24 AR, 2019).

New Zealand Customs Service *Remediation Report: Review of eGate Processes and the Use of the Decision Review Tool* (28 March 2019).

New Zealand Police *Annual Report 2018/19* (November 2019).

New Zealand Police *Assurance review of emergent technologies* (July 2020).

New Zealand Police *Police Proposals to test or trial the use of emergent technologies* (September 2020).

Aleksandr Parkin and Oleg Grinchuk *Recognizing Multi-Modal Face Spoofing with Face Recognition Networks* (CVPR Workshop Paper, Long Beach, 2019).

Police Scotland *Policing 2026: Our 10 Year Strategy for Policing in Scotland* (June 2017).

Principal Advisor: Privacy, Assurance Group, PNHQ *Assurance review of emergent technologies* (New Zealand Police, July 2020).

Privacy Commissioner *Privacy Impact Assessment Toolkit – Part 2: How to do a Privacy Impact Assessment (PIA)* (July 2015).

Privacy Commissioner *Privacy Commissioner's Submission to the Law and Order Commitee on the Enhancing Identity Verification and Border Processes Legislation Bill 147-1* (November 2016).

Privacy Commissioner and Stats NZ *Principles for the safe and effective use of data and analytics* (May 2018).

Harrison Rudolph, Laura M Moy and Alvaro M. Bedoya *Not Ready for Takeoff: Face Scans at Airport Departure Gates* (Georgetown Law Center on Privacy & Technology, 21 December 2017).

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

Neil Selwyn, Beatriz Gallo Cordoba, Mark Andrejevic and Liz Campbell *AI for Social Good? Australian public attitudes towards AI and society* (Monash University, 2020).

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

Stats NZ *Report to the Minister of Statistics: Releasing the Algorithm Charter* (July 2020).

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

UNICEF *Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes* (July 2019).

Michael Vale *Algorithms in the Criminal Justice System* (Law Society of England and Wales, 2019).

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

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

Silvia Venier, Emilio Mordini and Michael Friedewald *A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies Final Report* (European Commission EC FP7-SIS 244779; PRESCIENT, 2013).

Stats NZ *Algorithm Assessment Report* (October 2018).

Treasury *Impact Summary: Improvements to the accuracy and timeliness of Police information regarding name changes, deaths and non-disclosure directions* (April 2019).

The University of Auckland and Stats NZ *Surveys, social licence and the IDI* (December 2016).

Ursula von der leyen *A Union that strives for more - My agenda for Europe: political guidelines for the next European Commission 2019-2024* (European Commission, October 2019).

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

Paul Wiles *Annual Report 2019: Commissioner for the Retention and use of Biometric Material* (Office of the Biometrics Commissioner, March 2020).

8.5 PARLIAMENTARY MATERIALS/GOVERNMENT PUBLICATIONS

8.5.1 New Zealand

Cross Government Biometrics Group *Guiding Principles for the Use of Biometric Technologies for Government Agencies* (Department of Internal Affairs, April 2009).

Kenneth Keith "Introduction" in Cabinet Office, Department of the Prime Minister and Cabinet *Cabinet Manual* (Wellington, 2017).

Law Commission *A New Zealand Guide to International Law and its Sources* (NZLC R34, 1996).

Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123 2011).

Law Commission *Review of the Search and Surveillance Act 2012* (NZLC IP40, 2016).

Law Commission *Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012* (NZLC R141, 2017).

Law Commission *The Use of DNA in Criminal Investigations: Te Whakamahi i te Ira Tangata i ngā Mātai Taihara* (NZLC IP43, 2018).

Legislation Design and Advisory Committee *Legislation Guidelines: 2018 Edition* (March 2018) at [9.2].

Geoffrey Palmer "A Bill of Rights for New Zealand: A White Paper" [1984-1985] I AJHR A6.

Justice and Law Reform Select Committee "On a White Paper of a Bill of Rights for New Zealand" [1998] AJHR 3.

8.5.2 International

Amnesty International and Access Now *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems* (May 2018).

Article 29 Working Party *Opinion 02/2012 on facial recognition in online and mobile services* (European Commission, WP 192, 2012).

Article 29 Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (European Commission, WP 248 rev.01, 2017).

Edwin Chau *Resolution opposing California State Assembly Bill No. 2261* (City and County of San Fransisco, Res No 217-20, 12 May 2020).

Concluding Observations of the United Nations Human Rights Committee on New Zealand CCPR/C/SR. 2026 (17 July 2002).

Concluding Observations of the United Nations Human Rights Committee on New Zealand CCPR/C/NZL/CO/6 (31 March 2016).

Council of Australian Governments *Intergovernmental Agreement on Identity Matching Services* (Australia, 5 October 2017).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

European Data Protection Board *Guidelines 3/2019 on processing of personal data through video devices* (3/2019 v 2.1, 2020).

Government Digital Service *Data Ethics Framework* (2020).

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).

Parliamentary Joint Committee on Human Rights *Human rights scrutiny report: Report 3 of 2018* (Australia, 27 March 2018).

Parliamentary Joint Committee on Intelligence and Security *Advisory Report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* (PP 458/2019, Australia, 24 October 2019).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

Second Periodic Report of New Zealand to the Committee on the Rights of the Child CRC/C/93/Add.4 (2003).

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

UN Committee on Economic, Social and Cultural Rights *General Comment No. 20: Non-discrimination in economic, social and cultural rights (art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights)* E/C.12/GC/20 (2 July 2009).

UN Committee on Economic, Social and Cultural Rights *General Comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities* E/C.12/GC/24 (10 August 2017).

UN Committee on the Rights of the Child *Consideration of Reports Submitted by States Parties Under Article 44 of the Convention: New Zealand* CRC/C/93/Add.4 (2003).

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

UN Committee on the Rights of the Child *Draft General Comment No. 25 (202x): Children's rights in relation to the digital environment* CRC/C/GC/25 (13 August 2020).

United Nations Declaration on the Rights of Indigenous Peoples GA Res 61/295 (2007).

United Nations *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (United Nations Human Rights Office of the High Commissioner, New York and Geneva, 2011).

United States Constitution

8.6 NEWSPAPER ARTICLES

Rizwan Asghar "Covid-19 and the privacy trade-off" *Newsroom* (online ed, New Zealand, 22 May 2020).

Isaac Ashe "Face database to catch shoplifters in Leicestershire" The Hinckley Times (online ed, Leicestershire, 21 May 2016).

Leah Asmelash "New York's MTA is asking Apple to create a Face ID that works with masks" *CNN* (online ed, United States, 11 August 2020).

The Associated Press "UK, Australia investigate Clearview facial recognition firm" *ABC News* (online ed, Australia, 10 July 2020).

Tim Biggs "The fact and fiction of FaceApp" *Stuff* (online ed, New Zealand, 18 July 2019).

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

George Block “Privacy concerns over police’s new ‘state of the art’ facial recognition system” Stuff (online ed, New Zealand, 5 December 2019).

George Block “Police facial recognition: Privacy Commissioner not consulted on new system” *Stuff* (online ed, New Zealand, 8 December 2019).

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

Ariel Bogle “Porn age filter for Australia recommended by parliamentary committee” *ABC News* (online ed, Australia, 5 March 2020).

Vickie Chachere “Biometrics Used to Detect Criminals at Super Bowl” *ABC News* (online ed, Australia, 8 January 2006).

“Chinese police spot suspects with surveillance sunglasses” *BBC News* (online ed, United Kingdom, 7 February 2018).

Tom Chivers “Facial recognition…coming to a supermarket near you” *The Guardian* (online ed, United Kingdom, 4 August 2019).

Kate Conger, Richard Fausset and Serge F Kovaleski “San Fransisco Bans Facial Recognition Technology” *The New York Times* (online ed, New York, 14 May 2019).

Ben Cost “Russia rolls out new ‘Orwell’ facial recognition tracker for school kids” *New York Post* (online ed, United States, 18 June 2020).

Amanda Cropp “Border reform next in queue” *Dominion Post* (online ed, Wellington, 30 September 2017).

Jason Davis “Biometric screening at airports is spreading fast, but some fear the face-scanning systems” *NBC News* (online ed, United States, 15 March 2018).

Richard Davison “Southland farm owners ‘extremely gutted’ by $65k stock theft” *New Zealand Herald* (onlime ed, New Zealand, 21 May 2019).

Shawna De La Rosa “New York City students protest school surveillance cameras” (25 March 2019) Education Dive www.educationdive.com.

Collette Devlin “Wellington City Council and NEC camera technology watching commuters” *Stuff* (online ed, New Zealand, 7 April 2016).

Laurence Dodds “China’s TikTok twin using facial recognition to censor foreigners” *New Zealand Herald* (online ed, New Zealand, 13 July 2020).

Sue Dudman “New tool helps to recover lost pets” *Wanganui Chronicle* (Wanganui, 27 March 2018).

M L Elrick “Detroit protesters take fight against facial recognition tech to city leaders’ homes” *Detroit Free Press* (online ed, United States, 15 June 2020).

Carl Engelking “Facial Recognition Software: The Next Big Thing in Species Conservation?” *Discover* (online ed, United States, 18 February 2017).

Marrissa Fessenden “Researchers Are Using Facial Recognition Software To Save Lions” *Smithsonian Magazine* (online ed, United States, 7 July 2015).

“Fight for the Future: More Than 150 College Faculty Staff Sign Open Letter Against Facial Recognition on Campus” *Targeted News Service* (online ed, New York, 28 February 2020).

“Future facing: Ticketless plane travel and face scanners, what it means for privacy” *New Zealand Herald* (online ed, New Zealand, 12 June 2019).

Jono Galuszka “NZ must target the top products” *Manawatu Standard* (Palmerston North, 18 March 2017).

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

“Gujarat Police Tests Facial Recognition System To Track Missing Offenders” *NDTV* (online ed, India, 15 August 2020).

Fiona Hamilton “Police facial recognition robot identifies anger and distress” *The Times* (online ed, United Kingdom, 15 August 2020).

Alex Hern “Hacker fakes German minister’s fingerprints using photos of her hands” *The Guardian* (online ed, United Kingdom, 30 December 2020).

Kashmir Hill “The Secretive Company That Might End Privacy as We Know It” *The New York Times* (online ed, New York, 18 January 2020).

Kashmir Hill “Twitter tells facial recognition trailblazer to stop using site’s photos” *New Zealand Herald* (online ed, New Zealand, 24 January 2020).

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

Kashmir Hill "Activists Turn Facial Recognition Tools Against the Police" *The New York Times* (online ed, New York, 21 October 2020).

Afua Hirsch "The coronavirus pandemic threatens a crisis for human rights too" *The Guardian* (online ed, United Kingdom, 19 March 2020).

Connor Hoffman "State Sentate to vote on facial recognition moratorium bill" *Niagra Gazette* (online ed, Niagra Falls, 21 July 2020).

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

Tom Hunt "Police eyeing up newer, smarter CCTV facial recognition technology" *Stuff* (online ed, New Zealand, 18 April 2018).

Mary Ilyushina "How Russia is using authoritarian tech to curb coronavirus" *CNN* (online ed, United States, 29 March 2020).

Lucy Ingham "Coronavirus-fighting smart bus rolled out in China" *Verdict* (online ed, United Kingdom, 31 March 2020).

Nicolas Jackson "Facebook will start using facial recognition next week" *The Atlantic* (online ed, United States, 16 December 2010).

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

Rozi Jones "SmartSearch launches facial recognition feature" *Financial Reporter* (online ed, United Kingdom, 5 May 2020).

Binoy Kampmark "The Pandemic Surveillance State" *The Scoop* (online ed, New Zealand, 22 March 2020).

Lily Kuo "'The new normal': China's excessive coronavirus public monitoring could be here to stay" *The Guardian* (online ed, Hong Kong, 9 March 2020).

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

Eliza Mackintosh "What you need to know about coronavirus on Monday, March 30" *CNN* (online ed, United States, 30 March 2020).

"Man kidnapped as toddler 32 years ago reunited with parents thanks to facial recognition" *New Zealand Herald* (online ed, New Zealand, 20 May 2020).

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

Tim McDonald "Singapore in world first for facial verification" *BBC News* (online ed, Singapore, 25 September 2020).

Luke McGee "Power-hungry leaders are itching to exploit the coronavirus crisis" *CNN* (online ed, United States, 1 April 2020).

John McKenzie "Groundbreaking facial recognition software under development in Dunedin – for sheep" *One News* (online ed, New Zealand, 9 July 2019).

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

Rebecca Moore "Two Auckland men pass police checkpoint to go to Hamilton casino amid Level 3 restrictions" *One News* (online ed, New Zealand, 17 August 2020).

Madhumita Murgia "London's King's Cross uses facial recognition in security cameras" *Financial Times* (online ed, London, 13 August 2019).

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

Anuradha Nagaraj "Indian police use facial recognition app to reunite families with lost children" *Reuters* (online ed, United States, 15 February 2020).

Matt O'Brien "Covid-19 coronavirus: Pandemic masks thwarting face recognition tech" *New Zealand Herald* (online ed, New Zealand, 28 July 2020).

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

"One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority" *The New York Times* (online ed, New York, 14 April 2019).

Kari Paul "'Ban this technology': students protest US universities' use of facial recognition" *The Guardian* (online edition, United Kingdom, 3 March 2020).

Phil Pennington "Police open to using facial recognition from Auckland Transport CCTV cameras" *RNZ* (online ed, New Zealand, 15 August 2019).

Phil Pennington "Police setting up $9m facial recognition system which can identify people from CCTV feed" *RNZ* (online ed, New Zealand, 31 August 2020).

Phil Pennington "Global facial recognition company working closely with NZ govt" *RNZ* (online ed, New Zealand, 19 August 2020).

Phil Pennington "Government facial recognition tech deal offers wide access" *RNZ* (online ed, New Zealand, 12 October 2020).

"Police ending Armed Response Teams after trial – Commissioner" *RNZ* (online ed, New Zealand, 9 June 2020).

"Police unlawfully retaining custody images, claims Norman Lamb" *BBC* (online ed, United Kingdom, 6 February 2018).

Stella Qiu and Ryan Woo "Chinese exam authorities use facial recognition, drones to catch cheats" *Reuters* (online ed, Bejing, 8 June 2017).

James Regan "New Zealand passport robot tells applicant of Asian descent to open eyes" *Reuters* (online ed, Sydney, 7 December 2016).

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

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

Mary-Ann Russon "30 churches around the world using facial recognition to track congregants that skip services" *International Business Times* (online ed, United States, 26 June 2015).

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

Dan Sabbagh "Regulator looking at use of facial recognition at King's Cross site" *The Guardian* (online ed, United Kingdom, 12 August 2019).

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

Jack Shenker "Cities after coronavirus: how Covid-19 could radically alter urban life" *The Guardian* (online ed, United Kingdom, 26 March 2020).

Sam Sherwood and Collette Devlin "Police Commissioner rules out bringing back Armed Response Teams" *Stuff* (online ed, New Zealand, 9 June 2020).

Tom Simonite "How Facial Recognition Is Fighting Child Sex Trafficking" *Wired* (online ed, United States, 19 June 2019).

Mackenzie Smith "Police trial of facial recognition technology 'a matter of concern' - Andrew Little" *RNZ* (online ed, New Zealand, 12 May 2020).

Mackenzie Smith "Police trialled facial recognition tech without clearance" *RNZ* (online ed, New Zealand, 13 May 2020).

Mackenzie Smith "Police searched for suspects in unapproved trial of facial recognition tech, Clearview AI" *RNZ* (online ed, New Zealand, 15 May 2020).

Mackenzie Smith "Police 'stocktake' surveillance tech after Clearview AI facial recognition trial" *RNZ* (online ed, New Zealand, 18 May 2020).

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

Heather Somerville "Facial-Recognition Startup Clearview Moves to Limit Risk of Police Abuse" *The Wall Street Journal* (online ed, New York, October 20 2020).

Katri Uibu "Poland is making its citizens use a 'selfie' app during the coronavirus crisis" *ABC News* (online ed, Australia, 25 April 2020).

Abraham Vass "CCTV: Is it Big Brother or the Eye of Providence?" *Hungary Today* (online ed, Hungary, 18 January 2019).

Abraham Vass "Police to Use Facial Recognition From Now On" *Hungary Today* (online ed, Hungary, 11 December 2019).

Elias Visontay "Councils tracking our faces on the sly" The Australian (online ed, Canberra, 29 August 2019).

Oliver Wainwright "10 Covid-busting designs: spraying drones, fever helmets and anti-virus snoods" *The Guardian* (online ed, United Kingdom, 25 March 2020).

Jane Wakefield "Coronavirus: NHS app paves the way for 'immunity passports'" *BBC* (online ed, United Kingdom, 26 May 2020).

Shaun Walker "Authoritarian leaders may use Covid-19 crisis to tighten their grip" *The Guardian* (online ed, United Kingdom, 31 March 2020).

Yingzhi Yang and Julie Zhu "Coronavirus brings China's surveillance state out of the shadows" *Reuters* (online ed, United States, 8 February 2020).

8.7 INTERNET MATERIALS

Apple "Use Face ID on your iPhone or iPad Pro" (20 May 2020) www.support.apple.com.

"About TELEFI Project" TELEFI Project www.telefi-project.eu.

"Algorithm charter for Aotearoa New Zealand" (July 2020) data.govt.nz www.data.govt.nz.

Artificial Intelligence Research "Facial recognition for conservation" (17 July 2017) www.onartificialintelligence.com.

Australian Government: Department of Industry, Science, Energy and Resources "AI Ethics Principles" www.industry.gov.au.

Australian National University "Surveillance, public health ethics and trust in a time of corona" (4 June 2020) www.crawford.au.edu.au.

"Automated facial recognition" (10 September 2019) GOV.UK www.gov.uk.

Marcin Betkier "Clearview AI exposes our regulatory shortcomings" (28 *February* 2020) Privacy Foundation www.privacyfoundation.nz.

"Biometrics and Forensics Ethics Group: About Us" GOV.UK www.gov.uk.

BNZ "Help & Support - Mobile Touch ID, Fingerprint Login and Face ID" www.bnz.co.nz.

Russell Brandom "Why Facebook is beating the FBI at facial recognition" (7 July 2014) The Verge www.theverge.com.

Joy Buolamwini "Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces" (25 January 2019) Medium www.medium.com.

Chris Burt "Heathrow curb-to-gate biometrics said to be world's biggest single deployment" (29 April 2019) Biometric Update www.biometricupdate.com.

Chris Burt "NEC to provide curb-to-gate facial biometrics for Star Alliance frequent flyers" (26 July 2019) Biometric Update www.biometricupdate.com.

Chris Burt "Morocco places moratorium on facial recognition, California limits police use" (12 September 2019) Biometric Update www.biometricupdate.com.

Chris Burt "Biometric checks and facial recognition payments to support social distancing, fight spread of covid-19" (23 March 2020) Biometric Update www.biometricupdate.com.

Chris Burt "Morocco extends facial recognition moratorium to year-end, proposes biometric authentication service" (9 April 2020) Biometric Update www.biometricupdate.com.

Andrew Butler and Geoffrey Palmer "The Proposed Constitution" (2016) Constitution Aotearoa NZ: 2017 Archive www.archive.constitutionaotearoa.org.nz.

City of Melbourne "Safe City cameras" www.melbourne.vic.gov.au.

The Co-operative Bank "Terms and Conditions for our Digital Services" www.co-operativebank.co.nz.

Jared Council "Massachusetts Senate Passes Bill That Would Halt Police Use of Facial Recognition" (14 July 2020) WSJ Pro Artificial Intelligence www.wsj.com.

Data.govt.nz "Data Ethics Advisory Group" www.data.govt.nz.

Digital Rights Watch "Blog: Police drones and coronavirus surveillance" (27 August 2020) www.digitalrightswatch.org.au.

European Commission "Smart lie-detection system to tighten EU's busy borders" (24 October 2018) www.ec.europa.eu.

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

"Forensic Science Regulator" GOV.UK www.govt.uk.

"FRVT Quality Assessment" NIST www.pages.nist.gov/frvt/html/frvt-quality.html.

Future Travel Experience "Automated Border Control: Facilitation vs Security?" (April 2011) www.futuretravelexperience.com

Clare Garvie "Garbage In, Garbage Out: Face Recognition on Flawed Data" (16 May 2019) Flawed Face Data www.flawedfacedata.com.

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

Government of Canada "Algorithmic Impact Assessment (AIA)" (28 July 2020) www.canada.ca.

Government of Canada "Responsible use of artificial intelligence (AI)" www.canada.ca.

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

Karen Hao "Live facial recognition is tracking kids suspected of being criminals" (9 October 2020) MIT Technology Review www.technologyreview.com.

Laura Hautala "UCLA cancels on-campus facial recognition program after backlash" (19 February 2020) CNET www.cnet.com.

Heartland Bank "Biometrics" www.heartland.co.nz.

"How Clearview AI Works" www.clearview.ai.

Darren Hopper "Facial Recognition – The future of Payments?" (9 April 2019) Paymark www.paymark.co.nz.

Human Rights Commission "How to make a complaint" www.hrc.co.nz.

IBM "IBM CEO's Letter to Congress on Racial Justice Reform" (8 June 2020) www.ibm.com.

"Identity Verification Service Privacy Statement" (20 July 2020) RealMe www.realme.govt.nz.

Information Commissioner's Office "About the ICO" www.ico.org.uk.

Information Commissioner's Office "Data protection impact assessments" (24 June 2019) www.ico.org.uk.

IPVM "UK Facewatch GDPR Compliance Questioned" (27 August 2019) www.ipvm.com.

Tom Kelly "Facebook Can Now Find Your Face, Even When It's Not Tagged" (19 December 2017) Wired www.wired.com.

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

Dev Kundaliya "After IBM and Amazon, Microsoft bans facial recognition sales to police" (12 June 2020) Computing www.computing.co.nz.

Metropolitan Police "Live Facial Recognition" www.met.police.uk.

Girish Nazhiyath "Looking Customer Loyalty Right in the Face" (2 January 2018) NEC Today www.nectoday.com.

NEC "Facial Recognition in 2020 – 8 trends to watch out for" (25 November 2019) www.nec.co.nz.

NEC "NEC New Zealand, providing smart city solutions to the Wellington City Council to create smart city" www.nec.com.

New Zealand Customs Service "Customs confirms changes after eGate system review" (11 April 2019) www.beehive.govt.nz.

New Zealand Immigration "Biometric information" www.immigration.govt.nz.

Alfred Ng "How China uses facial recognition to control human behavior" (11 August 2020) CNET www.cnet.com.

Office of the Australian Information Commissioner "Guide to undertaking privacy impact assessments" www.oaic.gov.au.

"Office of the Biometrics Commissioner: About Us" GOV.UK www.gov.uk.

Office of the Privacy Commissioner "Can I use facial recognition technology?" www.privacy.org.nz.

Office of the Privacy Commissioner "Information matching provisions" www.privacy.org.nz.

Office of the Privacy Commissioner of Canada "Privacy Impact Assessments (PIAs)" www.priv.gc.ca

Office of the Privacy Commissioner "Privacy Impact Assessment Handbook" www.privacy.org.nz.

OriginID "APLY ID: A SaaS solution for AML compliance" www.originid.co.nz/aplyid.

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

Parliament of Australia "Review of the Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018: Submissions received by the Committee" www.aph.gov.au.

Parliament of Australia "Review of Identity-Matching Services Bill 2019 and the Australian Passport Amendment (Identity-matching Services) Bill 2019" www.aph.gov.au.

Luana Pascu "EU considers 5-year facial recognition ban for public spaces" (17 January 2020) Biometric Update www.biometricupdate.com.

Luana Pascu "EU no longer considering facial recognition ban in public spaces" (30 January 2020) Biometric Update www.biometricupdate.com.

Luana Pascu "Apple patents potential new Face ID biometrics system, to launch face recognition to iMac" (17 June 2020) Biometric Update www.biometricupdate.com.

J Purshouse "Facial Recognition Technology, the Metropolitan Police and the Law" (19 January 2020) Policing Law Blog www.policing.law.blog.

Qantas "Facial Recognition" www.qantas.com.

Ramco "Ramco Systems drives Payroll modernization across Australia & New Zealand" (April 2019) www.ramco.com.

Reveal "Customer Engagement Systems" www.reveal.co.nz.

Roy Morgan "Australians not concerned about use of mass facial recognition technology" (10 October 2017) www.roymorgan.com.

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

Brad Smith "Facial recognition: It's time for action" (6 December 2018) Microsoft blogs.microsoft.com.

Aaron Smith "More than half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly" (5 September 2019) Pew Research Center www.pewresearch.org.

Trey Smith "In Hong Kong, Protesters Fight to Stay Anonymous" (22 October 2019) The Verge www.theverge.com.

South Wales Police "South Wales Police trial new facial recognition app on officer's mobile phones" (8 August 2019) www.south-wales.police.uk.

Te Tari Taiwhenua: Department of Internal Affairs "Organisations approved to use Confirmation Service" www.dia.govt.nz.

Danny Thakkar "Smart Gates on Autopilot" Bayometric www.bayometric.com.

Peter Trepp "How Face Recognition Evolved Using Artificial Intelligence" FaceFirst www.facefirst.com.

University of Waikato "RFI - Smart Systems Development & Integration - CCTV Surveillance Systems" (17 January 2020) Government Electronic Tender Service www.gets.govt.nz.

Maya Wang "China: Fighting COVID-19 With Automated Tyranny" (1 April 2020) Human Rights Watch www.hrw.org.

"We are implementing a one-year moratorium on police use of Rekognition" (10 June 2020) The Amazon blog blog.aboutamazon.com.

Darrell M West "Brookings survey finds 50 percent of people are unfavorable to facial recognition software in retail stores to prevent theft" (8 October 2018) Brookings www.brookings.edu.

Jesse Davis West "3 Ways Future Stores Will Use Face Recognition for Retail" (2019) FaceFirst www.facefirst.com.

Westpac "Westpac EasyID" www.westpac.co.nz.

"Where to use RealMe®" RealMe www.realme.govt.nz.

Michael Whitener and Raquel Aragon "How should we regulate facial-recognition technology?" (29 January 2019) IAPP www.iapp.org.

Kelly Yamanouchi "Privacy Advocates Raise Concerns as Delta Airlines Expands Use of Facial Scanning at Atlanta International Airport" (19 September 2019) Governing www.governing.com.

8.8 OTHER RESOURCES

Asia Corporate News Network - ACN Newswire "The Ramco Innovation Lab Singapore Demos Touch-less Attendance System With Thermal Scan" (press release, 19 March 2020).

Chief Executive of the Department of Internal Affairs and Enterprise Services New Zealand *Master Syndicated Agreement: relating to the syndicated procurement of Facial Recognition Services* (14 December 2018).

Grab "Grab partners with Ministry of Transport to implement facial recognition technology in Malaysia" (press release, 11 April 2019).

The Hamburg Commissioner for Data Protection and Freedom of Information "Hamburg Police deletes the biometric database for facial recognition created in the course of the G20 investigations" (press release, 28 May 2020).

Koen Lenaerts, President European Court of Justice "Accountability in a digitalised world: the Court's role in enhancing data protection in the European Union" (speech to the General Data Protection Regulation five months on – 40th International Conference of Data Protection and Privacy Commissioners, 25 October 2018).

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

NEC New Zealand "Kiwi Developers And Global Technology Leader NEC Team Up To Fight Spread Of COVID-19" (press release, 26 March 2020).

New Zealand Customs Service "Record summer passenger numbers" (press release, 31 March 2016).

New Zealand Police *Request for Proposals ABIS 2 (Automated Biometric Identification Solution)* (TN 18/03, RFP released 15 January 2018).

New Zealand Police "Improvements to information sharing between DIA, the Registrar-General, Births, Deaths and Marriage and Police" (press release, 3 May 2019).

Portland.gov "City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces" (press release, 9 September 2020).

Prime Minister of Australia "Digital Business Plan to Drive Australia's Economic Recovery" (press release, 29 September 2020).

RealAML "RealAML Launches Industry-first Facial Recognition" (press release, 16 July 2020).

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

Stats NZ *Algorithm Charter for Aotearoa New Zealand* (July 2020).

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

FACIAL RECOGNITION TECHNOLOGY IN NEW ZEALAND

TOWARDS A LEGAL AND ETHICAL FRAMEWORK

The Law Foundation NEW ZEALAND
SUPPORTING INDEPENDENT LEGAL THINKING.