18

Principled Regulation of Facial Recognition Technology

A View from Australia and New Zealand

Nessa Lynch and Liz Campbell

18.1 INTRODUCTION

Scholarly treatment of facial recognition technology (FRT) has focussed on human rights impacts,[1] with frequent calls for the prohibition of the technology.[2] While acknowledging the potentially detrimental and discriminatory uses that FRT use by the state has, this chapter seeks to advance discussion on what principled regulation of FRT might look like. It should be possible to prohibit or regulate unacceptable usage while retaining less hazardous uses.[3] In this chapter, we reflect on the principled use and regulation of FRT in the public sector, with a focus on Australia and Aotearoa New Zealand. We draw on our experiences as researchers in this area and from our professional involvement in oversight and regulatory mechanisms in these jurisdictions and elsewhere. Both countries have seen significant growth in the use of FRT, but regulation remains patchwork. In comparison with other jurisdictions, human rights protections and avenues for individual citizens to complain and seek redress remain insufficient in Australia and New Zealand.

A note on scope and terminology. In this chapter we concentrate on FRT use by the state or public sector – by which we mean government, police, and security use. Regulation of private sector use is a wider issue that is outside the scope of this chapter.

[1] Joe Purshouse and Liz Campbell, 'Privacy, crime control and police use of automated facial recognition technology' (2019) 3 *Criminal Law Review* 188–204.

[2] Lindsey Barret, 'Ban facial recognition technologies for children-and for everyone else' (2020) 26 *BUJ Sci. & Tech. L.* 223–286

[3] Nessa Lynch, 'Beyond the ban – Principled regulation of facial recognition technology' in Kelly Pendergast and Anna Pendergast (eds.), *More Zeros and Ones: Digital Technology, Maintenance and Equity in Aotearoa New Zealand* (Bridget Williams Books, 2022), pp. 121–182.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

18.2 CONTEXT

18.2.1 *What Is FRT?*

FRT is a term used to describe a range of technologies involving processing of a person's facial image.[4] A facial image is a biometric that means a biological measurement or characteristic that can be used to identify an individual person. Though it may be collected from a distance, in public, and without the person's knowledge or consent, it remains an intrusion on the individual's privacy.[5] FRT may enhance and speed up existing human capabilities (such as finding an individual person in video footage) or create new capabilities (such as purporting to detect emotional states of people in crowds).

18.2.2 *Contemporary Usage in the Public Sector in Australia and New Zealand Jurisdictions*

FRT is a fast-growing technology, and it has many uses and potential uses in the public sector. In previous joint work we have canvassed the many usages of FRT across various sectors in New Zealand,[6] and discussed uses and potential uses in policing internationally and in New Zealand.[7] It is not possible here to review these uses in detail, but the main use-cases will be discussed briefly now.

First, the use of FRT is established in border security and immigration – the Smart Gate system widely in use at the Australian and New Zealand borders. The Australian Electronic Travel Authority may now be obtained by means of an app, using FRT. These use-cases are in the 'verification' category principally – comparing an individual's biometric template with another, but 'identification' (one to many) use-cases are also apparent.[8] Biometric data (including facial images) may be used to make or guide decisions.[9] Detection of identity fraud is the principal use-case.

Second, there is security usage by central government, local government, and policing authorities in camera networks in public spaces. For instance, police and councils in Perth and Melbourne use FRT to identify particular individuals,[10]

[4] Nessa Lynch and Andrew Chen, 'Facial recognition technology – Considerations for use in policing' (December 2021), New Zealand Police.

[5] Purshouse and Campbell, 'Privacy, crime control and police use'.

[6] Nessa Lynch, Liz Campbell, Joe Purshouse, and Marcin Betkier, 'Facial recognition technology in New Zealand: Towards a legal and ethical framework' (December 2020), The Law Foundation of New Zealand.

[7] Lynch and Chen, 'Facial recognition technology'.

[8] For example, in passport fraud detection. See Lynch et al., 'Facial recognition technology in New Zealand'.

[9] Immigration Act 2009 (NZ) s. 30.

[10] City of Melbourne, 'Safe city cameras' (n.d.), www.melbourne.vic.gov.au/community/safety-emergency/pages/safe-city-cameras.aspx; Elias Visontay, 'Councils tracking our faces on the sly' (29 August 2019), *The Australian*, www.theaustralian.com.au/nation/councils-tracking-our-faces-on-the-sly/news-story/eea2b51fa82b076796ad7e294e111d3e.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

and Adelaide is proposing to use FRT through its closed-circuit television (CCTV) network.[11]

Thirdly, FRT technology may be used in policing. In Lynch and Chen's independent review of New Zealand Police's use and potential use of FRT, it was found that current or imminent planned use of FRT by New Zealand Police was limited and relatively low risk, including authentication for access to devices such as iPhones, identity matching, and retrospective analysis of lawfully acquired footage in limited situations. There was no evidence that the police are using or formally planning the use of live automated FRT. By contrast, police forces across Australia use live FRT as a means of preventing and investigating crime.[12] Facial images may also be submitted manually by a specified list of law enforcement, anti-corruption, and security agencies to the federal Identity Matching Services for a 'Face Identification Service matching request'. This does not connect to live video feeds, such as CCTV, and is not available to private sector or local government authorities.[13]

Fourthly, digital identity face recognition can be used to access certain government services online.[14] For instance, in Australia, signing into the MyGov account to access government services can be through FRT.

18.2.3 *A Spectrum of Impact on Individual and Collective Rights*

The variety of use-cases for FRT means a spectrum of impact on individual and societal rights and interests. As we expand on through case-studies, FRT can impact rights and interests such as privacy (both individual and collective), freedom of association, lawful protest, freedom from discrimination, and fair trial rights.[15]

As discussed earlier, it is vital to note that FRT has a range of use cases, ranging from consensual one-on-one identity verification (e.g., at the border) to widespread and intrusive live biometric tracking in public spaces. FRT technologies can have many legitimate and socially acceptable uses, including speed and scale improvements in processing evidential footage, identity matching, security and entry

[11] Erik Tlozek, 'SA Police could use Adelaide City facial recognition technology, despite being asked not to' (20 June 2022), *ABC News*, www.abc.net.au/news/2022-06-20/sa-police-could-use-adelaide-city-facial-recognition-technology/101166064

[12] See NT Police, Fire and Emergency Services, 'Success for Northern Territory Police at IAwards' (20 June 2016), Media release, https://pfes.nt.gov.au/newsroom/2016/success-northern-territory-police-iawards; NSW Government, 'NSW Police Force and facial recognition' (2022) www.police.nsw.gov.au/crime/terrorism/terrorism_categories/facial_recognition.

[13] Australian Government, 'ID match' (2022), www.idmatch.gov.au.

[14] Judy Skatssoon, '600k MyGov accounts now connected to digital ID' (24 October 2021), *Government News*, www.governmentnews.com.au/600k-mygov-accounts-now-connected-to-digital-id/

[15] Bethan Davies, Martin Innes, and Andrew Dawson, 'An evaluation of South Wales Police's use of automated facial recognition' (September 2018), Report, Universities' Police Science Institute and Crime & Security Research Institute, Cardiff University; Suzanne Shale, Deborah Bowman, Priyah Singh, and Leif Wenar, 'London Policing Ethics Panel: Final report on live facial recognition' (May 2019), London Policing Ethics Panel, London.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

controls, and digital identity.[16] Factors such as who is operating the system, what the purposes are, whether there is independent authorisation or oversight, whether the person has consented to the collection and processing of their facial image, and whether the benefits are proportionate to the impacts are all relevant in considering the appropriate uses of FRT.[17]

18.2.4 *Case Studies of Human Rights Impact*

As an example of the rights and interests engaged by live automated FRT (AFR) in the context of a largely unregulated environment, there has been a legal challenge to police use in Wales. AFR is being deployed by police forces across England and Wales, with the Metropolitan Police and South Wales Police (SWP) among others trialling AFR for both live surveillance and identity verification.[18] As in Australia and New Zealand, the Westminster Parliament has not introduced any specific laws relating to AFR, but rather the police maintain that common law and human rights principles, the Data Protection Act 2018, and the Surveillance Camera Code of Practice provide a valid legal basis.

In the first ever legal challenge to the use of AFR, a Mr Bridges (described as a civil liberties campaigner) challenged the legality of SWP's general use and two particular deployments of AFR on the grounds that these were contrary to the Human Rights Act 1998, Data Protection legislation, and that the decision to implement was not taken in accordance with the Equality Act 2010.[19] The Divisional Court rejected this application.

On appeal, the Court of Appeal ruled that the Divisional Court erred in its finding that the measures were 'in accordance with the law'. The court engaged in a holistic analysis of whether the framework governing the SWP's use of live AFR was reasonably accessible and predictable in its application,[20] and sufficient to guard against 'overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights'.[21] While the Court of Appeal rejected that statutory authorisation was needed, it accepted that AFR requires more safeguards than for overt photography.[22] The legal framework gave too much discretion to individual officers to determine who was on the watchlist, and where AFR could be deployed.[23]

[16] Lynch and Chen, 'Facial recognition technology'.

[17] Lynch et al., 'Facial recognition technology in New Zealand'; Lynch and Chen, 'Facial recognition technology'.

[18] Gareth Corfield, 'Tech firm used by Met and MoD forced to delete billions of Facebook photos' (23 May 2022), *The Telegraph*; Home Office UK, 'Police transformation fund: Successful bids 2016 to 2017' (4 September 2017), www.gov.uk/government/publications/police-transformation-fund-successful-bids-2016-to-2017

[19] *R (Bridges)* v. *The Chief Constable of South Wales* [2019] EWHC 2341 (Admin).

[20] Here, *R (Catt)* v. *Association of Chief Police Officers* [2015] UKSC 9 at [11]–[14] per Lord Sumption was cited with approval.

[21] *Beghal* v. *Director of Public Prosecutions* [2016] AC 88 at [31] and [32] per Lord Hughes.

[22] *R (Bridges)* v. *The Chief Constable of South Wales*, [85]–[90].

[23] Ibid., [96].

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

Moreover, the Court of Appeal held that the SWP never had due regard to the need to eliminate discrimination on the basis of sex and race.[24]

That said, the Appeal Court held that the SWP's use of AFR was a proportionate interference with the European Court of Human Rights Article 8 right to privacy and family life, and as such was 'necessary' and 'in pursuit of a legitimate aim' under Article 8(2).

South Wales Police indicated that it would not appeal the Court of Appeal's decision: 'There is nothing in the Court of Appeal judgment that fundamentally undermines the use of facial recognition to protect the public. This judgment will only strengthen the work which is already underway to ensure that the operational policies we have in place can withstand robust legal challenge and public scrutiny.'[25]

In this region, a key illustration of the impacts on privacy concerns is the use by Australian police of Clearview AI's facial recognition software.[26] Though there has not been a legal challenge in the courts here, the Office of the Australian Information Commissioner (OAIC) has investigated and made findings as to the use of this software. Clearview AI's technology operates by harvesting images from publicly available web sources and offering its technologies to government and law enforcement agencies.[27] From October 2019 until March 2020, Clearview AI offered free trials to the Australian Federal Police, Victoria Police, Queensland Police Service, and South Australia Police.[28] This revelation about its use was despite initial police denials.[29]

In November 2021, following a joint investigation with the United Kingdom's Information Commissioner's Office, the OAIC found that Clearview AI breached Australia's privacy laws through its practice of harvesting biometric information from the web and disclosing it though a facial recognition tool. In a summary

[24] Ibid., [199]. See Joy Buolamwini and Timnit Gebru, 'Gender shades: intersectional accuracy disparities in commercial gender classification' *Conference on Fairness, Accountability, and Transparency*, New York (February 2018); Joy Buolamwini, 'Response: Racial and gender bias in Amazon Rekognition – Commercial AI system for analyzing faces' (25 January 2019), *Medium*, https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

[25] South Wales Police, 'Response to the Court of Appeal judgment on the use of facial recognition technology', South Wales Police, Media release (11 August 2020), www.south-wales.police.uk/en/newsroom/response-to-the-court-of-appeal-judgment-on-the-use-of-facial-recognition-technology/

[26] Stephanie Palmer-Derrien, 'Aussie entrepreneur launches "disturbing and unethical" facial recognition tech in Silicon Valley' (22 January 2020), *Smart Company*, www.smartcompany.com.au/startupsmart/news/aussie-clearview-ai/.

[27] Hannah Ryan, 'Australian Police have run hundreds of searches on Clearview AI's facial recognition tool' (28 February 2020), *BuzzFeed News*, www.buzzfeed.com/hannahryan/clearview-ai-australia-police.

[28] *Commissioner Initiated Investigation into Clearview AI, Inc. (Privacy)* [2021] AICmr 54 (14 October 2021) [8].

[29] Jake Goldenfein, 'Australian police are using the Clearview AI facial recognition system with no accountability' (4 March 2020), *The Conversation*, https://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

released with the OAIC's formal determination, the OAIC found that Clearview AI breached the Privacy Act 1988 (Cth) by:

- collecting Australians' sensitive information without consent;
- collecting personal information by unfair means;
- not taking reasonable steps to notify individuals of the collection of personal information;
- not taking reasonable steps to ensure that personal information it disclosed was accurate, having regard to the purpose of disclosure;
- not taking reasonable steps to implement practices, procedures, and systems to ensure compliance with the Australian Privacy Principles.[30]

Following the investigation, Clearview AI blocked all requests for user accounts from Australia, and there is no evidence of Australian users of the technology since March 2020.[31] Further, the OAIC required that all scraped images and related content be destroyed as they breached the Privacy Act.[32] Subsequently, the OAIC determined that the Australian Federal Police failed to comply with its privacy obligations in using the Clearview AI facial recognition tool, and instructed the AFP to review and improve its practices, procedures, systems, and training in relation to privacy assessments.[33]

18.3 OPTIONS FOR PRINCIPLED REGULATION

Despite the considerable impact on individual and collective rights and interests, there is no discrete law governing the use of FRT in either Australia or New Zealand. Patently, FRT can be subject to existing legislative regimes such as privacy and search and surveillance, but unlike other forms of biometrics, such as fingerprints and DNA, the collection and processing of facial images remains largely unregulated.

In this section we canvass various options for principled regulation of FRT, at state and international level, with different degrees of specificity and latitude. These include proposals for domestic legislation, a case study of cross-national regulation, state-level principles, and self-governance.

18.3.1 *Domestic Legislation*

We favour the introduction of specific and tailored legislative provisions with an associated code of conduct to regulate the use of FRT by public entities. In March

[30] Office of the Australian Information Commission (OAIC), 'Clearview AI breached Australians' privacy', OAIC Media Release (2 November 2021), www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy. See further, *Commissioner Initiated Investigation into Clearview AI, Inc.*

[31] *Commissioner Initiated Investigation into Clearview AI, Inc.*, at [239].

[32] Ibid., at [242].

[33] Office of the Australian Information Commissioner (OAIC), 'AFP ordered to strengthen privacy governance' (16 December 2021), www.oaic.gov.au/updates/news-and-media/afp-ordered-to-strengthen-privacy-governance.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

2021, the Australian Human Rights Commission (AHRC) released its report *Human Rights and Technology*, which assesses the impact of FRT and biometric technology and makes the case for regulation.[34] The report recognises the potential human rights impacts arising from the use of these technologies, including most obviously to the right to privacy.[35] To guard against this, the AHRC recommends that commonwealth, state, and territory governments should:

> Introduce legislation that regulates the use of facial recognition and other biometric technology. The legislation should:
>
> (a) expressly protect human rights
> (b) apply to the use of this technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement
> (c) be developed through in-depth consultation with the community, industry and expert bodies such as the Australian Human Rights Commission and the Office of the Australian Information Commissioner.[36]

Until such reforms can be enacted, the AHRC recommends a moratorium on the use of facial recognition and biometric technologies that would fit within para. (a) above.[37]

In September 2022, the newly formed Human Technology Institute based at the University of Technology Sydney released a report.[38] This proposes reform to existing regulation around FRT and outlines a Model Law 'to foster innovation and enable the responsible use of FRT, while protecting against the risks posed to human rights'.[39] While the report recognises that FRT can be used consistently with international human rights law, 'FRT necessarily also engages, and often limits or restricts, a range of human rights'.[40]

Reform to existing law dealing indirectly with FRT in Australia is needed because of the rapid development and deployment of FRT which can extract, store, and process a vast amount of information. Australia has existing laws that apply to the deployment and use of FRT, including privacy laws that regulate the handling of biometric information, but 'on the whole, these existing laws are inadequate in addressing many of the risks associated with FRT'.[41]

[34] Australian Human Rights Commission (AHRC), 'Human rights and technology' (March 2021), Final report, p. 9.
[35] Ibid., pp. 114–116.
[36] Ibid., p. 116.
[37] Ibid.
[38] Nicholas Davis, Lauren Perry, and Edward Santow, 'Facial recognition technology: Towards a model law' (September 2022), Report, Human Technology Institute, University of Technology Sydney, September. One of the report's authors, Professor Edward Santow, is the former Australian Human Rights Commissioner and worked on the AHRC's report just discussed.
[39] Ibid., p. 7.
[40] Ibid.
[41] Ibid., p. 8.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

The report sets out the following purposes of the Model Law:

- Uphold human rights
- Apply a risk-based approach
- Support compliance
- Transparency in the use of FRT
- Effective oversight and regulation
- Accountability and redress
- Jurisdictional compatibility.[42]

The human rights risks of FRT are discussed in Section 31–2, including infringements on the right to privacy and intrusion into private life. Other concerns are raised in relation to rights to equality and non-discrimination, and here the report authors note the *Bridges* case and the acknowledged discriminatory impact of FRT through inherently discriminatory algorithms. The potential of FRT to interfere with the right not to be subject to arbitrary arrest or detention and the rights to equality before the law and to a fair trial are also considered.

The Model Law includes specific legal requirements for the deployment of FRT, including compliance with specific technical standards,[43] and specific privacy law requirements.[44] Importantly, the Model Law also contemplates assigning regulatory oversight to a body that has human rights expertise, specifically expertise in privacy rights. The report suggests that potential regulators could be the OAIC or the AHRC, but notes that whatever regulatory body is given regulatory responsibility it must be provided with necessary financial and other resources to fulfil its role adequately in a sustainable long-term way.[45]

The risks of a legislative gap are clear. Indeed, ClubsNSW (the representative body for registered clubs in New South Wales, NSW) announced its intention to proceed with the roll-out of FRT in all NSW pubs and clubs (it is already being used at about a hundred licensed venues) after the NSW government announced that it would not proceed with law reform on the regulation of FRT.[46]

18.3.2 *State-Level Principles and Guidance*

In the absence of legislation, many jurisdictions worldwide have established state level principles and guidance to regulate algorithm and data driven technologies such as FRT. New Zealand is the first country to establish standards for algorithm

[42] Ibid., p. 13.
[43] Ibid., p. 65.
[44] Ibid., pp. 67–68.
[45] Ibid., p. 80.
[46] Tasmin Rose, 'Clubs likely to proceed with facial recognition after NSW Government shelves reform bill' (2 November 2022), *The Guardian Australia*, www.theguardian.com/australia-news/2022/nov/02/clubs-likely-to-proceed-with-facial-recognition-after-nsw-government-shelves-reform-bill.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

usage by government and public sector agencies.[47] The Algorithm Charter sets principles for public sector agencies using algorithms to make or guide decisions to which agencies can commit publicly. The term 'algorithm' is undefined, with a focus on the impact of the decision made using the algorithm rather than the complexity of the algorithm itself.

The Algorithm Charter requires transparency in algorithm use, respect for the Treaty partnership (with the Indigenous people of Aotearoa New Zealand), a focus on people, use of data that is fit for purpose, safeguarding privacy, human rights and ethics, and retention of oversight by human operators.[48] Also in New Zealand, the Government Chief Data Steward and the Privacy Commissioner have jointly issued guidelines for public sector use of data and analytics, with similar emphasis on transparency, societal benefit, retaining human oversight, and focussing on people:[49]

Principles and guidance of this nature are useful in setting high level expectations and entrenching fundamental values, but lack any regulatory enforcement mechanism. Unlike legislation, they cannot be used to respond to individual breaches of rights or provide an objective mechanism for redress.

18.3.3 *Cross-National Standards*

The Artificial Intelligence Act (AI Act) is a nearly-finalised European Union law that will introduce a common regulatory and legal framework for AI across all sectors (excluding the military) and all types of AI.[50] This is important because, like the General Data Protection Regulation (GDPR), the AI Act will have extra-territorial effect and immense influence on national laws, given the extent of the EU market. Technology suppliers are likely to align product design with these regulations even in non-EU countries. It seeks to so do through 'a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market'.[51]

AI is defined in the proposed AI Act in a two-stage model. First, it is defined in Article 3 somewhat generally by reference to the concept 'artificial intelligence system', which is 'software that is developed with one or more of the techniques and

[47] Charlotte Graham-McLay, 'New Zealand claims world first in setting standards for government use of algorithms' (28 July 2020), *The Guardian*, www.theguardian.com/world/2020/jul/28/new-zealand-claims-world-first-in-setting-standards-for-government-use-of-algorithms.

[48] Algorithm Charter for Aotearoa New Zealand (2020), https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/.

[49] Privacy Commissioner and the Government Chief Data Steward, 'Principles for the safe and effective use of data and analytics' (16 May 2018), www.privacy.org.nz/publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/

[50] Proposal for Artificial Intelligence Act (European Commission, 2021/0106 (COD)).

[51] Ibid.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions influencing the environments they interact with'. Annex I lists the techniques as:

- machine learning approaches, including learning supervised, unsupervised, and by reinforcement, using a wide variety of methods, including deep learning;
- approaches based on logic and knowledge, namely knowledge representation, inductive (logic) programming, knowledge bases, inferences and deduction engines, reasoning systems (symbolic), and expert systems; and
- statistical approaches, Bayes estimation, research and optimisation methods.

Regulation of AI technologies under the proposed Act are based on a risk assessment model. This model is complex. Article 5(1)(d) bans 'real-time remote biometric identification systems in publicly accessible spaces for law-enforcement purposes (and so would cover a *Bridges*-type scenario). However, the ban does not cover FRT used by law-enforcement that is not real-time, or that is used by other public or private entities but equally pose a threat to fundamental human rights.[52] Nevertheless, the majority of FRT is classified as a high-risk AI (save for emotional recognition systems), which is a classification updated in accordance with technological advances and takes into account not only the technology itself, but also the use to which that technology may be put.[53]

In a similar way to the GDPR, the proposed AI Act has a presumption prohibiting high-risk AI systems unless their use is subject to various requirements including a control and monitoring procedure and requirements to report serious incidents and malfunctions of these high-risk AI systems (Art. 6, Annex III). Conversely, those systems designated as being low-risk may be used without being subject to these requirements (Art. 52(2)).

A concern about the proposed AI Act in the EU is 'its silence on the right to take legal action against suppliers or users of AI systems for non-compliance with its rules'.[54] Other concerns have been raised about the potential for conflicts between bodies and institutions set up to regulate AI under the proposed law.[55] Concerns have also been raised about the broadness of the definition of AI in the proposed law, such that it does not account for combinations of algorithms and data and potentially covers software not generally considered AI.[56] These are fair criticisms.

Notwithstanding these concerns about the proposed AI Act, it has been argued that the AI Act will have international significance. Indeed, Dan Svantesson argues that the Act will first have an impact in Australia in the same way that the GDPR impacts cross-border data flows, with the likelihood being that it will become the

[52] Vera Lúca Raposo, 'Ex machina: Preliminary critical assessment of the European Draft Act on Artificial Intelligence' (2022) 30 *International Journal of Law and Information Technology* 88, 95.
[53] Ibid., p. 96.
[54] Ibid., p. 103.
[55] Ibid., p. 107.
[56] Ibid., p. 91.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

default international setting for dealing with AI given the size of the EU market.[57] Second, and perhaps more substantially, the AI Act may also apply indirectly to Australian actors who operate within the EU market, such as by providing AI systems.[58] Also important is the ability of the AI Act to be utilised in law reform in Australia and New Zealand as the basis for progressing towards an regional approach to the regulation of AI.[59]

At the time of writing, the AI Act has been voted on in the EU Parliament, and lawmakers are now conducting the negotiation to finalise the provisions of the new legislation, which could include revising definitions, revising the list of prohibited systems and the parameters of obligations on suppliers.[60]

On 12 May 2022, the European Data Protection Board adopted Guidelines 05/2022 on the use of FRT in the area of law enforcement (Guidelines 05/2022).[61] The Guidelines recognise that FRT 'may be used to automatically recognise individuals based on his/her face' and is 'often based on artificial intelligence such as machine learning technologies'.[62] For law enforcement agencies, Guidelines 05/2022 recognise that such technologies promise 'solutions to relatively new challenges such as investigations of big data, but also to known problems, in particular with regard to under-staffing and observation and search measures'.[63] The Guidelines recognise that the application of such technology by law enforcement agencies engages a number of human rights, including the right to respect for private and family life under Article 8 of the European Convention on Human Rights.[64] More broadly, the application of FRT by law enforcement will – and to some extend already does – have significant implications for individuals and groups of people, including minorities. The application of FRT is considerably prone to interfere with fundamental rights beyond the right to protection of personal data.[65]

Turning to the technology, the Guidelines differentiate FRT from biometric technology because the former technology can fulfil two distinct functions, namely: (1) the identification of a person in order to verify who that person claims to be (one-to-one verification); and (2) identification of a person among a group of individuals, in a specific area, image or database (one-to-many identification).[66] It is the unique

[57] Dan Svantesson, 'The European Union Artificial Intelligence Act: Potential implications for Australia' (2022) 47 *Alternative Law Journal* 4, 6.
[58] Ibid., pp. 6–8.
[59] Ibid., pp. 8–9.
[60] Tambiama Madiega, *Briefing: Artificial Intelligence Act* (2nd ed., European Parliamentary Research Service, 2023).
[61] Guidelines on the Use of Facial Recognition Technology in the Area of Law Enforcement, Guidelines No 05/2022 (European Data Protection Board, European Union, adopted 12 May 2022) (Guidelines 05/2022).
[62] Ibid., p. 6.
[63] Ibid., p. 6.
[64] Ibid., p. 2.
[65] Ibid.
[66] Ibid., p. 7.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

functions to which FRT can be put and the potential consequences of its use that justify special regulation.

The Guidelines next summarise the applicable legal framework as a guide 'for consideration when assessing future legislative and administrative measures as well as implementing existing legislation on a case-by-case basis that involve FRT'.[67]

The remainder of the Guidelines contains a number of annexes; these include Annex II (practical guidance for managing FRT projects in law enforcement agencies) and Annex III (practical examples). These form a potential starting point for the development of law enforcement agency guidelines, including of the kind contemplated by the English and Welsh Court of Appeal in *Bridges*.

18.3.4 *Self-Governance*

In the absence of legislative or robust state-level regulation, some state actors have moved to establish self-regulation. In New Zealand, trials of a FRT application (Clearview AI) by a section of New Zealand Police in 2020 sparked a review of the use of technology, owing to the adverse publicity generated and also the lack of any firm legislative or regulatory regime to govern its use.

Initial Guidelines for the trial of emerging technology were published in September 2020, and the Police Manual Chapter was published in July 2022.[68] New Zealand Police are now required to seek advice from senior management even when responding to an offer from a technology company and even when the new technology would only be explored in a non-operational test setting. Approval for any trial must go through a formal governance and risk assurance process. Submissions for approval are expected to consider ethical and legal considerations, including public expectations and legal obligations surrounding the right to privacy.

However, there is no reference in the guidelines to the principles of human rights (such as the right to be free from discrimination, freedom of expression, the right to peacefully protest).

In April 2023, New Zealand Police publicly released a stocktake list of technology capabilities. This is an extensive list that details all instances of technology capabilities – from routine business procedures to state-of-the-art technologies.[69]

Further, an independent review of FRT (carried out by one of the present authors with a co-author) investigated and reported on use and potential use of FRT within New Zealand Police and made ten recommendations, which were accepted by the

[67] Ibid., p. 11.

[68] New Zealand Police, 'Trial or adoption of new policing technology – Police Manual chapter' (July 2022), www.police.govt.nz/about-us/publication/trial-or-adoption-new-policing-technology-police-manual-chapter.

[69] New Zealand Police, 'NZ Police technology capabilities list' (April 2023), www.police.govt.nz/sites/default/files/publications/technology-capabilites-list.pdf.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

leadership.[70] This included a commitment to continue to pause any consideration of live automated FRT, ensure continuous governance and oversight of deployment of FRT, implement guidelines for access to a third party system, embed a culture of ethical use of data in the organisation, and implement a system for ongoing horizon scanning.

Again, in the absence of a state level regulatory mechanism, New Zealand Police has established an expert panel (composed of experts with expertise in technology, governance, assurance, criminal law, and Te Ao Māori). This panel's role is 'to provide advice and oversight from an ethical and policy perspective of emergent technologies'.[71]

In another example of self-regulation, Scotland has a moratorium on live AFR in policing. While Police Scotland's strategy document *Policing 2026* included a proposal to introduce AFR,[72] a Scottish parliamentary committee was critical of this owing to its discriminatory implications, lack of justification for its need, and its radical departure from the principle of policing by consent.[73] Police Scotland responded that the force was not using live FRT currently and that it would ensure safeguards were in place prior to doing so; it was agreed that the impact of its use should be fully understood before it was introduced.[74]

These decisions by police organisations to self-regulate the use of technology are probably driven as much by perceptions of social licence and public attitudes as principle. It demonstrates again that state-level regulation is required to provide an objective and transparent standard, with mechanisms for redress.

18.3.5 A *Robust Regulator*

Any regulation of FRT must be accompanied by a robust regulator.

A case study of a regulator in a comparable jurisdiction is the Biometrics Commissioner role in Scotland, who has established a Code of Practice for biometric data use (encompassing facial images) in policing. Scottish law defines biometric data as 'information about an individual's physical, biological, physiological or behavioural characteristics which is capable of being used, on its own or in combination with other information … to establish the identity of an individual'.[75]

[70] Lynch and Chen, 'Facial recognition technology'.

[71] New Zealand Police, 'Advisory panel on emergent technologies' (2022) www.police.govt.nz/about-us/programmes-and-initiatives/police-use-emergent-technologies/advisory-panel-emergent.

[72] Police Scotland and Scottish Police Authority, 'Policing 2026: Our 10-year strategy for policing in Scotland' (2017), Report.

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

[74] Letter from Assistant Chief Constable Duncan Sloan to Justice Sub-Committee Convener (8 April 2020).

[75] Scottish Biometrics Commissioner Act 2020, s 23(1) and (2).

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press

The purposes of the Scottish Biometrics Commissioner are to review law, policy, and practice relating to collection, retention, use, and disposal of biometric data by Police Scotland, keep the public informed and aware of powers and duties related to biometric data (e.g., how the powers are used and monitored, and how the public can challenge exercise of these powers), and monitor the impact of the Code of Practice and raise awareness of the Code.

As another example, the AHRC report cited earlier argues that the rise of AI technology (including FRT) provides an important moment to develop standards and apply regulation in a way that supports innovation while also addressing risk of human rights harm.[76] To this end, the AHRC recommends the establishment of an AI Safety Commission in Australia 'to support regulators, policy makers, government and business [to] apply laws and other standards in respect of AI-informed decision making'.[77]

18.4 CONCLUSION

While biometric technologies such as FRT have become more prevalent and more complex, and are being utilised in increasingly diverse situations, legislation, regulation, and frameworks to guide ethical use are less well developed.

This chapter has demonstrated how state agencies, particularly in policing and security services in New Zealand and Australia, have a broad discretion as to their use of FRT.

We suggest that FRT should be used only when predicated upon explicit statutory authorisation and following appropriate ethical review.[78]

Principled regulations should comprise a national statutory framework with a concomitant code of practice. Moreover, we recommend independent approval and oversight of the proportionality and necessity of operations. Jurisdictions should have a robust regulator, with the Scottish Biometrics Commissioner being a good example.

[76] AHRC, 'Human rights and technology', p. 127.

[77] Ibid.

[78] Cf. Biometrics and Forensics Ethics Group, 'Ethical issues arising from the police use of live facial recognition technology' (February 2019), where the pilot project had begun already.

https://doi.org/10.1017/9781009321211.021 Published online by Cambridge University Press