[redacted]
LAWS458
Word Count: 2808

Who Will Watch the Watchers?

Regulating Facial Recognition Technology in a Surveillance Society

---

It is difficult to pinpoint the moment that we became a surveillance society. The dawn of the millennium saw a period of rapid expansion in the use of surveillance technology, and these days the presence of camera surveillance in public spaces is the norm rather than the aberration. There has been a marked increase in the use of Facial Recognition Technology (FRT) in the past several decades, but its rapid rise has left regulators scrambling to keep pace.

FRT is an umbrella term used to describe a suite of applications that perform a specific task using a human face to verify or identify an individual.[1] FRT involves identification based on an analysis of facial features, and algorithmic comparison between features from stored images.[2] Despite promulgation of it in recent years, many countries do not have an express legislative framework for monitoring the regulation of FRT, including the United States, the United Kingdom and New Zealand. Though scope for FRT usage is broad, this essay will focus on issues of surveillance, data use, and the challenges regulators will face reconciling application of FRT with human rights.

I. Privacy

The most notable challenge facing regulators of FRT is ensuring sufficient protection is afforded to individual privacy. Automated FRT is already prolific, with use of automated control measures of biometric identifiers in banking, security and access contexts.[3] Biometric data is defined as personal data resulting from processing relating to the characteristics of a person and the unique identification of that person.[4] Despite the highly personal and private nature of biometric data, there is a dearth of legal provisions relating to the regulation of biometric data throughout the world.[5]

---

[1] Amnesty International, "Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance" (11 June 2020). https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/

[2] Nessa Lynch, Liz Campbell, Joe Purshouse and Marcin Betkier *Facial Recognition Technology in New Zealand: Towards an Ethical and Legal Framework* (November 2020) at 1.2.

[3] https://thespinoff.co.nz/society/25-08-2020/facial-recognition-technology-is-here-new-zealands-law-is-nowhere-near-ready/

[4] General Data Protection Regulation (GDPR) 2016 EU, art 4.

[5] ttps://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data

The most applicable existing regulation of FRT can be found in legislation relating to protection of privacy and personal data. In New Zealand, the Privacy Act 2002 regulates the collection, storage, use and disclosure of personal information by agencies.[6] Personal information means any information about an identifiable individual, and so all use of FRT must adhere to the Information Privacy Principles (IPPs) set out under s 22 of the Act. However, the Privacy Act offers one general level of protection to all personal information. A challenge facing regulators will be to ensure protection afforded to privacy is sufficient to cover the particularly intrusive nature of FRT data collection.

A. Ensuring Transparency and Accountability

Usage of FRT is subtle, and it is difficult for individuals when and where they are being subject to data collection. Usage is prolific, with surveillance and the use of FRT allowed in any public place in New Zealand provided there is a clearly defined and lawful purpose for it.[7] Under the Privacy Act, information must be collected directly from the individual concerned, and the agency must take reasonable steps to notify the individual of collection of the data.[8] But this carries caveats - notification is not mandatory where it is not reasonably practicable, or where non-compliance with notification requirements is necessary for the maintenance of the law or public interest.[9] Thus, the people we wish to be most transparent are shielded, as agencies like the police and the government collection of data is necessary for functioning in the public interest.

The European Union's General Data Protection Regulation (GDPR) places strong emphasis on the protection of personal data and transparency, creating special categories of sensitive personal data that are subject to higher protection levels, including biometrics.[10] The GDPR contains similar principles to the Privacy Act regarding the right of the data subject to be informed of collection, and art 9 prohibits processing of the special categories unless there is consent from the individual concerned. Consent is one of the best known legal 'tools' that enables individuals to exercise autonomy over their data is consent,[11] but is not always a viable tool as art 9 is also subject to the same caveats of allowing non-compliance where it is necessary for functions regarding to public interest.

Where guaranteeing full control of personal data is not possible, a regulatory strategy to increase transparency and accountability of FRT usage could be to mandate impact assessments before use. Under the GDPR, all data controllers processing biometric information must carry out a Data Protection Impact Assessment (DPIA). This is mandatory when using new technologies and particularly where data processing is "likely to result in a high risk to the rights and freedoms of natural persons."[12] A DPIA assesses the necessity and proportionality of the use of FRT in relation to the purposes of its use, considering and

---

[6] Privacy Act, s 4.
[7] Office of the Privacy Commissioner "Can I use facial recognition technology?" https://privacy.org.nz/tools/knowledge-base/view/485?t=120522_168918
[8] Privacy Act 2020, s 22 IPP3 cl 1.
[9] Section 22 IPP3 cl 4.
[10] GDPR, art 9.
[11] Lynch, Campbell, Purshouse and Betkier above n 2 at 5.4.
[12] Article 35.1.

weighing affected rights.[13] New Zealand has a similar framework in the form of the Privacy Impact Assessment (PIA). PIAs are not mandatory under the Privacy Act, but the Privacy Commissioner recommends any organisation commencing a new project or implementing new technologies to undertake one.[14] The Immigration Act 2009 is one of the few pieces of New Zealand legislation which refers to biometric information specifically, and mandates the completion of a PIA in relation to its collection and usage.[15]

In 2018, a man was mistakenly detained as a shoplifter at Dunedin Centre City New World. Although this particular misidentification was human error, the resulting investigation revealed that Foodstuffs had quietly rolled out FRT in many of their stores throughout the country.[16] FRT usage has crept silently in alongside other surveillance mechanisms, and although PIAs are useful, they satisfy the need for greater transparency surrounding FRT usage at ground level in relation to the general public. A regulatory strategy could be to implement transparency principles specifically relating to the use of FRT, similar to the guidelines surrounding the usage of CCTV, such as erecting signs and posting full privacy disclosures on agent websites.[17]

B. Conceptualising Privacy

Privacy is an ambiguous concept, and is evolving as our world is besieged by technology that draws individuals more and more under the public eye. A challenge facing regulators of FRT is establishing a concept of privacy that takes into account the intrusive nature of FRT, with regard to the highly personal nature of biometric data and the manner by which it is collected.

The Privacy Act states an agency may only collect information by a means that does not intrude to an unreasonable extent upon the personal affairs of the individual.[18] But what constitutes intrusiveness with regards to collection of data by FRT is not settled. The UK case of *R(Bridges) v Constable Chief of Police* noted that FRT was more intrusive than normal CCTV, but dismissed the idea that FRT was intrusive for purposes of collection of information.[19] This decision turned on the point that there is no interference with the physical space or body of the person, for instance in comparison to DNA swabbing.[20]

The unique problem posed by FRT is that our faces are linked to our identity, which is inherently personal, but is consistently exposed to public view. Whether collection of biometric data is intrusive depends on your understanding of intrusiveness. Is intrusiveness

---

[13] Els J Kindt "Transparency and Accountability Mechanisms for Facial Recognition" (3 February 2021) The German Marshall Fund of the United States. https://www.gmfus.org/news/transparency-and-accountability-mechanisms-facial-recognition
[14] Privacy Commissioner Te Mana Matapono Matatapu "Privacy Impact Assessment Toolkit" (7 July 2015). https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment/
[15] Immigration Act 2009, s 32.
[16] https://www.nzherald.co.nz/business/supermarket-chain-foodstuffs-admits-facial-recognition-technology-used-in-some-stores/JTIIVPNXLV53SIYLRVLEIY2R24/
[17] Privacy Commissioner "Privacy and CCTV" (2009). https://www.privacy.org.nz/assets/BROCHURES/Privacy-and-CCTV-A-guide-October-2009.pdf
[18] Privacy Act, s 22 IPP 4.
[19] *R(on the application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 at [85]-[89]
[20] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) at [74].

defined by the means in which it is collected? If so, is this limited to a spatial understanding of intrusiveness as taken in *R(Bridges)*? The manner of intrusive means itself may need to evolve in consideration of surveillance technology; for instance zooming up on someone or covertly filming when they think they are not being watched could constitute intrusive, as opposed to merely filming a passerby on the street.[21] A different conceptualisation of intrusive has regard to the nature of the data itself - should the highly personal nature of biometric data mean that any collection of it without express consent be considered intrusive?

Answers to these questions lie outside the scope of this essay, but it is necessary that conceptions of privacy evolve to mitigate the expanding reach of surveillance technologies. Linked to conceptions of privacy is the right to freedom from unreasonable search and seizure under s21 of the New Zealand Bill of Rights Act (NZBORA). The Supreme Court found in *Hamed v R* [2011] NZSC 101 that the right to protection from unreasonable search and seizure under s 21 applied not only to physical intrusions but also covert surveillance.[22] Though there is no Parliamentary protection of the right to privacy in terms of surveillance, the court 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. It is yet to be confirmed whether s 21 extends to FRT, but it is clear conceptions of intrusion are expanding in response to the proliferation of usage of surveillance technology.

Developing a standard concept of privacy is a herculean task, but regulators could begin by providing special protection to biometric data and other highly personal data collected by FRT, as seen in the GDPR. Section 32 of the Privacy Act provides that the Privacy Commissioner can issue codes of practice modifying application of the IPPs or in relation to a specified class of information, and special protection could be afforded to the protection of biometric data, particularly with regard to means of collection and transparency surrounding it. Sufficient protection of biometric data could also be ensured by the implementation of Biometric Commissions or other biometric-specific oversight mechanisms. The UK has an active Biometrics Commissioner whose role is to keep under review the retention and use by police of DNA samples.[23] Several New Zealand Law Commission reports have flagged this as a viable oversight strategy, noting that “having a consistent approach to all biometric data may be considered desirable.”[24]

C. Other Standards of Privacy

A key strategy that regulators could use to ensure protection of privacy is to mandate technology design in accordance with privacy principles. The GDPR mandates “data protection by design and by default,” requiring data controllers to implement appropriate technical and organizational measures when designing and operating their technology in order to integrate data protection safeguards.[25] Such a principle could imply minimising

---

[21] Lynch, Campbell, Purshouse and Betkier above n 2.
[22] *Hamed v R* [2011] NZSC 101 at [165].
[23] Office of the Biometrics Conditioner Gov.UK “About Us.” https://www.gov.uk/government/organisations/biometrics-commissioner/about
[24] Law Commission Review of the Search and Surveillance Act 2012: Ko te Arotake i te Search and Surveillance Act 2012 (NZLC R141, 2017).
[25] Kindt, above n 13.

reference data, limited or decentralised storage, pseudonymisation where appropriate, encryption of data during transmission and storage, and use of any other appropriate standards.[26]

Regulators will have to mandate usage of technology that incorporates these design frameworks. The rise of Artificial Intelligence (AI) has been accompanied by the drafting of charters relating to algorithmic standards. New Zealand claims to be the first country in the world to have a government commitment to a set of standards for the use of algorithms by the public service, with the creation of the Algorithm Charter in 2020.[27] The charter was drafted in response to a review of the government's use of algorithms and the risks attached, and outlines commitment by government agencies to manage how algorithms will be used "to strike balance between privacy and transparency, prevent unintended bias and reflect the principles of the Treaty of Waitangi."[28]

The algorithms and systems that power state FRT surveillance are often proprietary in nature, with states buying technology from companies, placing barriers in the way of their availability for scrutiny.[29] Mandating responsible use of FRT algorithms would force technology developers to adhere to appropriate safeguards in order to sell their product. To give full effect to this, regulators could mandate charters of safe use that are applicable to all users of FRT including commercial companies and individuals, not just government agencies.

II. Policing Discrimination

On January 9th 2020, Robert Williams was mistakenly arrested due to a false-positive FRT analysis that pinpointed him as an offender. Mr Williams has launched a lawsuit against the Detroit Police Department, one of the counts being for "employing technology that is empirically proven to misidentify Black people at rates far higher than other groups".[30] FRT is shown to have higher false-positive rates turned out for women and people of colour, reflecting the fact that training databases are often composed of white male faces, and that default camera settings are geared towards those with lighter skin tones.[31]

There is specific concern in relation to the scope for FRT racial discrimination in New Zealand, and one Māori AI expert believes it is only a matter of time before a Māori person is wrongfully arrested because of a false match on facial recognition software.[32] The disproportionate representation of Māori in the justice system may lead to more intensive scrutiny and surveillance of Māori due to the presence of images on police imaging

---

[26] Kindt, above n 13.
[27] James Shaw "New Algorithm Charter a world-first" (press release, 28 July 2020)
[28] https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf
[29] Michael Vale Algorithms in the Criminal Justice System (Law Society of England and Wales, 2019) at 21.
[30] Tate Ryan-Mosley "The New Lawsuit that Shows Facial Recognition Technology is Officially a Civil Rights Issue"(14 April 2021) MIT Technology Review. https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/
[31] https://www.nature.com/articles/d41586-020-03186-4
[32] Meriana Johnsen "Police facial recognition discrimination against Māori a matter of time – expert" RNZ (online ed, New Zealand, 2 September 2020).

databases.[33] An unknown variable is tā moko and the effect that this will have on FRT analysis, as most overseas training databases will not have encountered moko before.[34]

Studies show that racial biases of FRT differ depending on the origin of the developer.[35] Regulatory strategies to combat discrimination could focus on implementing technical standards to improve the technology itself. This could take the form of mandating diverse training databases, and assigning algorithmic and camera default standards. But the most important strategy regulators can use to overcome discrimination following the use of FRT is to legislate for people processes surrounding FRT. Introna and Nissenbaum suggest that risk of FRT is that people are often treated as "guilty until proven innocent."[36] When one looks at the false arrests in the US, this certainly seems to be the case. There seems to be a misguided feeling that judgement calls are to be made by either FRT or humans. Regulators must be careful to ensure that due processes are crafted around the use of FRT, with FRT evidence and human judgement regarded as supplementary.

III. Protecting Indigenous Data Sovereignty

Regulators of FRT must also balance public interest use of data while ensuring specific protection of Indigenous Data Sovereignty (IDS). IDS is defined as the right of a nation to govern the collection, application and ownership of its own data, and reflects the right to data as a strategic resource.[37] The United Nations Declaration Rights of Indigenous Peoples (UNDRIP) affirms the right of indigenous peoples to self-determination, which includes control of resources.

Specific to New Zealand, regulators must incorporate and adhere to the principles of Te Tiriti o Waitangi. Maori data is subject to Te Tiriti o Waitangi as a resource, and the rise of big data and AI systems has led to calls for greater protection of Māori data sovereignty. Te Mana Raraunga has been established to advocate for Māori rights and interests in data to be protected as the world moves into an increasingly open data environment.[38] Regulators will have to ensure proper frameworks are in place to ensure proper protection of indigenous rights. In accordance with Te Tiriti, all drafting of guidelines must include consultation and co-drafting with Māori.

IV. Regulating in Favour of Freedom

The use of FRT also raises general concerns about the effect on civil rights. 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.[39] The current covid era has led to acceptance of higher levels of surveillance. For instance, existing FRT may be

---

[33] Lynch, Campbell, Purshouse and Betkier above n 2 at 4.7.
[34] Above n 32.
[35] National Institute of Standards and Technology, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software"(19 December 2019).
[36] Lucas Introna and Helen Nissenbaum "Facial Recognition Technology: A Survey of Policy and Implementation Issues" Lancaster University Management School Working Paper 2010/030.
[37] Tahu Kukutai, Stephanie Russo Carrol and Maggie Walter "Indigenous Data Sovereignty" IWGA The Indigenous World 654.
[38] Te Mana Raraunga Māori Data Sovereignty Network https://www.temanararaunga.maori.nz/
[39] Lynch, Campbell, Purshouse and Betkier above n 2 at 4.6.

employed sooner than previously thought in order to reduce touch to combat the spread of COVID-19.[40] Regulators must be careful to not be myopic in their provision for the use of FRT, and that the long-term freedoms are not sacrificed in the knee-jerk response to the COVID crisis. Regulators must also be cautious to legislate against the potential for usage of FRT to extend past the scope of its original purpose. For instance, China deployed a vast network of cameras with FRT capacity in the wake of the COVID outbreak, but the technology is now being used to ethnically discriminate against the Uyghur population.[41]

A strategy regulators could use to combat these issues could be to legislate with a presumption towards cautious use of FRT. Particularly with regard to use by the state, the minority view of Elias CJ in *Hamed v R* was that public officials should not be allowed to use FRT unless with express lawful authority. Regulators could craft the frameworks within which FRT is allowed to be used, rather than having a default stance of general usage. Another overarching regulatory strategy could be to afford a constitutional level of protection to the right to privacy, and allowing recourse to rectifying breaches of privacy. There is currently no right to privacy in NZBORA, with only recourse to invasion of privacy being through breaches of the Privacy Act and the tort of privacy, and there have been suggestions to the incorporation of a right to privacy into a new constitution.[42]

Experts have advised placing a moratorium on the technology altogether in New Zealand until more is known and better regulatory frameworks are put in place.[43] Some cities are so concerned about its application that they have banned use of it outright. Usage of FRT has been silent but quick, and regulators must implement appropriate frameworks now, lest we wake one day to the shadow of Big Brother much closer than we thought.

---

[40] Jackie Snow “Nano needles. Facial recognition. Air travel adapts to make travel safer” National Geographic (online ed, United States, 13 August 2020).
[41] “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).
[42] Andrew Butler and Geoffrey Palmer “The Proposed Constitution” (2016) Constitution Aotearoa NZ: 2017 Archive www.archive. constitutionaotearoa.org.nz.
[43] Lynch, Campbell, Purshouse and Betkier above n 2.