Human Rights Law Centre

The dangers of unregulated biometrics use (Part 2)

Supplementary submission to the Parliamentary Joint Committee on Intelligence and Security

5 September 2019

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

[redacted]
[redacted]
Human Rights Law Centre Ltd
Level 17, 461 Bourke Street
Melbourne VIC 3000

[redacted]
[redacted]
[redacted]
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses a strategic combination of legal action, advocacy, research, education and UN engagement to protect and promote human rights in Australia and in Australian activities overseas. It is an independent and not-for-profit organisation and donations are tax-deductible.

The Human Rights Law Centre acknowledges the people of the Kulin and Eora Nations, the traditional owners of the unceded land on which our offices sit, and the ongoing work of Aboriginal and Torres Strait Islander peoples, communities and organisations to unravel the injustices imposed on First Nations people since colonisation and demand justice for First Nations peoples.

Contents

1. Introduction

1. Thank you for the opportunity to provide a supplementary submission to the Parliamentary Joint Committee on Intelligence and Security's (**PJCIS**) review of the Review of Identity-Matching Services Bill 2019 (the **Bill**) and the Australian Passports Amendment (Identity-matching Services) Bill 2019.

2. On 29 May 2018, the Human Rights Law Centre (**HRLC**) provided a detailed submission to the PJCIS' inquiry on the earlier iteration of the Bill. We thank the Committee for accepting that submission in evidence to this review.

3. We continue to welcome the approach of providing a legislative framework for the collection, retention, use and sharing of facial images and other biometric data. As we explained in our earlier submission, new capabilities for search and surveillance must be governed by law, and existing laws are insufficient to ensure this. **However we remain of the view that the proposed Bill is manifestly and dangerously insufficient for this purpose.**

4. This submission does not repeat the arguments put in our earlier submission, but instead provides legal and policy updates from two comparative domestic jurisdictions, the United Kingdom and the United States, that are relevant to identity-matching or facial recognition services.

5. Two matters are clear from developments abroad. **First, use of facial recognition and identity matching services must be subject to a clear legal regulatory system** that not only enables authorities to undertake identity matching but safeguards the civil liberties of people whose facial images are used. There are serious rights implications from deployment of facial recognition technology that go to our right to privacy but also to our ability to participate in public spaces in a democracy, particularly for people of colour. These matters are:

   (a) the subject of the first judgment concerning automated facial recognition the UK High Court of Justice (*Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin) (see part 2.1 below);

   (b) the basis for a finding by an independent review into London Metropolitan Police trials of facial recognition technology that London's police trials of facial recognition are likely to violate human rights (see part 2.3 below);

   (c) the rationale for three US cities banning the use of facial recognition technologies (see part 3.2 below); and

(d) a reason behind a ruling by the US Court of Appeals certifying a case against Facebook for its use of facial recognition (see part 3.1 below).

6. Secondly, facial recognition technologies are advancing apace and the law is slow to keep up. **In the absence of legal regulation, the use of facial recognition continues albeit without necessary safeguards for human rights.** Law enforcement are understandably keen to deploy new technologies that might assist in policing and investigations. South Wales police proceeded with a trial of a facial recognition app even as their earlier trial of facial recognition technology was subject to judicial consideration (see part 2.2 below).

7. The comparative experience is relevant to Australia in a number of ways:

(a) It highlights that the use of facial recognition technology and identity matching involves the capture of biometric data, personal information of a highly sensitive nature, without consent. That intrusive nature is only more reason for such technologies and surveillance to be strictly law-governed.

(b) The Bill does not provide a legal basis for use of identity matching services and little, if any, safeguards for Australians whose information will be vacuumed into databases used for search comparisons. The Bill can be characterised as providing authorities with extraordinarily broad capabilities to use facial recognition technology without any apparent regard for the civil liberties of all of us who will be affected. The Bill does not provide the necessary details of the regulation of the Interoperability Hub, the National Driver Licence Facial Recognition Solution (**NDLFRS**) and the identity matching services that would allow for a proper, informed parliamentary and public debate over the proposals.

(c) According to the Bills Digest, at least two of the six identity-matching services are already in operation.[1] We need much greater openness and transparency around their operation, safeguards for privacy, and to have clear law governing the operation of these services and providing the necessary safeguards for using sensitive biometric information.

(d) The Bill is more draconian than the UK scheme, making Australians more vulnerable to privacy intrusions. Unlike the UK, where people subject to facial recognition surveillance are compared to a "watchlist" of suspects, missing people and persons of interest to the police, the Bill establishes a scheme whereby everyone with government-approved documentation is effectively part of the comparative search or on the "watchlist", regardless of their being suspected of a crime.

[1] Parliamentary Library, *Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019*, Bills Digest, 26 August 2019, p 13.

8. The remainder of the submission provides more detail in relation to the updates from the UK and US.

2. United Kingdom

2.1 UK legal challenge to facial recognition (September 2019)

9. On 4 September 2019 the High Court of Justice delivered judgment in *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin). The case concerned the trial of Automated Facial Recognition (**AFR**) technology by South Wales Police, who used facial recognition technology to map faces in a crowd and then compared those images to a "watchlist". The claimant alleged that the use of AFR was a violation of his right to privacy under the *Human Rights Act* and was also contrary to the requirements of the UK's data protection legislation. The Court found that facial recognition interferes with the privacy and data protection rights of everyone who is scanned and on the watchlist, but nonetheless its use in the circumstances of the case is currently lawful.

10. The case is worth considering as it may be the first in the world to consider AFR, and although the claimant was unsuccessful, there are some material differences between the UK legal scheme and the Australian context that highlight the lack of safeguards here.

11. First the court noted the potential for menacing use of AFR and the need for proper legal frameworks around it:

> AFR is another new and powerful technology which has great potential to be put to use for the prevention and detection of crime, the apprehension of suspects or offenders and the protection of the public. **Its use by public authorities also gives rise to significant civil liberties concerns. Using AFR can involve processing the facial biometric data of large numbers of people. The raw power of AFR – and the potential baleful uses to which AFR could be put by agents of the state and others – underline the need for careful and ongoing consideration of the effectiveness of that framework as and when the uses of AFR develop.**" [emphasis added][2]

12. It said that it is technology that must "give pause for thought" because of its potential to impact upon privacy rights.[3] It quoted *S v United Kingdom* (2009) 48 EHRR 50 at [112]:

> The protection of [privacy] would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important

[2] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), [7].

[3] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), [46].

> private life interests…any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[4]

13. The court found that AFR-derived biometric information is "an important source of personal information" and "information of an 'intrinsically private' character". The manner in which South Wales Police use AFR "goes much further than the simple taking of a photograph. The digital information that comprises the image is analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlist information."[5]

14. The court found that although the use of AFR infringed the right to privacy, it was nonetheless according to law and a proportionate infringement. There are a few issues worth drawing out and contrasting with the Bill, as the UK has important safeguards in its legislation that formed the basis of the court's finding of proportionality, safeguards that are not apparent from analysis of the Bill.

15. **Limited watchlists**: In the UK, facial recognition technology maps faces in a crowd and then compares them to a watchlist of images, which can include suspects, missing people and persons of interest to the police. Watchlists are usually around 400-800 people, and maximum capacity is 2000.[6] The fact that watchlists are clearly targeted was a factor in the police's favour in the proportionality analysis.[7]

16. In comparison, the Bill would provide authorities with access to much broader databases for identity matching, databases comprised of people with licences and passports, among other things, and therefore a much greater intrusion on nearly all Australians' privacy without consent. As the court held in this case, the violation of privacy happens not just for people whose faces are scanned in the crowd, but also for those whose faces are used as a comparator.

17. **Data retention**: The South Wales Police had very strict retention policies and if no match (false or positive) is made, then the police do not retain the facial biometrics or image of person whose faces are scanned.[8] The court was satisfied that any interference would be "near instantaneous" before discarding the Claimant's data.[9] The Bill on the other hand makes provision for the Department of Home Affairs to collect and use data for an extraordinarily broad range of purposes but provides no protections for people whose facial images are retained in terms of how that data is retained, used or discarded.

---

[4] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), [46].

[5] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), [54].

[6] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin) [31].

[7] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin) [104].

[8] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), [37].

[9] *Q (Edward Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), [101].

18. **AFR deployed in open and transparent way**: When AFR was used at events, it was signposted and there was significant public engagement. In contrast it is very unclear if and how AFR will be regulated, how the Interoperability Hub and NDLFRS will work, any safeguards on the collection, retention or use of data that flows through and is held in those systems.

2.2 Welsh police identity matching app (August 2019)

19. The experience in the UK is that police are keen to adopt the new facial recognition technology as it becomes available, even where there were serious question marks over the legality and human rights impacts.

20. Welsh police are reportedly planning to use a facial recognition app on their phone that will allow them to identify suspects without taking them to a police station.[10] The app will allow officers to run a snapshot of a person through the UK's watchlist, and find potential matches.

2.3 Evaluation of UK Police Trial (July 2019)

21. In July 2019, the Human Rights, Big Data and Technology Project published the findings of an independent review of the trials of live facial recognition (**LFR**) by London police in the UK.[11] Live facial recognition technology "allows for the real time biometric processing of video imagery in order to identify particular individuals."[12] If such technology is used in Australia, images captured could be shared through the Interoperability Hub or the NDLFRS established by the Bill.

22. The review included observation of the police's six test deployments from beginning to end, attending briefing and de-briefing sessions with police as well as planning meetings and presence in the control room. There are a few key points to draw from that review to inform the Committee's consideration of the Bill.

Absence of specific legal basis for facial recognition technologies

23. The review highlights the critical importance of having an explicit legal basis when engaging in rights-intrusive surveillance. In contrast to the judgment considered above, a major problem

[10] Sample, S, "South Wales police to use facial recognition to identify suspects," The Guardian, 7 August 2019, available at https://www.theguardian.com/technology/2019/aug/07/south-wales-police-to-use-facial-recognition-to-identify-suspects.

[11] Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

[12] Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, section 1.2.1, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

identified through the police trial was the absence of an explicit legal basis for the use of LFR. In the UK, no single piece of legislation provides explicit authorisation for police to use LFR. However the police purported that their legal mandate derived from a range of sources of law, despite the fact that none of those sources provide an explicit legal authorisation for LFR as such. Nor are there any publicly available frameworks governing use of the technology.

24. Under the UK Human Rights Act, any interference with individuals' rights must be in accordance with the law, pursue a legitimate aim and be "necessary in a democratic society." Use of LFR, the review found, "is a particularly invasive surveillance technology directly affecting a number of human rights protections, including those relevant to democratic participation."[13] It referred to UK and European law in support of the proposition that specific statutory measures or other express legal authorities are required to justify more invasive measures taken in the course of police investigation, so as to guard against arbitrary application and abuse of surveillance technologies.[14]

25. The report concludes that the implicit legal authorisation claimed by the police is inadequate and would likely not withstand a legal challenge under the UK Human Rights Act, on the basis that it is not "in accordance with law".[15] It also concluded that it was highly possible that the police trial would be found to be not "necessary in a democratic society if challenged in a court."[16] As stated above, the High Court has since found that the existing legal framework was adequate.

26. Similarly, the Bill does not establish a solid legal basis for the collection, retention, use and sharing of biometric data including facial images. Whilst the Bill before the Committee is of a different structure to that in the UK, like the UK scheme the Bill does not expressly authorise access by agencies – entities requiring access to the Interoperability Hub or NDLFRS will need another legal basis for access and must meet access requirements set out in the Intergovernmental Agreement on Identity Matching Services (**IGA**). Whilst Qld and NSW have

[13] Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, p 54, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

[14] See discussion of *Catt v the United Kingdom*, Judgment, ECtHR, App No 43514/15, 24 January 2019, para 114, referencing *PG and JH v the United Kingdom*, judgment, ECtHR, App No 44787/98, 25 September 2001, para 62, in Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, p 54, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

[15] See discussion in Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, section 3.2, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

[16] Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, p 6, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

passed laws to provide a legal basis, it is unclear the particular laws that other states and territories will use to justify their participation.[17] Further, safeguards such as access criteria are not contained in the Bill, but in the IGA instead. We note the Victorian Information Commissioner's concern that compliance through such instruments may not be robust and could lead to controls being amended without parliamentary oversight.[18]

27. The use of biometric data should be governed by laws with sufficient detail for Australians to understand what is being done with their sensitive personal information, as well with as adequate safeguards to protect against mission creep, misuse of data and inaccuracy. We need meaningful parliamentary understanding and agreement to any proposed regime, which is virtually impossible given the absence of detail in the Bill.

Technology is inaccurate

28. The trial program demonstrated a technology that is not reliable. From the trials, facial recognition matches were only correct eight out of 42 times, 19.05%.[19] Therefore the technology alone does not confirm an identity, without added human assessment.

3. United States

3.1 Court ruling on case against Facebook (August 2019)

29. On 8 August 2019, a US Court of Appeals allowed a case to be brought against Facebook for its use of facial surveillance technology against its users without consent.[20] In *Patel v Facebook*, the Court of Appeals certified a class of Facebook users to bring the action alleging that Facebook's use of facial recognition technology violated their rights under the Biometric Information Privacy Act.[21] The court found that "the development of a face template using facial-recognition technology without consent (as alleged in this case) invades an individual's private affairs and concrete interests."[22]

---

[17] See Parliamentary Library, *Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019*, Bills Digest, 26 August 2019, p 15.

[18] Office of Victorian Information Commissioner, Submission to PJCIS pp 1, 3, cited in Parliamentary L brary, *Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019*, Bills Digest, 26 August 2019, p 19.

[19] Fussey, P & Murray, D, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology", July 2019, p 10, available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

[20] *Patel v Facebook* No. 18-15982 (9th Cir. 2019) available at https://www.aclu.org/legal-document/patel-v-facebook-opinion.

[21] *Patel v Facebook* No. 18-15982 (9th Cir. 2019) available at https://www.aclu.org/legal-document/patel-v-facebook-opinion.

[22] *Patel v Facebook* No. 18-15982 (9th Cir. 2019), summary, available at https://www.aclu.org/legal-document/patel-v-facebook-opinion.

30. The ruling allows the case to proceed as a class action against Facebook in the District Court.

3.2 Facial recognition banned in cities in the USA (May 2019)

31. The use of facial recognition technologies have been banned in San Francisco and Oakland, California, as well as Somerville, Massachusetts.

32. San Francisco was the first city to introduce a ban as part of a broader ordinance regulating surveillance.[23] It stated:

> The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring.[24]

33. Police in San Francisco did not use facial recognition, although they had trialled it.

[23] Conger, K et al, "San Francisco bans facial recognition technology", New York Times, 14 May 2019, available at https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

[24] Stop Secret Surveillance Ordinance, (05/06/2019) available at https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019.