Australian Identity-Matching Services Bill

Jake Goldenfein (Melbourne Law School)
Monique Mann (Deakin University)

Since 2017, the Australian federal government has pushed for political and legal changes to make facial recognition technology more widely available to civil and policing agencies. These efforts, part of a long-term and continuing expansion of surveillance powers by the Australian federal government, have culminated in a new biometric identity-information system. Federal authorities have argued that facial recognition technology is useful for law enforcement and preventing identity fraud, but to achieve those benefits, they have combined civil and criminal, as well as state and federal, identity systems into a powerful intelligence apparatus controlled by a single government department: the Australian Department of Home Affairs.

Home Affairs was created in 2017 through a merger of the Department of Immigration and Border Protection and the Australian Border Protection Service. As a result of the merger, Home Affairs assumed multiple policing and intelligence competencies from the Attorney General's Department (AGD), including those related to national security, immigration, organized crime, cybersecurity, and public safety policing. Home Affairs also took over control and operation of the national identity-matching services, which included the one-to-one facial recognition verification system known as the "Face Verification Service" (FVS).[1]

[1] One-to-one verification means that an image is submitted along with a stated identity, and the system responds with a "yes" or a "no." The purpose is to prevent identity fraud by ensuring an individual presenting to an agency is who they claim to be.

The Australian government has been developing the institutional, technical, and legal architecture for facial recognition capabilities for several years,[2] culminating in the 2019 federal Identity-Matching Services Bill.[3] The original bill was rejected, however, for a lack of privacy protection and oversight, and is presently being redrafted. The new bill will likely increase parliamentary oversight of the system and the amount of necessary reporting, but will not challenge the fundamental institutional changes that are already underway, such as the aggregation of civil and criminal systems, or increased control of state-level civic data within a federal intelligence system.

Although governments have always had the function of identifying their citizens,[4] they have not always linked those identities to intelligence dossiers or made them available to law enforcement agencies. Indeed, the intermingling of civil and criminal identity systems has been the concern of human rights jurisprudence for some time.[5] Biometrics are of particular concern to the linkage of criminal and civil systems, and surveillance more generally, because they act as a conduit between an individual's physical presence and digital databases, thus amplifying surveillance capacities. By advancing a centralized identity matching system, Australia is pushing beyond the limits of legitimate state function.

BIOMETRICS DEVELOPMENT IN AUSTRALIA

Australia has collected biometric information, including images for facial recognition, since at least 2007. This began with border-protection agencies collecting information from noncitizens, such as people caught fishing illegally in Australian waters, and eventually from visa applicants. It has progressively expanded to include information collected from Australian citizens, both at the border and through civic licensing agencies.[6] States have also used biometric systems for matching against their police information holdings (i.e., mug shot databases) since at least 2009.[7]

The 2007 Intergovernmental Agreement to a National Identity Security Strategy[8] proposed the development of a national biometric interoperability framework,[9] which was launched in 2012.[10] Plans for a further national facial biometric matching "Capability" to enable cross-jurisdictional sharing of identity information, the precursor to the identity matching system operated by Home Affairs, were announced in 2014.[11]

[2] See, e.g., Australian Government, Department of Home Affairs, "Agreement to a National Identity Security Strategy," April 2007, https://www.homeaffairs.gov.au/criminal-justice/files/inter-gov-agreement-national-identity-security-strategy.pdf.

[3] Identity-Matching Services Bill 2019 (Cth). The note (Cth) indicates that this is a commonwealth or federal bill. The Identity-Matching Services Bill was first introduced in February 2018, but did not progress through parliament and lapsed in April 2019. It was reintroduced in July 2019.

[4] See, e.g., Markus Dirk Dubber, *The Police Power: Patriarchy and the Foundations of American Government* (New York: Columbia University Press, 2005).

[5] See, e.g., Jake Goldenfein, *Monitoring Laws: Profiling and Identity in the World State* (Cambridge: Cambridge University Press, 2019).

[6] Dean Wilson, "Australian Biometrics and Global Surveillance," *International Criminal Justice Review* 17, no. 3 (September 2007): 207–219.

[7] Parliament of Australia, "CrimTrac Overview 2009" (direct download, PDF), https://www.aph.gov.au/DocumentStore.ashx?id=dd60984f-33e2-4836-85a4-690052ca7914.

[8] Australian Government, Department of Home Affairs, "An Agreement to a National Identity Security Strategy," April 2007, https://www.homeaffairs.gov.au/criminal-justice/files/inter-gov-agreement-national-identity-security-strategy.pdf.

[9] Australian Government, Department of Home Affairs, "A National Biometric Interoperability Framework for Government in Australia," n.d., https://www.homeaffairs.gov.au/criminal-justice/files/national-biometric-interoperability-framework-for-government-in-australia.pdf.

[10] Attorney-General's Department, National Identity Security Strategy 2012, Canberra, 2013.

[11] Law, Crime and Community Safety Council, *Communique*, COAG Meeting, Canberra, October 3, 2014, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/3523779%22.

The one-to-one face verification system (FVS) that Home Affairs took over from the Attorney-General's Department (AGD) began operating in 2016, but only included passport images held by the federal Department of Foreign Affairs and Trade (DFAT).[12] Given the uptake of driver's licenses in the general population and the ambition for a national system, the policy goal has long been to integrate state-controlled driver's license images into a general database for policing and intelligence.[13] Efforts by federal entities to access driver's license images have been, however, frustrated by state privacy laws, which prohibit providing federal agencies direct access to their databases.[14] The result has been limited and complex arrangements for cross-jurisdictional information sharing. This began to change, however, with the 2017 Intergovernmental Agreement on Identity Matching Services (IGA)[15]—the precursor to the Identity-Matching Services Bill—and the corresponding formation of the Department of Home Affairs, with its very broad federal policing and intelligence remit.

CENTRALIZATION OF IDENTITY DATABASES

In 2017, the Australian states agreed multilaterally to enable federal access to their identity data under the auspices of the IGA. Some states made explicit the value they saw in the system, with the Queensland Minister for Police noting the value that one-to-many facial recognition would contribute to enhanced security at the Commonwealth Games.[16] Other states were more reluctant, raising the alarm about possible contravention of state-level human rights protections, and suggesting that there were inadequate protections for civil liberties.[17]

Nonetheless, the IGA established the framework for a data-sharing regime, gave immunity from state-level privacy laws, and introduced new identity-matching services, including a one-to-many facial identification service (FIS) to complement the FVS. Such systems are the primary facial recognition tool used in policing in Australia. The system allows for law enforcement, national security, and related entities at state and federal level to run queries through the technical infrastructure of a host agency: originally the AGD, and then the Department of Home Affairs. Importantly, while the IGA introduced a technical architecture for information sharing, it left control over identity databases with the states.[18]

[12] See Allie Coyne, "Australia's New Facial Verification System Goes Live," *IT News*, November 16, 2016, https://www.itnews.com.au/news/australias-new-facial-verification-system-goes-live-441484. That federal system was populated by passport photos, which in 2010–2011 covered approximately 48 percent of the Australian population (Department of Foreign Affairs and Trade (Cth), "Program 2.2: Passport Services," *Annual Report 2010–2011*, https://nla.gov.au/nla.obj-990174440/view?partId=nla.obj-994334219#page/n161/mode/1up) and presently covers about 57.9 percent of the population (https://www.passports.gov.au/2019-passport-facts).

[13] Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Strengthening Oversight," *UNSW Law Journal* 40, no. 1 (2017): 121–145.

[14] See, e.g., the Parliament of the Commonwealth of Australia, "Identity Matching Services Bill 2019, Explanatory Memorandum," describing Clause 19 of the Bill. An exception is the NSW Roads and Maritime Services, which provides access to the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) for the purposes of investigating terrorism offenses.

[15] Council of Australian Governments, "Intergovernmental Agreement on Identity Matching Services," October 5, 2017, https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf.

[16] Mark Ryan, "Queensland Leads Nation to Strengthen Security Measures," Queensland Government, The Queensland Cabinet and Ministerial Directory, March 7, 2018, http://statements.qld.gov.au/Statement/2018/3/7/queensland-leads-nation-to-strengthen-security-measures.

[17] See, e.g., Adam Cary, "Biometrically Opposed: Victoria Queries Peter Dutton over Facial Recognition Scheme," *Sydney Morning Herald*, May 2, 2018, https://www.smh.com.au/politics/federal/biometrically-opposed-victoria-queries-peter-dutton-over-facial-recognition-scheme-20180502-p4zcvs.html.

[18] Note that the IGA architecture replicates, and was perhaps inspired by, the FBI's Next Generation Identity system, launched in 2014. See FBI, Next Generation Identification (NGI), https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

A few months later, the government introduced the Identity-Matching Services Bill, which ostensibly legislated for the IGA. In reality, however, the bill went significantly further, shifting the system from one that facilitated information sharing into one that enabled the aggregation and centralization of identity information in the Department of Home Affairs.

This increased centralization is in no way integral to satisfying the objectives of the system, at least as publicly stated. The bill's explanatory memorandum, for instance, outlined the primary goal as preventing fraud and identity theft (described as an enabler of organized crime and terrorism), but not to build an intelligence apparatus.[19] Despite the limited technical capacity necessary to achieve that stated objective, the system specified in the bill would fold state-level transport authorities' data and images into the data-intensive apparatuses of federal security and intelligence agencies.

The centralizing dimensions of the system architecture become apparent when looking closely at the differences between the IGA and the bill. Beyond addressing identity fraud, we suggest these changes reveal the true underlying political rationalities and motivations for establishing this national facial recognition system as a radical shift in identity data governance arrangements.

LEGAL CONCENTRATION OF POWER

The Identity-Matching Services Bill sought to establish Home Affairs as the "hub" through which government identity-verification and law enforcement suspect-identification requests are processed, establishing Home Affairs as the central point of information processing across the public sector and for law enforcement agencies. But there were meaningful departures from the system described in the bill and the 2017 IGA.

The IGA outlined two technical architectures: 1) The National Driver License Facial Recognition Solution (FRS), a biometric identity image database; and 2) the "interoperability hub," a communications system for processing and routing data access requests from agencies around Australia.

In the IGA, the FRS was described as a federated database system, in which state-level data would be partitioned, and state agencies could control the conditions of access. Databases would be linked through Home Affairs, which would operate the facial recognition technology that performs identity matching. The FRS was described as retaining only biometric identity templates and no other identity or personal data. The IGA stipulated that the host agency (initially the AGD, but subsequently Home Affairs) could not view, modify, or update information in partitioned federated databases containing state-level information. However, the bill only prescribed that Home Affairs could not modify or update that data; in other words, it could still view it.[20] In fact,

[19] The Australian Government IDMatch home page, for example, promotes "Identity Matching Services that help verify and protect your identity" (https://www.idmatch.gov.au). See also the Parliament of the Commonwealth of Australia, "Identity Matching Services Bill 2019, Explanatory Memorandum," https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6387_ems_f8e7bb62-e2bd-420b-8597-8881422b4b8f/upload_pdf/713695.pdf;fileType=application%2Fpdf.

[20] Sup. 11. See IGA clause 6.16.

the legislation clarified that Home Affairs *could* collect, effectively without limit, information flowing through the systems for satisfaction of its "community safety" purposes, which include law enforcement, national security, community safety, protective security, and road safety, along with identity verification. The bill effectively vested control over the databases of driver's license images squarely within Home Affairs, and enabled unrestrained collection of information.

With respect to the "interoperability hub," the IGA described it as a "router" through which agencies around the country could request and transmit information to one another. That is, it could be used for "relaying electronic communications between bodies and persons for the purposes of requesting and providing identity-matching services." Rather than simply routing information from place to place, however, the bill enabled Home Affairs to collect data flowing through the hub whenever an agency used an identification, verification, or information sharing service, both for the sake of operating that database,[21] as well as for its identity and community protection activities.[22] The bill thus enhanced the legal capacity of Home Affairs from an infrastructure provider into a data aggregator.

Other important elements of the bill gave greater power than envisaged to the Department of Home Affairs. For instance, the bill enabled the Minister for Home Affairs to expand the powers under the regime without parliamentary oversight. Furthermore, the identity information that could be collected through those systems was far broader than anticipated by the IGA,[23] including information held by agencies that is about or associated with the identity document.

It is difficult to identify a single rationale that may have motivated the changes between the IGA and the Identity-Matching Services Bill. New technological affordances associated with facial recognition may have animated interest in developing a comprehensive national system, especially considering international trends. The institutional culture and political power of the Department of Home Affairs may also have made centralization and the use of civil documents in intelligence investigation more feasible. Indeed, its participation in forms of intelligence work and political policing connects it to a policing tradition that has always involved information aggregation, not necessarily in line with traditional liberal political limits.[24] That expansion of political and technological power is also consistent with Home Affairs' broad portfolio.

Australia lacks enforceable human rights protections at the federal level (though some states have their own independent human rights protections), which raises a number of issues and concerns with the centralization of data and surveillance capabilities within federal agencies. Under the Australian Constitution,[25] crime control and criminal justice are a competency of the states, not the federal government. Policing agencies are historically restricted to identity matching against data in local policing information systems (such as mug shots), which

[21] Sup. 3. See § 17 (2).

[22] Sup. 3. See § 17(2)(b); note that the purposes for which Home Affairs can collect data flowing through the interoperability hub is not clear in the legislation because it is split over two provisions. However, it has been interpreted to mean collection is permitted for the broader range of purposes (Bills Digest).

[23] In the Bill, § 5; in the IGA, clause 3.1.

[24] See, e.g., Bernard Porter, *The Origins of the Vigilante State: The London Metropolitan Police Special Branch before the First World War* (London: Weidenfeld and Nicolson, 1987).

[25] *Commonwealth of Australia Constitution Act 1900* (Cth).

have comprehensive rules and limits on retention.[26] As Home Affairs moves to aggregate and centralize biometric data, it is violating privacy norms by way of "scope creep," i.e., generating data for one government purpose (e.g., licensing drivers), and using it for another (e.g., policing or other punitive applications).

PJCIS REJECTS THE BILL

Ultimately, the Identity-Matching Services Bill did not pass parliamentary scrutiny and was rejected by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). But the specific issues that led to its rejection are unlikely to halt the system's development. In fact, the rejection can be interpreted as an endorsement of the general system and the resultant centralization, subject to privacy and accountability "tweaking."

When the bill reached the PJCIS, it was rejected largely due to concerns that it would grant too much executive authority to the Department of Home Affairs, meaning that the Minister for Home Affairs could change rules without legislative oversight.[27] The PJCIS also echoed the fears of privacy advocates around the possibility of a real-time, facial recognition-powered CCTV mass surveillance system which could end anonymity in public and stifle political action like protesting. The report also noted accountability issues like the absence of judicial warrant requirements, and the lack of a dedicated biometric oversight body (both of which exist in the United Kingdom).

On a broader level, the PJCIS expressed anxieties around the system not being proportionate to the issues it purported to solve, or sufficiently privacy-protective. But those concerns were connected to possible problematic "uses" of the system, not the broader structural issues of data centralization or the aggregation of civil and criminal identity databases. Instead, there was general approval that this type of data sharing would occur subject to a binding legislative framework rather than through creative interpretations of law enforcement and security exemptions to privacy laws.[28]

[26] Jake Goldenfein, "Police Photography and Privacy: Identity, Stigma, and Reasonable Expectation," *University of New South Wales Law Journal* 36, no. 1 (2013): 256–279.

[27] See Parliament of Australia, "Review of Identity-Matching Services Bill 2019 and the Australian Passports Amendment (Identity-Matching Services) Bill 2019," n.d., https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019.

[28] See the "Parliamentary Joint Committee on Intelligence and Security" (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security), the "Advisory Report on the Identity-Matching Services Bill 2019 and the Australian Passport Amendment (Identity-matching Services) Bill 2019" (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report), and "A Workable Identity-Matching Regime" (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report/section?id=committees%2Freportjnt%2F024343%2F27805). Specifically, the PJCIS argued that the Identity-Matching Bill is designed to "permit all levels of government and the private sector unprecedented access to Australian citizens' private biometric information in the form of a facial image" and that "given the significance of these measures, the Committee considers it preferable that privacy oversight and safeguards are established and set out in this enabling legislation rather than only being provided in supplementary agreements or arrangements."

The PJCIS accordingly recommended redrafting the bill to make its function and purpose clearer to the ordinary reader, reduce Ministerial rule-making power, fund a biometric oversight commission, and require more comprehensive reporting.[29] The PJCIS did not, however, completely reject the bill, the use of facial recognition technology, or the new data governance arrangements that would power the system.

FUTILITY OF AUSTRALIAN REGULATORY OVERSIGHT

The Identity-Matching Services Bill is presently being redrafted, with the new text yet to be released. Nonetheless, the states continue to upload identity images to the system in anticipation of the law passing and the system developing along similar lines. One reason political review has failed to meaningfully challenge the general structure of the identity matching and facial recognition system is that the debate, especially as expressed in the PJCIS report, has taken up a “privacy versus security” framing. International human rights law requires that state surveillance be “reasonable” and “proportionate,” and this language clearly influenced the PCJIS.

Under a human rights framework, to legitimately limit fundamental freedoms like privacy, a surveillance intervention must be directly related to, and the least restrictive measure for, the “necessary” purpose pursued. A true proportionality analysis might question whether such dramatic data governance rearrangements are necessary to address the stated purpose of identity fraud. In reality, however, this framing is operationalized in ways that enable continuing expansion of surveillance systems, especially in nations like Australia, where it is not backed up by actionable protections.

When privacy is pitched against security, the benefits of centralization and surveillance technology to purposes like identity fraud are taken as given, and the question becomes: Which civil liberties are we willing to curtail or limit in exchange? Blanket data sharing for policing and intelligence agencies is thus readily accepted and normalized as a necessary response to crime and insecurity, subject to privacy *balancing* intended to curtail its most abusive and authoritarian dimensions.[30] That framing fails to address the reality that the system fundamentally eliminates the need for the largest policing and intelligence apparatus in the country to justify its access to personal data that was previously distributed to the states. This goes beyond agencies using biometrics for their democratically constituted civic purposes (e.g., driver’s licenses), and beyond the stated intention of the bill (e.g., detecting identity fraud). By pushing this bill forward, Home Affairs is promoting facial recognition technology as a necessary solution to identity crime, while sidelining concerns around the institutional and data governance rearrangements that it claims are necessary for its introduction.

[29] It should be noted that there are oversight bodies responsible for Commonwealth law enforcement agencies under the Law Enforcement Integrity Commissioner Act 2006 (Cth) that established the Commonwealth Integrity Commissioner and the Australian Commission for Law Enforcement Integrity, which has jurisdiction over all Commonwealth law enforcement agencies (including those responsible for the facial biometrics matching system).

[30] See, for example, Monique Mann et al., “The limits of (Digital) Constitutionalism? Exploring the Privacy-Security (Im)balance in Australia,” *International Communication Gazette* 80, no. 4 (2018), 369–384.

From this position, it becomes impossible to challenge the construction of the surveillance system, or to fight the technical or institutional architecture, in any meaningful way. The institutional momentum also makes resisting significant data governance rearrangements difficult. One recent positive development, however, has been the Australian Human Rights Commissioner calling for a moratorium on the use of facial recognition technology as part of the Technology and Human Rights Project, which mirrors some international trends.[31] However, it is uncertain what impact this will have on the design, development, and eventual deployment of facial recognition technology in Australia, especially considering the extent to which the infrastructure is already in place.

Finally, technologies like Clearview AI, which has aggregated billions of identified images from the public web, complicate how to parse these developments.[32] Private providers, not constrained in the same way, can undermine relevant privacy protections or political processes by secretly selling surveillance *services* to government, while using their own privately operated infrastructure. When governments procure those services, they bypass whatever regulatory or financial obstacles might have prevented or limited those developments by the state itself. To that end, it is at least admirable that the Australian identity matching regime will be implemented in law, subject to democratic process and parliamentary oversight. Nonetheless, even when that is the case, the purposes expressed to justify new facial recognition *implementations* for the sake of those democratic processes appear not to tell the full story. It remains imperative to identify and address the institutional realignments and data governance reconfigurations connected to technologies like facial recognition and not be distracted by any single new surveillance capacity.

[31] Australian Human Rights Commission, "Human Rights and Technology Discussion Paper," December 2019, https://www.humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019.

[32] "Australian police agencies initially denied they were using the service. The denial held until a list of Clearview AI's customers was stolen and disseminated, revealing users from the Australian Federal Police as well as the state police in Queensland, Victoria and South Australia." See Jake Goldenfein, "Australian Police Are Using the Clearview AI Facial Recognition Technology with No Accountability," *The Conversation*, March 4, 2020, https://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667.