Australian Privacy Foundation

https://www.privacy.org.au

Secretary@privacy.org.au

https://privacy.org.au/about/contacts/

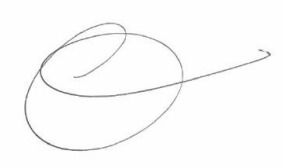
15th of August 2018

Dear Professor Cannataci

As agreed during your recent travel to Australia we provide a background brief on issues of privacy in Australia including an examination of the main shortcomings in the legal and regulatory framework, and details of specific recent incidents of privacy violations in Australia. We conclude with a series of recommendations for you to consider in the Australian context.

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is also attached at the conclusion of this brief.

Yours sincerely,



Dr Monique Mann
Co-Chair Surveillance Committee
Member, Board of Directors

Privacy in Australia
Brief to UN Special Rapporteur on Right to Privacy

(1) Executive Summary

This brief has been prepared by the Australian Privacy Foundation[1] in response to a request by the UN Special Rapporteur on Privacy Professor Joseph Cannataci. This arose following a meeting of civil society representatives in Sydney in late July 2018 to discuss issues of privacy in Australia. This brief is structured as follows. First, an overview of some of the systemic issues in Australia's human rights and privacy framework is provided. This is followed by an examination of some of the recent symptomatic manifestations of these systemic issues. We conclude with a list of key recommendations for the UN Special Rapporteur on Privacy to consider in the Australian context. Our main recommendations are:

1. Introduce an enforceable charter or bill of human rights at the federal level;
2. Introduce a privacy tort;
3. Appoint a Federal Privacy Commissioner and increase funding to the Office of the Australian Information Commission;
4. Implement proactive principles of privacy by design and data protection by design and default rather than reactive remedial attempts;
5. Consider the impacts of data collection and use in ways that extend beyond privacy, and;
6. Encourage, respect and promote Indigenous Data Sovereignty initiatives and associated principles in the collection and use of information concerning Australia's Indigenous Peoples.[2]

[1] We wish to acknowledge the contributions of APF Professional Placement Students Lauren Jewson and Hannah Taylor. We also wish to acknowledge the excellent research assistance provided by Harley Williamson, and the QUT Faculty of Law for financing Harley's contribution.
[2] See for example: Kukutai, T., & Taylor, J. (2016). Data Sovereignty for indigenous peoples: current practice and future needs. In *Indigenous Data Sovereignty: Towards an Agenda* (1-23), Canberra: Australian National University Press.

(2) Systemic Issues: Gaps in Australia's Privacy Framework

This section canvasses some (but not all) of the main failings of Australia's human rights and privacy framework. It is worth noting at the outset that the *Privacy Act 1988* (Cth) is deficient compared to the new European Union General Data Protection Regulation (GDPR). Further, Australia has failed to fulfil its obligations arising under the International Covenant on Civil and Political Rights. The systemic issues that we consider in this section include an absence of comprehensive constitutional protection of human rights, no cause of action for serious invasions of privacy (i.e. a privacy tort), narrow definitions of 'personal information' and significant exemptions to the *Privacy Act 1988* (Cth), and a captive and underfunded regulator. These issues are compounded by a complete failure to meaningfully consult or consider the recommendations of civil society organisations such as the Australian Privacy Foundation.

No constitutional protection of human rights and no court of human rights in Australia

Currently in Australia there is no comprehensive constitutional protection of the general rights of citizens or a charter of human rights at the federal level,[3] which leaves citizens vulnerable to human rights infringements by both the state and other citizens.[4] In recent years Australian parliaments have demonstrated a willingness to pass laws that weaken the realisation of basic human rights such as freedom of speech and privacy.[5] As Australia lacks comprehensive constitutional protection of human rights, courts are unable to properly address instances of human rights abuses, and furthermore there is no specific court of human rights. In having a court that is solely focused on human rights, it would relieve the burden upon the High Court of Australia which currently deals with the few human rights cases that can be heard under Australian law.[6] There are some *unenforceable* human rights protections in the Australian

[3] Kirby, M. (2009). *Arguments for an Australian Charter of Rights*. Ultimo, NSW: Constitutional Education Fund of Australia. Retrieved from: https://www.michaelkirby.com.au/images/stories/speeches/2000s/2009%2B/2398.Cefa_-_Blog_-_Arguments_For_Aust.Charter_Of_Rights.pdf.
[4] Williams, G. & Reynolds, D. (2017). *A charter of rights for Australia*. Sydney, NSW: NewSouth Publishing.
[5] Homer, R. (2017, August 10th). Time to fix Australia's odd absence of rights protections, *Financial Review*. Retrieved from: https://www.afr.com/business/legal/time-to-fix-australias-odd-absence-of-rights-protections-20170809-gxt0hh.
[6] Johns, F.E. (2005). Human rights in the High Court of Australia, 1976-2003: The righting of Australian law, *Federal Law Review*, *33*(2), 287-332. Retrieved from: http://classic.austlii.edu.au/au/journals/FedLawRw/2005/10.html.

Capital Territory[7] and Victoria,[8] and the Palaszczuk Government has made a commitment to introduce a Human Rights Act in Queensland.

No cause of action for serious invasions of privacy in Australia (privacy tort)

The Australian Law Reform Commission (ALRC) has called for enhanced privacy protections, in 2008[9] and more recently in its 2014 report, 'Serious Invasions of Privacy in the Digital Era'.[10] Australians have limited available legal avenues if their privacy is breached, although they can make a complaint to Privacy Commissioner (there is currently no appointed Privacy Commissioner at the federal level). In Australia case law has followed the UK position that privacy is a species of confidence however breach of confidence has not proved itself to be as comprehensive a right as a clear right to privacy would afford. The ALRC has recommended the introduction of a privacy tort that would focus on intrusion into seclusion and misuse of private information.[11] This would be more aligned with the approaches adopted in the United States, the United Kingdom and New Zealand.[12] There are three main considerations to take into account, first, the need for the law to catch up with current technological advances (such as telephoto lenses, mobile phone cameras, the internet etc.), second, the need for the law to be adequately enforced in a way that ensures the human right to privacy is recognised (as required by Article 17 of the International Covenant Civil and Political Rights[13]), and thirdly, the recognition of privacy as a right in various international covenants and conventions that Australia is party to.[14] Further, considering the new European Union General Data Protection Regulation (GDPR) and the very active European Court of Justice, that a right to data protection (such as in the EU Charter of Fundamental Rights) would also be helpful.

---

[7] *Human Rights Act 2004* (ACT) (Austl.)
[8] *Charter of Human Rights and Responsibilities Act 2006* (Vic) (Austl.)
[9] Australian Law Reform Commission. (2008). *For your information: Australian Privacy Law and Practice Report*. Canberra, ACT: Australian Government. Retrieved from: https://www.alrc.gov.au/publications/report-108.
[10] Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era: Final report.* Canberra, ACT: Australian Government. Retrieved from: https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf.
[11] Ibid, p. 7, section 5.
[12] Butler, Des. (2005). A Tort of Invasion of Privacy in Australia?, *Melbourne University Law Review, 29*(2). Retrieved from: http://www.austlii.edu.au/au/journals/MelbULawRw/2005/11.html.
[13] Office of the High Commissioner for United Nations Human Rights. (2018). International Covenant on Civil and Political Rights. Retrieved from: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[14] Ibid.

Definitions of 'personal information' and exemptions from the Privacy Act 1988 (Cth)

The *Privacy Act 1988* (Cth) regulates the use and distribution of personal information. However, the law is limited by the definition of 'personal information'. As it defines 'personal information' as information that either includes identification of an individual or identifiable through data, it does not include peripheral data such as IP addresses, geolocation data or browsing history. Further, 'personal information' has been interpreted more narrowly than in Europe, and in Australia there is no indication of how to understand 'indirect' identification. Moreover, there are significant exemptions from the *Privacy Act 1988* (Cth). The Australian Law Reform Commission has criticised the number and scope of the exemptions.[15] For example, the *Privacy Act 1988* (Cth) does not apply to small businesses (annual turnover of less than AUS$3 million), media or political organisations.[16] There are also broad exemptions for enforcement agencies or agencies with enforcement functions. There is complete exemption for Australia's intelligence and security agencies.

Captive Regulator: What Federal Privacy Commissioner?

There has been a history of Government hostility towards the Office of the Australian Information Commissioner (OAIC) (and previous iterations of it). This has included, for example, attempts to abolish the office entirely[17], as well as severe reductions in budgetary allocations. At present, there is no dedicated Federal Privacy Commissioner appointed to complete the statutory functions of this office. Both the role of Privacy Commissioner and the Information Commissioner are currently held by Angelene Falk in a placeholder position. This has been the case since the 24th of March 2018,[18] when the previous Privacy Commissioner Timothy Pilgrim retired.

---

[15] Australian Law Reform Commission. (2008). Overview: Exemptions from the Privacy Act. In *For your information: Australian Privacy Law and Practice.* Canberra, ACT: Australian Government. Retrieved from: https://www.alrc.gov.au/publications/33.%20Overview%3A%20Exemptions%20from%20the%20Privacy%20Act/number-and-scope-exemptions

[16] Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era: Final report.* Canberra, ACT: Australian Government (p. 61, section 4.11). Retrieved from: https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf.

[17] *Freedom of Information Amendment (New Arrangements) Bill 2014* (Cth) (Austl.)

[18] Office of the Australian Information Commissioner. (2018, March 23rd). *Farewell to Timothy Pilgrim PSM - Australian Information Commissioner and Australian Privacy Commissioner*. Canberra, ACT: Australian Government. Retrieved from: https://www.oaic.gov.au/media-and-speeches/news/farewell-to-timothy-pilgrim-psm-australian-information-commissioner-and-australian-privacy-commissioner.

In 2018, mandatory data breach notification legislation was introduced which is a welcomed development in the Australian privacy framework.[19] This requires eligible entities to report eligible data breaches to Federal Privacy Commissioner.[20] However, with no current appointed Federal Privacy Commissioner combined with the very limited funding to perform statutory functions, it is not clear how effective this scheme will be. Further, there are additional concerns as regards to the mandatory data breach notification scheme, such as a reactive rather than proactive approach to information security. The scheme is also limited in scope due to the focus on 'personal information' only, which may not take into account data collected by interconnected computing devices (Internet of Things (IoT)).[21] It also does not take into account breaches that affect commercially sensitive information or other data that is not considered 'personal' as per the criticism of the narrow definition of personal information as discussed above.[22]

Successive Privacy Commissioners have also failed to make section 52 determinations and plaintiffs or defendants are unable to compel them to do so. Between 1988 and 2015 only ten determinations awarding compensation were made under Section 52 of the *Australian Privacy Act 1988* (Cth).[23] These are when the Commissioner can either dismiss a complaint after an investigation or they can find that a complaint has merit. Should the complaint be substantiated they can declare that the respondent must; a) take specific steps with a specific time period to stop and not repeat the particular conduct; b) perform an act or series of acts to redress loss and damages; c) compensate the complainant monetarily for any loss or damage; or d) decide that no further action.[24]

---

[19] Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view, *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(3), 477-495.
[20] Australian Institute of Criminology. (n.d.) *Notifiable data breaches scheme*. Canberra: Australian Government. Retrieved from: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.
[21] Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view, *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(3), 477-495.
[22] Ibid.
[23] Gunning, P. (2015, April 29th). Another privacy commissioner determination awarding compensation, *IP Whiteboard.* Retrieved from: http://ipwhiteboard.com.au/another-privacy-commissioner-determination-awarding-compensation/.
[24] Federal Register of Legislation. *Privacy Act 1988.* Retrieved from: https://www.legislation.gov.au/Details/C2018C00292.

(3) Symptomatic indicators

As a direct consequence of these wider systemic failings and significant gaps in the Australian privacy legislative and regulatory framework as described above, there have been many recent examples of the introduction (or proposed introduction) of new laws, government programs and systems that severely infringe individual privacy. The following section details some recent examples to highlight the consequences of a weak privacy framework in the Australian context. It is anticipated that without reform of the Australian privacy framework these types of symptomatic manifestations will continue to eventuate with significant impacts for individuals.

Better Management of the Social Welfare System initiative also known as 'RoboDebt'

In July 2016 the Department of Human Services - via the main welfare office Centrelink - launched an online debt raising and recovery program that automatically matched earnings reported on clients records to annual income recorded by the Australian Taxation Office.[25] In comparing these data sources, an algorithm identified discrepancies that were meant to identify 'over-payments' of social security benefits. Within the first three months of the program over 230,000 letters were sent to Centrelink clients seeking repayment for debt[26] at a rate of around 20,000 debt notices being issued every week.[27] It is estimated that around 20-38% of the debt letters issued were incorrect,[28] as a direct consequence of removing the human oversight of the process. In essence, the program resulted in the use of mismatched and inaccurate data to target thousands of welfare recipients and a lack of fair processes enabling clients to have their debt notice reviewed.[29] A subsequent parliamentary inquiry recommended suspending the system until issues of procedural justice (i.e. errors in matching, data inaccuracies and avenues for review of automated decisions) were addressed.[30] While this relates to areas of administrative

---

[25]Glenn, R. (2017). *Centrelink's automated debt raising and recovery system: A report about the Department of Human Services' online compliance intervention system for debt raising and recovery*. Brisbane, QLD: Commonwealth Ombudsman. Retrieved from: https://www.ombudsman.gov.au/__data/assets/pdf_file/0022/43528/Report-Centrelinks-automated-debt-raising-and-recovery-system-April-2017.pdf.

[26] Anonymous. (n.d.). The issue. *#NotMyDebt.* Retrieved from: https://www.notmydebt.com.au/the-issue.

[27] Ibid.

[28] Ibid.

[29] Galloway, K. (2017). Big data: A case study of disruption and government power. *Alternative Law Journal* 42(2), 89-95.

[30] Community Affairs References Committee (2017). *Senate inquiry into the design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*. Canberra: Commonwealth of Australia.

justice, the control (and correction) of personal information is of significant concern. It also raises the issue that we have few controls over automated decision-making. The Australian *Privacy Act 1988* (Cth) would benefit from similar limitations on automated decision-making and profiling as per Art. 22 of the GDPR.

Attempts to undermine encryption

Australian Prime Minister Malcolm Turnbull has announced new plans to limit the use of encryption by putting the onus on domestic and offshore technology companies to assist law enforcement and security agencies to access information (the 'not-a-backdoor *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*).[31] Former Attorney-General Brandis stated that encryption was "going to degrade if not destroy our capacity to gather and act upon intelligence" as "within a short number of years, effectively 100% of communications are going to use encryption."[32] Following this logic, the Australian Government has recently introduced a draft of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (14th August 2018).

The *Assistance and Access Bill 2018* aims to facilitate a partnership between law enforcement agencies and the communications industry, to ensure law enforcement agencies can access data. For example, the Bill allows the Director-General of Security or the chief officer of an interception agency to compel a provider to do an unlimited range of *acts or things*. That could mean anything from removing security measures to deleting messages or collecting extra data. Providers will also be required to conceal any action taken covertly by law enforcement. Further, the Attorney-General may issue a technical capability notice *directed towards ensuring that the provider is capable of giving certain types of help* to ASIO or an interception agency.

This means providers will be required to develop new ways for law enforcement to collect information. Following the release of the draft *Telecommunications and Other*

[31] Mann, M, Molnar A, and Daly, A. (2018). Undermining encryption won't work, and police have enough powers anyway. Retrieved from: https://www.policyforum.net/undermining-encryption-wont-work-police-enough-powers-anyway/.

[32] Wroe, D. (2017, June 11th). How the Turnbull government plans to access encrypted messages, *The Sydney Morning Herald.* Retrieved from: https://www.smh.com.au/politics/federal/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html.

Legislation Amendment (Assistance and Access) Bill 2018, Greens Senator Jordon Steele-John expressed concern by stating "installing software or legislating some other means to capture data as it is unencrypted on the receiving device undermines the very principle of end-to-end encryption".[33] However, as the Bill would trigger penalties for refusing to provide data to government agencies or leaking information about government activities, there are significant issues regarding transparency and accountability of these government agencies.[34]

This approach is modelled on the UK approach in the *Investigatory Powers Act 2016* (UK). The legislation in the UK and Australia's proposed bill stipulate that communications companies provide assistance to law enforcement, when compelled to do so. For example, section 253 of the UK's *Investigatory Powers Act 2016*, on 'technical capability notices' provides that the Government minister, subject to approval by a 'Judicial Commissioner', can issue a communications operator with a notice which can oblige the operator to remove 'electronic protection applied by or on behalf of that operator to any communications or data'. Similarly, Australia's *Assistance and Access Bill 2018* establishes three levels of assistance[35] that can be sought by law enforcement personnel.[36] The third and most extreme level mirrors the UK legislation and stipulates that communications companies must build capabilities in order to assist law enforcement agencies. However the Director-General of Security, the chief officer of an interception agency and the Attorney-General can issue notices without judicial oversight. This differs from how it works in the UK, where a specific judicial oversight regime was established, in addition to the introduction of an Investigatory Powers Commissioner.

At present, it is not clear whether a provider receiving a technical capacity notice would be able to provide true end-to-end encryption for its customers in the first place, in order to

---

[33] Sarraf, S. (2018, August 14th). Federal Govt. releases proposed reform to access encrypted communications, *ARN*. Retrieved from: https://www.arnnet.com.au/article/645175/federal-govt-releases-proposed-reform-encryption-laws/.
[34] Mann, M. (2018, August 15th). The devil is in the detail of government bill to enable access to communications data, *The Conversation*. Retrieved from: https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909.
[35] The first level is a "technical assistance request" which denotes voluntary assistance by a communications company. The second level is a "technical assistance notice" that compels a communications company to offer assistance that is within the bounds of their resources (e.g., decrypting data using a key already in the provider's possession).
[36] Pearce, R. (2018, August 14th). New law to force tech companies to build features for police, *Computerworld*. Retrieved from: https://www.computerworld.com.au/article/645174/new-law-force-tech-companies-build-features-police/.

ensure that the provider has a means of decrypting communications.[37] This is concerning because encryption tools are essential to protect individual privacy and critical digital infrastructure. Any attempt to weaken or undermine strong encryption poses serious risks to both information security and privacy.

MyHR

My Health Record (MyHR) is an online database of sensitive medical data established by the Australian Government that collects summary health information for all Australians who do not opt-out. There are various issues with My Health Record including the government changing the system from 'opt-in' (requiring consent to gather and share health data) to one that requires Australians to 'opt-out' during a four month period beginning 16 July 2018.[38] After the end of the 'opt-out' period only newborns or new citizens will be permitted to opt-out. There is a disturbing lack of control in regards to which health professionals can gain access to private medical data and default privacy settings. The default setting is that health professionals decide whether they should have access to private information meaning that by default, all data in a record is viewable by all health professionals. The only stipulation is that it is part of the health care of the patient. How this is to be policed is unclear. Many patients will not have the capability to monitor who has accessed their health record, something that is particularly difficult to do because the logs do not show which individuals have accessed a record, only which institutions. More alarmingly, this information can also be accessed by a wide range of non-health related agencies. For example, police and other non-health professionals can access records[39] in situations such as preventing or investigation a crime and 'protection of public revenue.' The government has announced that it intends changing the law such that a court order is required by these agencies to access a My Health Record, but it will still be without the consent of the patient. It is important to realise that the data in My Health Record is intended to be downloaded to other systems where the legislative protections of the system no longer apply. The My Health Record system is part of a larger environment of medical data with varying

[37] Smith, G (2017b). Squaring the circle of end to end encryption. Cyber Legal Eagle. Retrieved from: https://www.cyberleagle.com/2017/05/squaring-circle-of-end-to-end-encryption.html.
[38] Australian Privacy Foundation. (n.d.) *My health record: what is it, and why should I care?* Australia: Australian Privacy Foundation.
[39] *My Health Records Act 2012* (Cth) (Austl.)

degrees and levels of access control and visibility to patients, most of which are unclear to patients and health professionals alike.

Censusfail and the creation of statistical linkage keys

In December 2015 the Australian Bureau of Statistics (ABS) announced that the 2016 Census would involve the collection and retention of names and addresses to "enable a richer and dynamic statistical picture of Australia."[40] This would differ to previous administrations of the census where this information was not required. The ABS would then use this information to create a 'statistical linkage key' (SLK) that enables data linkage and longitudinal tracking creating a detailed picture of every Australian resident.[41] The APF made a submission to the Senate Inquiry following the 2016 Census regarding various privacy issues.[42] The changes to the Census and the creation of SLKs change this data collection exercise from statistical data collection to individual tracking and surveillance.[43] This constitutes a massive breach of public trust and social license to operate, especially since there was inadequate consultation with the public or civil society.

Barcodes on ballot papers

In 2017 the ABS conducted a (non-binding) survey (postal plebiscite) of all Australians listed on the Electoral Role in order to inform whether marriage laws should be amended to allow same-sex couples to marry.[44] On the survey forms that were sent via Australia Post there was a unique

[40] Australian Bureau of Statistics. (2015, December 18th). *Retention of names and addresses collected in the 2016 Census of Population and Housing*. Canberra, ACT: Australian Government. Retrieved from: http://www.abs.gov.au/websitedbs/D3310114.nsf/home/Retention+of+names+and+addresses+collected.
[41] Australian Privacy Foundation. (2016). The problems with the 2016 Census, *Australian Privacy Foundation*. Retrieved from: https://privacy.org.au/campaigns/census2016/.
[42] Galloway, K., Mann, M., & Goldenfien, J. (2018). *Joint submission to the Parliamentary Joint Committee on Intelligence and Security:* Review of the *Identity-matching Services Bill 2018* and the *Australian Passports Amendment (Identity-matching Services) Bill 2018*. Canberra: Australian Government. Retrieved from: https://eprints.qut.edu.au/116911/1/FW_APF_BiometricSubmission_Final.pdf.
[43] Australian Privacy Foundation. (2016). Inquiry: Census 2016, *Australian Privacy Foundation.* Retrieved from: https://privacy.org.au/Papers/Sen-Census-160927.pdf.
[44] Australian Bureau of Statistics. (2017). *1800.0 - Australian Marriage Law Postal Survey, 2017.* Canberra, ACT: Australian Government. Retrieved from: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/1800.0~2017~Main%20Features~Survey%20process~30; Mann, M. (2017, August 21st). Privacy and the postal plebiscite: Can the Australian Bureau of Statistics be trusted with voters' data? *Asia & The Pacific Policy Society*. Retrieved from: https://www.policyforum.net/privacy-postal-plebiscite/.

barcode enabling the ABS to link the voting paper to the eligible Australian voter who cast it.[45] This allowed the ABS to ensure that only one survey result was counted per-person, preventing individuals from returning multiple copies of their surveys in an attempt to influence the results.[46] Although the ABS made claims to the contrary, this barcoding system allowed the individual to be personally identified which is problematic when considering the politically sensitive nature of the ballot and also the potential for a chilling effect. There is also the scope for this information to be connected with other data sources, for example, the statistical linkage keys created as part of the 2016 Census.[47]

Mandatory Metadata Retention

In 2015, the Australian Government amended the T*elecommunications (Interception and Access) Act 1979 (Cth)* to introduce a statutory obligation for telecommunication and internet service providers (ISPs) to retain the metadata of their subscribers for a period of two years.[48] The retention of individuals' data who have no connection to any investigations concerning serious crime or national security is unnecessary and the government would be better served utilising targeted investigation techniques.[49]

This amendment grants law enforcement and security agencies the ability to request access to an individual's metadata without a judicial warrant.[50]Agencies who have access to this data include Australian Security Intelligence Organisation (ASIO), Australian Federal Police

---

[45] Kalisch, D.W. (2017). *Report on the conduct of the Australian Marriage Law Postal Survey 2017*. Canberra, ACT: Australian Bureau of Statistics. Retrieved from: http://www.abs.gov.au/ausstats/abs@.nsf/6630eff525d4cdc1ca25763e0075754f/7cbde85f96095fa4ca25822400162fc2/$FILE/700652_ABS_AMLPS_A4_Report_Conduct_0118_FA4.002.pdf/700652_ABS_AMLPS_A4_Report_Conduct_0118_FA4.pdf.

[46] Ibid.

[47] Mann, M. (2017, August 21st). Privacy and the postal plebiscite: Can the Australian Bureau of Statistics be trusted with voters' data? *Asia & the Pacific Policy Society.* Retrieved from: https://www.policyforum.net/privacy-postal-plebiscite/.

[48] *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth)* (Austl.). Retrieved from: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r5375.

[49] Linsay, D. (2015). *Submission to the Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*. Retrieved from: https://privacy.org.au/Papers/PJCIS-DataRetention-150119.pdf; Lane, K., Lindsay, D., & Vaile, D. (2016). *Submission to Review of Access to Retained Data in Civil Proceedings.* Australia: Australian Privacy Foundation. Retrieved from: https://www.ag.gov.au/Consultations/Documents/Access-to-telecommunications-data/Australian-Privacy-Foundation.DOCX

[50] Sarre, R. (2017). Metadata retention as a means of combating terrorism and organised crime: A perspective from Australia, *Asian Journal of Criminology, 12*(3), 167-179. Retrieved from: https://link.springer.com/article/10.1007/s11417-017-9256-7.

(AFP), and any other federal, state and territory agencies.[51] Initially there were over 60 agencies (many not concerned with matters of national security or law enforcement) that could access this information. This was then restricted to enforcement agencies, although there has been evidence of agencies funneling requests to authorised agencies and then subsequently informally sharing the information to circumvent this restriction.[52] While described as assisting law enforcement and national security efforts,[53] there is also particular concern with the data retention regime regarding the ability for agencies to access the metadata of journalists.[54] Indeed, the Australian Federal Police, by their own admission, accessed the data of a journalist without warrant (as the legislation introduced a 'safeguard' of journalist information warrants requiring law enforcement to obtain a warrant before accessing journalists' metadata). This highlights that there is not only the potential for, but actual, abuse of the data retention system. Further, there are insufficient oversight and accountability mechanisms to ensure that this does not occur.

Australia's data retention laws are in direct conflict the Court of Justice of the European Union ruling in the *Digital Rights Ireland* case that struck down the Data Retention Directive in the EU. The retention of metadata represents a disproportionate interference with individual rights and is at off with international precedent.[55] The law enables agencies to create a comprehensive digital picture of individuals' movements, contacts, interests and associations.[56]

Criminalisation of the re-identification of 'de-identified' data

In September 2016, a team of researchers from Melbourne University, namely Vanessa Teague, Chris Culnane and Ben Rubinstein, found that it was possible to re-identify practitioner details

---

[51] *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* (Cth) (Austl.)
[52] Mann, M et al. (2018). The limits of (digital) constitutionalism: Exploring the privacy- security (im)balance in Australia, *The International Communication Gazette 80 (4), 369–384. Retrieved from:* https://doi-org.ezp01.library.qut.edu.au/10.1177/1748048518757141.
[53] Ibid.
[54] Royes, L. (2017, April 29th). AFP officer accessed journalist's call records in metadata breach, *ABC News.* Retrieved from: http://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-in-metadata-breach/8480804; Suzor, N., Pappalardo, K., & McIntosh, N. (2017). The passage of Australia's data retention regime: National security; human rights, and media scrutiny, *Internet Policy Review, 6*(1), 1-16.
[55] Lane, K., Lindsay, D., & Vaile, D. (2016). *Australian Privacy Foundation: Submission to Review of Access to Retained Data in Civil Proceedings.* Australia: Australian Privacy Foundation.
[56] Sarre, R. (2017). Metadata retention as a means of combating terrorism and organised crime: A perspective from Australia, *Asian Journal of Criminology, 12*(3), 167-179. Retrieved from: https://link.springer.com/article/10.1007/s11417-017-9256-7.

within a research dataset the Department of Health had placed in its open data portal.[57] This data set had over 1 billion lines of 'de-identified' data (that was actually readily re-identifiable), with over 30 years of coverage. The researchers contacted the Department of Health to inform them of this data breach and the Department immediately removed the dataset from their website.

In response, the Government introduced the *Privacy Amendment (Re-identification Offence) Bill 2016* (Cth) that, if passed, would retroactively criminalise the re-identification of de-identified data punishable by up to 2 years imprisonment.[58] The Senate Legal and Constitutional Affairs Legislation Committee outlined various issues with the bill which, at the time of writing, is still before the Senate. These included the release of de-identified information, breadth of the Minister's discretionary powers, retrospectivity and the reversal of the burden of proof.[59]

The National Facial Biometrics Matching Capability and Identity-matching Services Bill 2018 (Cth) and Australian Passports Amendment (Identity-matching Services) Bill 2018 (Cth)

In late 2015, via an agreement made by the Council of Australian Governments (COAG), the Commonwealth government implemented a national facial recognition system—the National Facial Biometric Matching Capability, or simply the Orwellian sounding 'Capability.' This system uses existing identification documents, such e-passports, to extract and share biometric information between government databases.

In 2018, the Government introduced two bills to respond legislatively to the activities already sanctioned under COAG agreements and, in an attempt to obtain access to all state and territory driver license or roads traffic authority databases. This included the *Identity-matching Services Bill 2018* (Cth) which will authorise the Department of Home Affairs to collect, use and

---

[57] Culnane, C., Rubinstein, B., & Teague, V. (2016, September 29th). Understanding the maths is crucial for protecting privacy, *Pursuit.* Retrieved from: https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy.

[58] Brandis, G. (2016). *Privacy Amendment (Re-identification Offence) Bill Explanatory Memorandum*. Canberra: Parliament of the Commonwealth of Australia. Retrieved from: http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s1047_ems_bbb11ed5-cc19-4a1b-9e11-2e05f8a4c915/upload_pdf/497384em.pdf;fileType=application%2Fpdf; Parliament of Australia. (2016). *Privacy Amendment (Re-identification Offence) Bill 2016.* Canberra: Australian Government. Retrieved from: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1047.

[59] *Privacy Amendment (Re-identification Offence) Bill 2016* (Cth) (Austl.)

disclose identification information in order to operate the systems that will support a set of new biometric face-matching services and also the *Australian Passports Amendment (Identity-matching Services) Bill 2018* (Cth) will authorise the Minister for Foreign Affairs to disclose personal information for the purpose of participating in a service to share or match information relating to the identity of a person. The *Identity-matching Services Bill 2018* (Cth) allows information to be collected about individuals who have not been convicted of a crime, which is considered neither a legitimate nor proportionate invasion of privacy and is at odds with precedent set by the European Court of Human Rights in *S & Marper*.[60] There are a number of issues and concerns associated with the collection, sharing and use of biometric information including that they are extraordinarily privacy-invasive, highly error-prone and unreliable and discriminatory.[61] It also brings under a central federal authority, tasked with policing, migration, intelligence the richest datasets of personal information previously held at state level. Due to the limited protections in relation to biometrics information in Australia (which is defined under the Australian Privacy Principles as 'sensitive information'), and the numerous exemptions and carve outs in the *Privacy Act 1988* (Cth) as discussed above, there is a significant gap in proper governance and oversight.[62] Currently, Australia's regulations do not align with international regulatory practices, such as those in the UK which has a dedicated Biometrics Commissioner.[63]

The 'Trusted' Digital Identity Framework

The Data Transformation Agency (DTA) is responsible for leading the development of a national federated digital identity system, knowns as the Trusted Digital Identity Framework (TDIF).[64] In essence, this is an online identity system that is governed by a set of rules used to manage identity transactions.[65] The Australian government intends the TDIF will form the basis of a

---

[60] Galloway, K., Mann, M., & Goldenfien, J. (2018). Submission to the Parliamentary Joint Committee on Intelligence and Security: Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018. *FutureWise and the Australian Privacy Foundation.* Retrieved from: https://eprints.qut.edu.au/116911/1/FW_APF_BiometricSubmission_Final.pdf

[61] Ibid.

[62] Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal, 40(1), pp. 121-145.*

[63] Ibid.

[64] Digital Transformation Agency. (2018). *Overview and Glossary: Trusted Digital Identity Framework February 2018, version 1.0.* Canberra, ACT: Australian Government. Retrieved from: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-overview-and-glossary.pdf.

[65] Ibid.

federated system known as 'Govpass,' which will serve as a "one stop shop" for identity confirmation and access to online government services.[66] Govpass requires individuals to prove their identity in order to access a range of government services.[67] More alarmingly, the Govpass system will be accessed by the user through the new Facial Identification Service (as part of 'The Capability' as described immediately above), which requires an individual to take and upload a 'selfie'[68] which will then be compared to a passport or drivers license photo to confirm identity.[69] This mechanism will serve as the first part of a two-factor authentication process, the second being a code sent to either an email address or a phone number. The DTA have not yet discussed how they plan to ensure the photo taken by the website is live, or not a printed photo, but these possibilities raise obvious concerns as regards to the security of users' information. The DTA claims that privacy and the protection of personal information is at the "heart of this project"[70] but despite these reassurances there still remains serious concern about data retention and access.

Data discrimination: Targeting data collection towards minorities and vulnerable populations

There is growing recognition of the ways in which Australia's surveillance and data collection practices are targeted directly at, and significantly impact, minority and already marginalised populations, including Indigenous peoples, refugees and welfare recipients.[71] It is clear though scandals such as RoboDebt (as discussed above), regimes such as the BasicsCard,[72] Suspect Targeted Management Plans[73], the use of facial recognition by Centrelink,[74] and surveillance of

---

[66] Digital Transformation Agency. (n.d.). *Govpass*. Canberra, ACT: Australian Government. Retrieved from: https://www.dta.gov.au/what-we-do/platforms/govpass/.
[67] Ibid.
[68] Digital Transformation Agency. (2018). *Identity Proofing Requirements: Trusted Digital Identity Framework February 2018, version 1.0.* Canberra, ACT: Australian Government. Retrieved from: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-identity-proofing-requirements.pdf.
[69] Ibid.
[70] Digital Transformation Agency. (n.d.). *Govpass*. Canberra, ACT: Australian Government. Retrieved from: https://www.dta.gov.au/what-we-do/platforms/govpass/.
[71] Mann, M. & Daly, A. (2018). (Big) Data and the North-in-South: Informational Imperialism and Digital Colonialism in Australia. Special issue on Big Data from the South in *Television and New Media,* (forthcoming).
[72] Dee, M. (2013). Welfare surveillance, income management and new paternalism in Australia. *Surveillance & Society* 11(3), 272-286.
[73] Sentas, V., & Pandolfini, C. (2017). *Policing Young People in NSW: A Study of the Suspect Targeting Management Plan. A Report of the Youth Justice Coalition NSW*. Sydney: Youth Justice Coalition NSW. Retrieved from: http://www.yjc.org.au/resources/YJC-STMP-Report.pdf.
[74] Lackey, B. (2018, July 2nd). Centrelink to face-scan welfare recipients in crackdown on fraud. *Daily Mail Online*. Retrieved from: http://www.dailymail.co.uk/news/article-5907569/Centrelink-face-scan-welfare-recipients-drastic-new-crackdown-benefits-fraud.html.

public computers in remote Indigenous communities,[75] the Australian Government data practices assume somewhat of a colonial character. They are explicitly designed to target the most vulnerable and marginalised parts of our community. It is important that the Australian Government encourage, respect and promote Indigenous Data Sovereignty initiatives and associated principles and practices.[76]

[75] Rennie, E., Goldenfein, J., & Thomas, J. (2007). Internet policy and Australia's Northern Territory intervention. *Internet Policy Review,* 6(1), 1-17.
[76] See for example: Kukutai, T., & Taylor, J. (2016). Data Sovereignty for indigenous peoples: current practice and future needs. In *Indigenous Data Sovereignty: Towards an Agenda* (1-23). Canberra: Australian National University Press.

(4) Recommendations

In the context of the above systemic failings and symptomatic indicators of them, and in addition to Australian Privacy Foundation established policies on privacy[77], we suggest that the following recommendations are important areas of reform and go some of the way to addressing the systemic issues as described above:

1. Introduce an enforceable charter or bill of human rights at the federal level;
2. Introduce a privacy tort;
3. Appoint a Federal Privacy Commissioner and increase funding to the Office of the Australian Information Commission to enable them to undertake their statutory functions;
4. Implement proactive principles of privacy-by-design and data protection by design and default (as per Art. 25 of General Data Protection Regulation) rather than reactive remedial attempts (i.e. the criminalisation of the re-identification of de-identified data);
5. Consider these issues in ways that extend beyond privacy more than privacy, for example the discriminatory impacts of data collection and use practices targeted towards minority and marginalised groups or the information security impacts of weakening encrypted form of communication, and;
6. Encourage, respect and promote Indigenous Data Sovereignty initiatives and associated principles in the collection and use of information concerning Australia's Indigenous Peoples.[78]

[77] Australian Privacy Foundation. (n.d.) *Policy statements.* Retrieved from: https://privacy.org.au/policies/; Australian Privacy Foundation. (2017). *Human rights protections*. Retrieved from: https://privacy.org.au/policies/human-rights/; Australian Privacy Foundation. (n.d.) *Meta-principles for privacy protection*. Retrieved from: https://privacy.org.au/policies/meta-principles/; Australian Privacy Foundation (n.d.). *Australian privacy charter*. Retrieved from: https://privacy.org.au/about/privacycharter/.

[78] See for example: Kukutai, T., & Taylor, J. (2016). Data Sovereignty for indigenous peoples: current practice and future needs. In *Indigenous Data Sovereignty: Towards an Agenda* (1-23), Canberra: Australian National University Press.

Australian Privacy Foundation Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies https://privacy.org.au/publications/by-date/
- Media https://privacy.org.au/home/updates/
- Current Board Members https://privacy.org.au/about/contacts/
- Patron and Advisory Panel https://privacy.org.au/about/contacts/advisorypanel/

The following pages provide outlines of some of the campaigns that the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Census (2006) https://privacy.org.au/campaigns/census2006/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html

- The Media (2007-) https://privacy.org.au/campaigns/privacy-media/
- The MyHR (2012-) https://privacy.org.au/campaigns/myhr/
- The Census (2016) https://privacy.org.au/campaigns/census2016/