Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
Phone: +61 2 6277 2360
Fax: +61 2 6277 2067
pjcis@aph.gov.au

6 September 2019

Review of the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019

Genna Churches
Monika Zalnieriute
Lyria Bennett Moses
The Allens Hub for Technology, Law & Innovation
UNSW Law

About Us

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub adds breadth and depth to research on the diverse interactions among technological change, law, and legal practice. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, industry, government and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

Genna Churches is a PhD candidate at UNSW Law. Her thesis, 'The Evolution of Metadata Regulation in Australia: From Envelopes and Letters to URLs and Web Browsing', focuses on the access to, and retention of, telecommunications metadata, questioning if historical parliamentary debates and legislation of analogous technologies, such as the post and the telephone, have informed the balance between privacy protections and other social objectives in current telecommunications legislation.

Dr Monika Zalnieriute is a Research Fellow at the Allens Hub for Technology, Law & Innovation the UNSW Law, where she leads an interdisciplinary research stream on *Technologies and Rule of Law*. Monika's research explores the interplay between law, technology, and politics, and focuses on international human rights law Internet policy in the digital age.

Professor Lyria Bennett Moses is Director of the Allens Hub for Technology, Law and Innovation and a Professor in the Faculty of Law at UNSW Sydney. Lyria has been a Key Researcher and Project Leader on the Data to Decisions CRC, exploring legal and policy issues surrounding the use of data and data analytics for defence, national security and law enforcement.

About this Submission

This submission responds to the call for submissions by the Parliamentary Joint Committee on Intelligence and Security Review of the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019. As scholars working at the intersection of law and technology, we are delighted to participate in this inquiry led by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The opinions expressed in this submission are the views of the authors, and do not necessarily reflect or present the institutional views or positions of the Allens Hub or the UNSW Law.

The three sections of the submission correspond to research projects we have undertaken, in particular in relation to:

Part 1: Technologies and the Rule of Law;

Part 2: Thesis research, 'The Evolution of Metadata Regulation in Australia: From Envelopes and Letters to URLs and Web Browsing';

Part 3: Data to Decisions Co-operative Research Centre; Articulating law and policy principles for guiding Big Data usage for defence, national security and law enforcement purposes.

Rule of Law

In this section, we rely on an article some of us have written on the rule of law[1] in the context of automated decision-making.[2] This focuses on the importance of preserving the core rule of law values of accountability and transparency, predictability and consistency, and equality before the law in the face of moves to automate (fully or partially) government decision-making. While such relevant rule of law values are discussed in the Explanatory Memoranda,[3] there are still some concerns.

1.1. Transparency and Accountability

Transparency and accountability, as well as the Open Government Partnership which Australia has joined,[4] suggest that citizens are entitled to understand as much as possible about government processes and that government decision-makers are held accountable (in Australia, through responsible government and administrative law). We believe that these principles imply:

1. That inter-agency agreements and contracts with private sector providers related to the proposed systems are made public (and are required, by legislation, to be public). The submissions from the Department of Home Affairs ('Home Affairs') indicate these are important components of the governance arrangements that cannot go directly into legislation. Their transparency is thus essential to public accountability of the regime as a whole.
2. The Intergovernmental Agreement on Identity Matching Services 5 October 2017 ('IGA'),[5] envisaged under page 5 of the Identity-matching Services Bill 2019 (Cth) ('IMS Bill') which is described as viewable by the public in 2019, should be given a permanent web link which is recorded in the Bill.
3. Where possible, matters of importance to the public (including in relation to privacy) should be set out explicitly in the legislation rather than being added by subsequent regulations and rules as per cls 5(1)(n), 7(1)(f), 8(2)(q) of the IMS Bill.
4. Software used by government should be open source. In other words, we suggest that procurement of any privately provided software should specify as a requirement that the software code should not be treated as a trade secret. Where aspects of software need to remain confidential for operational or security reasons, secrecy should be minimised to that which can be justified as reasonably necessary.[6] Further, decisions to keep secret components of systems should themselves be accountable.

---

[1] On the importance of this principle generally, see International Congress of Jurists, 'The Rule of Law in a Free Society' (Report of the International Commission of Jurists, New Delhi, 1959) [1].

[2] Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'Rule of Law and Automation in Government Decision-Making' (2019) 82(3) *Modern Law Review* 425; see also Monika Zalnieriute, Lisa Burton Crawford, Janina Boughey, Lyria Bennett Moses, Sarah Logan, 'From the Rule of Law to Statute Drafting: Legal Issues for Algorithms in Government Decision-Making,' in Woodrow Barfield (ed) *Cambridge Handbook on Law and Algorithms,* (Cambridge University Press, UK, 2019).

[3] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) and Explanatory Memorandum, Australian Passports Amendment (Identity-Matching Services) Bill 2019 (Cth).

[4] https://www.opengovpartnership.org/.

[5] *Intergovernmental Agreement on Identity Matching Services*, 5 October 2017.

[6] Lyria Bennett Moses and Louis de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41 *Melbourne University Law Review* 530.

5. Where there are intellectual property rights in relation to systems or software procured, there should be a contractual licence that permits government and third party use for the purposes of evaluation.

The level of accountability required for government decisions is contextual. It would not be appropriate for the output of an automated identity-matching tool based on complex and non-explainable algorithms to have a significant impact, such as deprivation of liberty, without a human taking responsibility for and explaining the decision.[7]

1.2. Equality Before the Law

Australians are entitled to equal treatment before the law. Studies have demonstrated that facial recognition software may be less accurate in identifying women and people of colour.[8] Legislation should therefore require evaluation of software products, not only for predictive accuracy, but also for fair treatment of diverse subpopulations.

2. Proportionality

2.1. The Need for Proportionality Analysis

The proposed system and legislation should be proportionate.[9] This requires a demonstration that the legislation is reasonably necessary in pursuit of a legitimate objective and that its impact on fundamental individual rights are proportionate to this objective. In this regard, we highlight that the Parliamentary Joint Committee on Human Rights, in reporting on the Bills in 2018, outlined a number of European cases which considered the proportionality of similar schemes and similar data.[10] For example, *Digital Rights Ireland*,[11] handed down by the Court of Justice of the European Union, found that indiscriminate metadata retention of all people was a disproportionate response to the legitimate aim of protecting national security and preventing crime.[12] Similarly, indiscriminate retention of biometric data of all people, with the broad ability to access and match images for any offences, could be considered equally disproportionate.[13]

More generally, legislation in Australia that responds to national security threats has often been passed and implemented in a rushed manner.[14] In particular, discussion is often framed as a choice

---

[7] See, eg, Monika Zalnieriute and Felicity Bell, 'Technology and Judicial Role' forthcoming in Gabrielle Appleby and Andrew Lynch (eds), *The Judge, the Judiciary and the Court: Individual, Collegial and Institutional Judicial Dynamics in Australia*, (Cambridge University Press, UK, 2020); Danielle Keats Citron, 'Technological Due Process' (2008) 85 *Washington University Law Review* 1249; D K Citron and F Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 *Washington Law Review* 1.

[8] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, (2018) 81 PMLR 77; see generally Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.

[9] See further explanation of proportionality from an Australian High Court perspective in appendix document attached, part IIB.

[10] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Report 3 of 2018*, 47-48.

[11] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* [2014] ECR I-238.

[12] Ibid [56]-[58].

[13] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Report 3 of 2018*, citing these further cases: *S and Marper v United Kingdom*, European Court of Human Rights Application Nos.30562/04 and 30566/04 (2008) [119]; *NK v Netherlands*, UN Human Rights Committee, CCPR/C/120/D/2326/2013 (27 November 2017); *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414 (21 May 2009).

[14] See, eg, Monika Zalnieriute 'Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement' (2018) 81(6) *The Modern Law Review* 1046-1063; <https://newsroom.unsw.edu.au/news/law/%E2%80%98good-government%E2%80%99-gets-lost-pursuit-national-security>.

between security and freedoms.[15] This, we suggest, should be rectified with a comprehensive proportionality analysis of the proposed Face Verification Service, Face Identity Service, and all other information sharing, recording and access systems envisaged in the Bills.

2.2 Face Verification Service (FVS)

Focusing on the FVS, proportionality requires an explanation of the deficiencies of current identity verification mechanisms. The Explanatory Memorandum for the Identity-matching Services Bill 2019 (Cth) ('EM IMS Bill') justifies the FVS by citing an 'estimated annual cost of over $2.2 billion'[16] attributed to identity crime caused by the misuse of personal information. The Australian Institute of Criminology Report cited indicates that the top three misuses of personal information were to, 'obtain money from a bank account … (31.1%); to purchase something (29.7%) [credit card information]; and to file a fraudulent tax return (8.6%)'. However, the EM IMS Bill is unclear how the FVS will alleviate the problem, particularly the second category relating to the misuse of credit card information to make unauthorised purchases.[17] Further, it is unclear how the FVS is a numerically proportionate response given only 21.5 per cent of the 9,956 respondents reported misuse of their personal information at *any* time in their lives and only 8.5 per cent experienced misuse during the last 12 months.[18] Of the 8.5 per cent of respondents affected, the majority reported losses of *up to* $1000.[19] For such a small impact on a small range of individuals, the FVS appears a disproportionate response, particularly given the lack of evidence to demonstrate how the FVS will resolve these issues.[20]

The creation of new identity-matching systems should be evaluated in light of existing databases and systems, including those provided by actors such as Australia Post.[21] We recommend Home Affairs provide evidence of a significant shortfall in the way identities are currently verified, how the FVS would fill that gap, and how the FVS is a proportionate response.

2.3. Face Identity Service ('FIS')

Because the FIS can be accessed through self-authorisation by an extensive list of law enforcement agencies and other governmental organisations,[22] without any threshold of the seriousness of the offence or type of investigation, the IMS Bill is not sufficiently circumscribed to be a proportional response. Similarly, the interoperability hub[23] and National Driver Licence Facial Recognition Solution ('NDLFRS') appear to be able to receive data from several different state and federal

---

[15] See, eg, Christopher Michaelsen, 'The Proportionality Principle, Counter-terrorism Laws and Human Rights: A German–Australian Comparison' (2010) 2(1) *City University of Hong Kong Law Review* 19, 23.

[16] This estimate is made up of both direct and indirect costs and is based on Russel G Smith and Penny Jorna, Australian Institute of Criminology, *Identity Crime and Misuse in Australia: Results of the 2016 Online Survey Report* (2018).

[17] Russel G Smith and Penny Jorna, Australian Institute of Criminology, *Identity Crime and Misuse in Australia: Results of the 2016 Online Survey Report* (2018), 34; Identity-matching Services Bill 2019 cl 6(2).

[18] Ibid xxi, 33.

[19] Ibid xiv.

[20] We acknowledge the ABC news Online report regarding the theft of Drivers Licences and the potential for money lending to occur, but question if there is a more proportionate response to this type of crime and question how other jurisdictions have managed this issue, <https://www.abc.net.au/news/2019-09-06/drivers-licence-identity-theft-leaves-victims-exposed/11439668>.

[21] <https://www.digitalid.com/personal>.

[22] Identity-matching Services Bill 2019 (Cth) cl 8.

[23] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) explains 'the central system through which identification information is transmitted between entities participating in the identity-matching services', 28.

agencies both with and without consent of the individual.[24] This means that the full extent of the information to be retained, recorded, accessed or passed through the interoperability hub and NDLFRS or accessed by law enforcement agencies is not defined. We remain concerned that this data could include live feed CCTV and other information, such as images from social media, which could provide location and other more detailed information on the individual.[25] The IMS Bill's impact on the right to privacy could therefore be severe, indirectly affecting freedom of expression, freedom of association and ultimately democracy.

These impacts need to be weighed against the Bill's objectives. The EM IMS Bill describes the objective as: preventing and detecting identity fraud; law enforcement; national security; protective security; community safety; road safety; and identity verification.[26] We agree these are legitimate objectives, perhaps even agreed to under the IGA,[27] however, legitimate objectives and agreement do not necessarily mean that broad legislation such as the IMS Bill is a proportionate response. This would require additional evidence in the EM.[28]

We also note the concerns regarding facial recognition emerging from the private sector, including from companies building such software. For example, Microsoft has taken an ethical stance on providing facial recognition services to law enforcement agencies and has highlighted a number of ethical considerations which need to be resolved before the deployment of the technology.[29] In December 2018, Brad Smith, Microsoft's President described three areas which currently need to be resolved:

> First, especially in its current state of development, certain uses of facial recognition technology increase the risk of decisions and, more generally, outcomes that are biased and, in some cases, in violation of laws prohibiting discrimination.
>
> Second, the widespread use of this technology can lead to new intrusions into people's privacy.
>
> And third, the use of facial recognition technology by a government for mass surveillance can encroach on democratic freedoms.[30]

These kinds of issues are also being raised in the Australian government, including in Data61's work on developing ethical principles for AI.[31] The Committee should consider the implications of rising ethical concerns, particularly in relation to facial recognition, when reviewing this legislation.

2.4. Restrict Access to Only the Most Serious Crimes

If the Home Affairs is able to evidence deficiencies in the law which would be resolved by legislation such as the IMS Bill, then we recommend access to the interoperability hub/FIS/FVS without

---

[24] Identity-matching Services Bill 2019 (Cth) cl 17.

[25] <https://ia.acs.org.au/article/2019/government-wants-facial-recognition-database.html>; Parliamentary Joint Committee on Intelligence and Security, *Inquiry Identity-Matching Services Bill 2018 and The Australian Passports Amendment (Identity-Matching Services) Bill 2018,* Supplementary Submission No 9.

[26] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth), 9.

[27] *Intergovernmental Agreement on Identity Matching Services*, 5 October 2017.

[28] We note the findings of Russel G Smith and Penny Jorna, Australian Institute of Criminology, *Identity Crime and Misuse in Australia: Results of the 2016 Online Survey Report* (2018) but the Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth) does not explain how the IMS Bill will resolve the issue of Identity Crime, particularly credit card information usage.

[29] <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/>.

[30] <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/>.

[31] Data61, *Artificial Intelligence: Australia's Ethics Framework: A Discussion Paper* (2019).

consent of the individual[32] be restricted for only the most serious crimes and national security threats.[33] Alternatively, access to the system could be restricted through a warrant system, perhaps similar to a telecommunications interception warrant issued under the *Telecommunications (Interception and Access) Act 1979 (Cth)* ('*TIA Act*').[34]

2.5. Data Access/Recording as Permitted by External Laws

We note several exceptions throughout the Identity-matching Services Bill 2019 permitting access to, provision of, and sharing of information based existing legislation external to the IMS Bill.[35] This is similar to s 280 of the *Telecommunications (Interception and Access) Act 1979* (Cth). It has been revealed that hundreds of agencies with permission to access data external to the *Telecommunications (Interception and Access) Act 1979* (Cth) are seeking access to telecommunications data despite purported restrictions enacted in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) to reduce the number of agencies permitted to access the data.[36] We suggest that the same legal anomaly could occur under the Identity-matching Services Bill 2019[37] and, to avoid it, we recommend the inclusion of a definitive list of the external laws permitting additional access to the information.[38]

3. Good Governance

As part of the Data to Decisions Cooperative Research Centre, Lyria Bennett Moses and colleagues developed a set of high-level principles to apply to the use of Big Data systems for defence, national security and law enforcement purposes (attached as appendix). Some of these principles are already discussed in the explanatory memoranda (directly or indirectly) or in earlier parts of this submission, but increased focus is required on Principle D (integrity and reliability) and Principle E (security). In line with the Principles set out in the High Level Principles, we make a number of specific recommendations.

3.1. Evaluation and Testing

We suggest that the systems described in the draft Bills ought to be subject to rigorous evaluation and testing. This should include:

1. Evaluation of the overall predictive accuracy of comparisons between facial images or identity data (such as age and gender) and facial images being conducted by systems;
2. As mentioned in 1.2, evaluation of differential impact on diverse subpopulations;

---

[32] Consent for a FVS to gain a security clearance where an employee might consent to the verification of their image with their identity documents.

[33] See, eg, *Telecommunications (Interception and Access) Act 1979 (Cth)* Division 4—Warrants; see also Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* [2014] ECR I-238 [58]-[60].

[34] *Telecommunications (Interception and Access) Act 1979 (Cth)* Division 4—Warrants; see also Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* [2014] ECR I-238 [62].

[35] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth), 3, 41, 55.

[36] Communications Alliance, Submission No 27 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry of the Mandatory Data Retention Regime Prescribed by part 5-1a of the Telecommunications (Interception and Access) Act 1979 (Cth)* July 2019. <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime>; see amendments to *Telecommunications (Interception and Access) Act 1979 (Cth)* s 110A.

[37] Identity-matching Services Bill 2019 (Cth) cls 5(1)(j)(iii), 6(3), 7(3)(d)(ii), 21(2).

[38] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Report 3 of 2018*, 45-46.

3. Rigorous "red team" cyber security testing against attempts to improperly obtain or alter identity information or sabotage the system.

The purpose of this evaluation and testing is twofold. First, there should be minimum standards that a system should meet before deployment. Second, it is important that those using these systems (within agencies or within the private sector) are aware of the possibility of false positives and false negatives. Understanding risk is an essential first step in the context of avoiding, managing or mitigating a risk.

In addition, the system should be evaluated regularly not only against the above requirements, but also in relation to its effectiveness against statutory goals. For example, measuring the reduction of identity theft since the Act's introduction would be one way to measure the Act's effectiveness. Further, there would be concrete figures for false positives and negatives (see below on Managing error) and any security breaches (including those identified through audit monitoring). This could be made subject to the reporting to parliament in cl 28 of the IMS Bill. This could also include more granular information, such as the identity of non-government entities making requests and the terms of consent given, which could be cross-correlated with data breach reporting by those entities as part of an overall risk assessment.

3.2 Managing Error

The possibility of error should be acknowledged and managed in the legislative scheme. Even if the performance of an identity/facial/biometric matching system meets minimum metrics, it is unlikely that an identity/facial/biometric matching system will have 100% accuracy rate across all subpopulations. We note that individuals may be affected by error in a variety of ways, for example:

1. There may be a false negative in a match comparing a person's image with identity documents. This may lead to a person being refused services or employment.
2. There may be a false positive in a match between comparing two sets of identity documents (for example, licenses held in different jurisdictions) leading to an individual being denied a licence or having a licence cancelled.
3. There may be a false positive in a match comparing an alleged offender and a person's image in identity documents. This may lead to a person being arrested.
4. Individuals may have multiple identities but not in a manner that is fraudulent, for example married women may use both maiden and married names in different contexts, Chinese Australians may use Chinese and English names in different contexts, and those undergoing gender transition may try out a new name.

The main concern with 'Robodebt' was not simply that the system included false positives (creating a debt where none existed) but rather that these cases were not well managed in how the system was designed.[39] There are important questions about who bears the 'onus of proof' of establishing (in that case) that no debt exists or (in this case) that there is a false positive or false negative in the context of identity-matching. Ideally, there would be an easy-to-use, costless mechanism through which individuals could appeal an identity-finding that had impact on them personally.

3.3 Auditing

Auditing of systems is an important aspect of good governance. The IMS Bill and EM IMS Bill refers to auditing.[40] In addition to existing statutory purposes, this should capture:

[39] Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'Rule of Law and Automation in Government Decision-Making' (2019) 82(3) *Modern Law Review* 425.

[40] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth), 25 [147].

1. The identity of Home Affairs employees accessing identity information at particular times; and
2. The identity of individuals (with affiliations) making requests through the system, including information relating to compliance with statutory requirements.

Individuals who misuse the system should not only be criminally liable but should also be liable, along with their employers, to compensate individuals and organisations harmed through such misuse. Both criminal and civil liability should relate not only to improperly obtaining information but also actions that impact on data integrity or the system's operations as a whole. This needs to go beyond the minimal civil protections in the *Privacy Act 1988* (which, where it applies, avoids the requirements in cl 7(4)(c) of the IMS Bill). It is also odd that the Minister's rules cannot create such civil liability under cl 30(2)(a) of the IMS Bill.

3.4 Consent

As noted above, privacy is an important right impacted by the proposed legislation. One mechanism used in the legislation to protect the privacy of individuals is a requirement for individual consent in some circumstances. This includes express and implied consent.[41] The ACCC has recently noted that consent is often meaningless in practice, particularly given unequal bargaining power.[42] A robust definition of consent is required, as recommended by the ACCC.[43] In addition, individuals should be informed when their identification information has been accessed by local government or non-government entities.[44] This will provide an opportunity for individuals to complain and, ideally, seek a remedy where there is no *actual* consent.[45]

3.5 Data Governance

We further suggest that data governance arrangements for the distributed system and allocation of responsibilities should be clarified. The following matters, in particular, should be clarified:

- Responsibility for data integrity and security (including in the context of liability for harm);
- Responsibility for integrity of the operation of the system as a whole (including responses to alleged false positives and false negatives);
- Responsibility for meeting other statutory obligations (such as under Freedom of Information and subpoena laws) for those with access to data (Home Affairs) as well as those with control over datasets (current data holders);
- Clear and transparent oversight of the system by an independent body (such as IGIS, the Commonwealth Ombudsman or a newly created body); and

[41] Explanatory Memorandum, Identity-Matching Services Bill 2019 (Cth), 36 [232].

[42] ACCC, *Digital Platforms Inquiry – Final Report* (2019) 23.

[43] Ibid recommendation 16(c).

[44] See, eg, Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitlinger and Others* [2014] ECR I-238 [66]; the risk of abuse and unlawful access.

[45] Providing a right to an effective remedy; *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, ratified Australia 13 November 1980, 999 UNTS 171 (entered into force 23 March 1976) art 2.3.

- No private software provider should be able to gain access to the identity information held within the system. There is a need, in particular, to avoid the controversy surrounding the use by DeepMind of British health information for commercial purposes.[46]

Whilst we note the inclusion of reporting mechanisms in the Identity-matching Services Bill 2019,[47] we highlight that the reporting mechanisms in place under s 186 of the *TIA Act* have not had the same impact as the ability for the Commonwealth Ombudsman to conduct reviews of access to telecommunications data under 186B of the *TIA Act*.[48] Considering the Ombudsman's successes in highlighting unlawful access to telecommunications data,[49] we recommend that if the IMS Bill is recommended to be passed, it be amended to include review by the Commonwealth Ombudsman.

Conclusion

The proposed legislation has important implications for Australians. It is essential that the Australian government comply with the rule of law, act proportionately, and exercise good governance in relation to the systems that will be established. These systems need to be scrutinised and monitored by parliament through carefully drafted legislation and ongoing oversight. We hope that our suggestions go some way towards achieving this.

[46] Information Commissioner's Office (UK), 'Royal Free - Google DeepMind trial failed to comply with data protection law' (3 July 2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law.

[47] Identity-matching Services Bill 2019 cl 29.

[48] Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data Under Chapters 3 and 4 Of Telecommunications (Interception and Access) Act 1979 (Cth)* (2018).

[49] Ibid.

Appendix

Project D: Articulating law and policy principles for guiding Big Data usage for defence, national security and law enforcement purposes

Policy Report:
High Level Principles

Authors:
Professor Lyria Bennett Moses, Project Leader, UNSW Law
Professor Louis de Koker, Program Lead, La Trobe University
Dr Sarah Logan, Lecturer, Australian National University

With thanks to:

The broader Data to Decisions CRC Law and Policy team (2014-2019).

Stakeholders who contributed and provided feedback on earlier drafts of this document, both in workshops and through correspondence.

11 June 2019

I. Introduction

This report identifies a set of high-level principles to guide the development of recommendations concerning a regulatory framework for the appropriate use of Big Data for defence, national security and law enforcement (**DNSLE**) purposes. The report, compiled by the Law and Policy Program of the Data to Decisions Cooperative Research Centre (D2D CRC), reflects insights gained in the course of a five-year program of research in a number of research projects on specific aspects of the use of Big Data in national security and law enforcement.

1. Objective of this report

The objective of this report is to articulate the Law and Policy Program's understanding of the key governing principles as it evolved in accordance with new literature and our own research findings throughout the D2D CRC. These are principles against which we believe:

- existing and proposed legal frameworks can be assessed, reflective of emerging "best practice" in relation to matters such as privacy and data protection, record-keeping, data governance, and protective security; and
- existing and proposed socio-technical systems used for data processing (**systems**), including design specifications and procurement standards, can be assessed in line with a compliance through design approach in relation to privacy and data protection, record-keeping, data governance, and protective security.

The report is being prepared near the conclusion of the Data to Decisions CRC in order to share what has been learnt by researchers in the D2D CRC Law and Policy Program, in particular through projects and activities conducted with stakeholders in DNSLE and policy agencies. There are several factors that, in combination, suggest the importance of this exercise:

- New data science techniques create an opportunity to gain insights from Big Data. These methods create new opportunities but also generate new risks and harms, particularly in relation to privacy, fair and equal treatment of individuals, and abuse of power.
- The D2D CRC has developed new Big Data tools for DNSLE agencies; the role of the Law and Policy program includes assessing legal, ethical and policy issues associated with the development and use of such tools. The role of the Law and Policy program included initiating and facilitating conversations about these issues with D2D CRC management and technical researchers.
- The Law and Policy program worked directly with DNSLE and policy agencies on a range of projects relating to the use of Big Data for DNSLE purposes. These included projects around identity assurance, information sharing, data governance, the use of "open source" data, and compliance through design. The role of the Law and Policy Program in these projects included analysis of existing regulatory frameworks and developing proposals for reform.
- Specific decisions about what laws and control measures ought to apply, both in the specific context of the use of Big Data for DNSLE purposes, and more broadly, are often controversial. However, there is potential for greater consensus at the high level at which these principles are drafted.
- It is desirable that conversations around the appropriateness of existing regulatory frameworks and the development of reform proposals be based on a common understanding of the principles on the basis of which such arguments are made. Especially where reasonable minds may differ on the

appropriate high level principles to be applied, it is important to be explicit about which principles have been deployed.

The principles are authored by researchers in the final research project of the Law and Policy Program of the Data to Decisions CRC. They have not been adopted, directly or by implication, by the Australian government or by any of the DNSLE agencies participating in the D2D CRC. While these principles are informed by earlier drafts produced by the Law and Policy program, the current version reflects the opinions of the authors of this document and not necessarily all researchers who have worked on D2D CRC projects over the period 2014-2019.

These principles are not intended to duplicate or replace aspects of existing regulatory frameworks or technical standards, nor are they intended as articulating a new regulatory framework. For example, they do not interact directly with legislation such as the *Privacy Act 1988* (Cth) and do not provide a similar level of detail. They operate at a "high level", providing a normative framework against which regulatory frameworks and technical standards can be evaluated in the context of the use of Big Data for DNSLE purposes. But they do not attempt to prescribe things that agencies can or cannot do: rules governing agency practices are found in legislation, regulations, inter-agency agreements, mandated standards, and elsewhere. This report is not itself a regulatory instrument, and there is no proposal that it become one.

These principles have been developed with the Australian context in mind, but with an eye to learning from similar exercises in comparable jurisdictions studied throughout the Law and Policy Program.[50]

The primary audience thus comprises:

- policy agencies (responsible for legislation regulating data processing by DSNLE agencies),
- those responsible for systems design specifications and procurement (adopting a compliance through design approach, these systems are themselves regulatory), and
- civil society (as a basis for support or critique of the existing regulatory framework by reference to agreed principles)

Data analysts in DSNLE agencies are *not* the primary audience for this document. These analysts are expected to comply with existing law and use systems as designed. Because the principles are directed at the regulatory framework and not at specific actors (such as data analysts working in DNSLE agencies), they are not properly described as ethical guidelines. There are ethical guidelines that have been proposed in related contexts,[51] but the purpose of these high level principles is distinct.

The principles are not intended as comprehensive. The reach of the High Principles below is limited by the research projects on which the Law and Policy program has been engaged and the topics we have had the opportunity to explore. Further, there is much more that can be said about principles such as transparency and proportionality. This document is however intended to provide a normative framework for evaluation; more detailed analysis can be found in the reports and publications of the Law and Policy Program of the D2D CRC (and elsewhere in the academic literature).

High level principles exist in a culture of interpretation. They might be interpreted as broad and constraining or as a compliance requirement to be overcome. Should these principles be adopted, it is important that they are interpreted in light of rule of law values and with a mindset geared towards stewardship as opposed to minimalist or technical compliance.

---

[50] For example, see *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, RUSI, 2015.

[51] Eg Data61, *Artificial Intelligence: Australia's Ethics Framework: A Discussion Paper* (2019), Accenture, *Universal principles of data ethics*; Data Science Organisation, *Code of Conduct*.

This document remained live throughout the duration of the D2D CRC, with amendments made and communicated as insight deepened or consensus developed. It was presented in final form at the end of the D2D CRC, along with specific recommendations arising from D2D CRC Law and Policy projects.

Throughout the D2D CRC and specifically towards its end, we engaged with government agencies (including the Attorney General's Department), civil society organisations and within academia. Although such engagement enhanced the insights underpinning the report, not all suggestions have been adopted and thus mere engagement with the drafters (specifically by government agencies and civil society organisations) does not amount to their endorsement of the principles.

2. Terminology

Big Data is a controversial term, but is intended here to refer to large, diverse or evolving[52] data collections that may be processed (data processing defined below). While we acknowledge the importance of questions relating to the sharing of specific information about an individual or a small number of individuals between agencies in response to a specific request, and we are mindful that complex data analysis can also be carried out with smaller data sets, this report focuses on larger or "bulk" data sets. This decision is not justified normatively (and terminology in this area continues to shift), but to ensure alignment with the scope of D2D CRC research projects conducted by the Law and Policy program.

The **information lifecycle**,[53] for purposes of this report, includes:

(a) Collection of data for DNSLE purposes,
(b) Access to data by DNSLE agencies (including government data, privately held data (held in Australia or overseas), data held by foreign governments accessible through partnerships, and publicly available data), including decryption of encrypted data where appropriate,
(c) Data merger, matching or linking,
(d) Data aggregation
(e) Correcting data (including data scrubbing),
(f) Facilitation of data discovery (for example, by allowing DNSLE agencies to search over data held centrally or in another agency),
(g) Disclosure or "sharing" of data (within government, within Australia and with foreign governments/agencies), including open publication of data (where permitted, including through treaties and partnerships),
(h) Data analysis,
(i) Data retention and storage (within government or mandated by government in accordance with relevant records retention and management policies), and
(j) Data erasure.

Personal information is defined in *Privacy Act 1988* s 6(1).

Processing of data or information includes creation, access, collection, storage, scrubbing, linking, merging, altering, sharing, aggregating, searching, discovering or otherwise using data/information (see "information lifecycle" above, but noting erasure is not "processing" in our definition). Data can also be derived from other data, or in other words "created" from data, as well as from sensors and individuals. The processing of data

[52] Referring to the three V's – volume, variety, velocity. See Pompeu Casanovas, Louis de Koker, Danuta Mendelson and David Watts, 'Regulation of Big Data: Perspectives on Strategy, Policy, Law, and Privacy' (2017) 7 *Health and Technology* 335, 336.

[53] The definition here is broad in order to clarify the scope of the Policy Paper. By listing activities here, we are not implying endorsement, either generally or in specific cases. We are not considering some activities, in particular de-identification and re-identification, within this Policy Paper.

will often include specific techniques such as machine learning, although the focus here is on data practices rather than on what is sometimes described as artificial intelligence " (although there is obviously overlap).

Proportionality[54] is a comparative relation of one thing to another as respects magnitude, quantity or degree. In relation to fundamental rights, the Australian High Court,[55] employs proportionality analysis to "ascertain the rationality and reasonableness" [56] of the restriction on the fundamental right: the greater the restriction on the fundamental right, the more important must be the public interest purpose of the legislation for the proposed restrictive measure to be proportionate.

Adapted to the context of these principles, proportionality analysis comprises of the following components/questions:

1. Whether the legislation or a particular measure/action by the DNSLE agency that will result in limiting a fundamental right pursues a legitimate specific objective (one that does not impinge upon the functionality of the system of representative government) of sufficient importance to warrant limiting this right;
2. If so, whether the proposed means (including processing of data) in service of the objective are rationally connected (suitable) to the specific objective;
3. Whether the rights-limiting means in service of the objective are necessary to achieve that objective. In other words, are there alternative reasonably practicable means of achieving the same purpose without impairing, or significantly impairing the fundamental right. For example, an alternative reasonably practical means may include restricting the access to or adopting a more narrowly focussed collection of data. If, and only if, these alternative measures are identical in their effects to the measures which have been chosen, the proposed measure is not necessary.
4. Whether the proposed measure involves adequate balance between the importance of the law's proper purpose to be furthered by the restrictive measure and the extent of the restriction it thereby imposes on the fundamental right. The balancing process for ascertaining proportionality requires examination and evaluation of evidence but does not include determining policy or fiscal choices.

This report adopts "proportionality" as a guiding principle for understanding the extent to which Big Data should be used for DNSLE purposes. Data practices have the potential to infringe fundamental rights inherent in the rule of law and international human rights, including the right to privacy, the right to equal treatment under the law, and the right to protection from abuse of power. Any impact on these fundamental rights should be proportionate to public interest purposes associated with the use of Big Data for DNSLE purposes.

Appropriate in this document means reasonable and justifiable in an open and democratic society in light of anticipated benefits, costs and risks for affected parties.

Regulatory framework, for the purposes of this report, is a framework comprising a sustained and focussed attempt intended to produce a broadly defined outcome or outcomes directed at a sphere of social activity

[54] This approach to proportionality is informed by the High Court's decisions in *Unions NSW v New South Wales* [2013] HCA 58; at [55]-[56]; *Murphy v Electoral Commissioner* [2016] HCA 36 at [64]-[65], *McCloy v New South Wales* [2015] HCA 34 at [87] and [67]. The discussion of proportionality was contributed by Professor Danuta Mendelson.

[55] "The term 'proportionality' in Australian law describes a class of criteria which have been developed by this Court [the High Court of Australia] over many years to determine whether legislative or administrative acts are within the constitutional or legislative grant of power under which they purport to be done." *McCloy v New South Wales* [2015] HCA 34 at [3] per French CJ, Kiefel, Bell and Keane JJ.

[56] *Murphy v Electoral Commissioner* [2016] HCA 36 at [65] per Kiefel J.

according to defined standards or purposes that affect others in order to address a collective concern or problem,[57] and can include laws, formal regulations, policies, procedures and elements of technological design.

II. High level principles on the use of Big Data for DNSLE purposes

The use of Big Data for DNSLE purposes offers new opportunities. It may improve the efficiency of national security and law enforcement analysis, possibly leading to faster and better insights, including by identifying and assessing potential threats. It also creates risks, particularly for data subjects, for example relating to over-collection of data, the use of inaccurate or incompatible data, the use of inappropriate, biased or inaccurate analysis, the generation of unjustified or untested inferences, and (as a result) the making of unfair or unjustified decisions, potentially involving differential treatment of people with particular innate characteristics.[58] Current rules are not necessarily designed to maximise these opportunities and detect, investigate, avoid, prevent and/or mitigate the risks effectively. A regulatory framework that reflects these high-level principles collectively and comprehensively will, in the view of the Law and Policy program, enable the use of appropriate technologies while providing important protections and oversight.

A. Justification as reasonably necessary

DSNLE agencies should only process personal information in circumstances justified as reasonably necessary to achieve defined and legitimate DNSLE objectives.

This objective can be achieved by limiting agency powers in line with agency functions as well as procedures and processes that require explicit justifications for data processing. Personal information should not be retained for longer than can be justified as reasonably necessary.

B. Proportionality

The design, operation and management of all elements of the information lifecycle, including the processing of Big Data for DNSLE purposes, must be proportionate.

Practices (in particular the use of Big Data for DNSLE purposes) and controls (through law, regulation, design and processes) must be proportionate within the meaning set out above and in line with the justification referred to in Principle A. Measurement of the likelihood and severity of any risk to data subjects needs to done with an understanding of context, including the category of data subject (offender, suspect, victim, witness, etc), nature of the data and the manner of processing.

C. Clarity, consistency and predictability

The regulatory framework should be clear and consistent and the application of its rules should be predictable in foreseeable circumstances.

The regulatory framework should be easy to navigate. It should be terminologically consistent (to the extent possible across jurisdictions), logically consistent (for example, not simultaneously prohibiting and requiring a particular activity) and normatively consistent (for example, not making arbitrary distinctions that lack normative justification). Rules should be broad and agile enough to operate in a dynamic environment while

[57] Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2 *Regulation and Governance* 137, 139; Karen Yeung, 'Are Human Biomedical Interventions Legitimate Regulatory Policy Instruments?' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook on the Law and Regulation of Technology* (2017) 823, 834-5.

[58] Opportunities and risks are outlined in reports of the D2D CRC project entitled 'Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law'.

being specific enough to avoid ambiguity, and so maintain auditability. Secret interpretations that deviate from plain language understandings or ordinary interpretations of a statutory provision would not be considered predictable for the purposes of this Principle.

D. Integrity and reliability

Integrity and reliability of data and analysis should be supported by law, regulation and systems design.

The regulatory framework and design specifications should, so far as is possible, support:

- the integrity of data collected, retained and accessed by government for DNSLE purposes, and
- the reliability of analytical and decision-making uses of such data and systems in light of data integrity and context of use (including the potential for harm or disparate impact).

Where integrity of data or techniques is assessed as low, so that inferences drawn therefrom would be unreliable, decisions about retention or use should reflect that fact.

E. Security

Data and systems must be protected from illegitimate access and use.

The security of relevant data and systems, both within and outside DNSLE agencies, must be kept safe from internal and external security breaches in line with the sensitivity of data held and existing legal requirements and technical standards. In particular, access should be limited to appropriately authorised and trained personnel. Technical, management and governance measures must include procedures empowering individuals to report concerns or breaches internally and require appropriate reporting to oversight agencies and regulators, and, where appropriate (and after internal and oversight mechanisms are utilised), alerting individuals and organisations affected by an adverse event.

F. Accountability and Explainability

Laws, regulations and systems should ensure the accountability of DNSLE agencies and officers.

Systems should be designed so that access to data and analysis of data is tracked, recorded and audited for justification, security and intrusiveness, both internally and through relevant forms of oversight (executive, independent, Ministerial). Compliance by Design principles should be implemented to ensure that systems operate in compliance with legal requirements. Where appropriate, Compliance through Design[59] approaches should support human decision-takers. Decisions made on the basis of inferences drawn from data processing should be subject to appropriate internal governance and auditing as well as effective, independent and Ministerial oversight and accountability. Similarly, decisions on design specifications for systems deployed need to be justified with reference to purpose, capabilities, limitations and risks, and always be subject to oversight. Auditing, oversight and accountability mechanisms and their enforcement need to be appropriately resourced (including in terms of technical expertise) and backed by appropriate sanctions.

Human decision-makers should remain accountable for decisions of DNSLE agencies that produce significant adverse legal or practical effects for individuals. Where decisions are based on inferences drawn from data processing, accountability requires that decision-makers (including, where relevant, oversight bodies and judges) have a sufficient understanding of the provenance, meaning and quality of data, of any sources of incompatibility among the meanings and qualities of the different sources of data, of the applicability of the analytical procedures to the relevant kinds of data, and of any biases or other weaknesses in the analytic process. This requirement of explainability may be achieved through a variety of means, including choice of

[59] Pompeu Casanovas, Jorge González-Conejero and Louis de Koker, 'Legal Compliance by Design (LCbD) and Through Design (LCtD): Preliminary Survey' in Víctor Rodríguez-Doncel, Pompeu Casanovas and Jorge González-Conejero (eds), *Technologies for Regulatory Compliance* (CEUR Workshop Proceedings vol 2049, 2018) 33.

process (for example, explainable artificial intelligence) or evaluation and testing (including for particular biases) of inputs and outputs of otherwise opaque processes.

Accountability is essential to protect individuals adversely affected by DNSLE decisions based on inferences drawn from data processing. Executive, independent and Ministerial accountability are also necessary to promote trustworthiness and, hence, public confidence in DNSLE agencies.

G. Review

Laws, regulations, processes and systems should be reviewed initially, regularly and when warranted.

Principles, rules, processes and systems should be subject to regular, transparent review, and be reviewed, when warranted, internally and by independent external bodies. The reviews need to consider the alignment with DNSLE objectives (see Principle A), alignment with other principles, the impact of new developments in technology, potential for abuse. They should provide evidence (including through evaluation) as to whether the system delivers intended results effectively, efficiently, reliably and is proportionate to impacts on civil liberties, legal rights, and other individual and collective interests. The nature of such review is contextual but should include a privacy impact assessment and community engagement where relevant. Reviews will be warranted when there is a specific risk or evidence of abuse, and should result in improved mitigation of such risks in the future. Reviews, evidence and evaluations should feed back into the strategy and methods of DNSLE agencies, the design of the regulatory framework and specific future application of all other Principles.

H. Transparency

The regulatory framework should support openness and transparency while safeguarding operational secrecy, where reasonably necessary.

Agency powers regarding the collection of, access to and use of Big Data, justifications for those powers, and the regulatory framework governing the use of those powers should be clear (a) to those with an interest in policy- and rule-making (including the public) to facilitate public debate and democratic accountability, and (b) to those potentially adversely affected by decisions. Operational secrecy should be limited to circumstances in which it is reasonably necessary, and decisions to keep information secret should be accountable (see Principle F).[60] Procurement should have regard to (1) the extent to which software can form part of an accountable decision-making system (Principle F), and (2) any contractual terms or intellectual property rights that restrict transparency (beyond the need for operational secrecy).

Transparency is an enabling Principle, facilitating evaluation of practices and regulatory frameworks against other Principles.

[60] Lyria Bennett Moses and Louis de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41(2) *Melbourne University Law Review* 530, 542-4.