



AUSTRALIAN
LAWYERS
FOR
HUMAN RIGHTS

5 November 2019

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

The Privacy and Responsible Information Sharing team
Public Sector Reform Unit, Department of the Premier and Cabinet
Locked Bag 3001
West Perth WA 6872

By email: email withheld

Dear The Privacy and Responsible Information Sharing team

Response to Government of Western Australia's, 'Privacy and Information Sharing for the Western Australian Public Sector: Discussion Paper'

Australian Lawyers for Human Rights (**ALHR**) is grateful for the opportunity to provide this submission in relation to the Government of Western Australia's, 'Privacy and Information Sharing for the Western Australian Public Sector: Discussion Paper.'

About ALHR

ALHR was established in 1993 and is a national association of Australian solicitors, barristers, academics, judicial officers and law students who practise and promote international human rights law in Australia. ALHR has active and engaged National, State and Territory committees and specialist thematic committees. Through advocacy, media engagement, education, networking, research and training, ALHR promotes, practices and protects universally accepted standards of human rights throughout Australia and overseas.

1. Background

- 1.1. Pursuant to the rule of legality, Australian legislation should adhere to international human rights standards, unless legislation contains clear and unambiguous language otherwise.
- 1.2. Furthermore, the Australian parliament should properly abide by its binding obligations to the international community in accordance with the seven core international human rights treaties and conventions that it has signed and ratified, according to the principle of good faith, and State Parliaments should likewise abide by Australia's human rights obligations.

- 1.3. **ALHR** endorses the views of the Parliamentary Joint Committee on Human Rights (**PJCHR**) expressed in Guidance Note 1 of December 2014¹ as to the nature of Australia’s human, civil and political rights obligations, and agrees that the inclusion of human rights ‘safeguards’ in Commonwealth legislation is directly relevant to Australia’s compliance with those obligations.
- 1.4. Generally, behaviour should not be protected by Australian law where that behaviour itself infringes on other human rights. There is no hierarchy of human rights. Human rights are all interrelated, interdependent and indivisible. Where protection for particular behaviour is sought, the extent to which that behaviour is compatible with the enjoyment of rights by others is relevant.
- 1.5. It is only through holding all behaviours up to the standard of international human rights law that one can address harmful and discriminatory practices.
- 1.6. Legislation should reflect an **appropriate and proportionate** response to the harms it is purporting to address, and adherence to international human rights law and standards is an important indicator of proportionality.²
- 1.7. While the introduction of a legislative framework for Western Australia is encouraging, a framework based on the *Privacy Act 1988* (Cth) (**the Privacy Act**) and the Australian Privacy Principles (**APPs**) alone is not likely to be adequate to effectively protect human rights in respect to privacy and data sharing.
- 1.8. The Privacy Act regulates the collection and use of personal information through thirteen ‘Australian Privacy Principles’ but does not address surveillance, which is permitted for law enforcement agencies under various legislation.³ Nor does it apply to Commonwealth intelligence agencies⁴ or State or Territory government agencies such as the NSW Police Force.⁵ Some States

¹ Commonwealth of Australia, Parliamentary Joint Committee on Human Rights, Guidance Note 1: Drafting Statements of Compatibility, December 2014, see also previous Practice Note 1 which was replaced by the Guidance Note. Available at < <https://www.humanrights.gov.au/parliamentary-joint-committee-human-rights>>.

² See generally Law Council of Australia, ‘Anti-Terrorism Reform Project’ (October 2013). Available at: <http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/a-z-docs/Oct%202013%20Update%20-%20Anti-Terrorism%20Reform%20Project.pdf>>

³ The States have their own legislation. Relevant Commonwealth legislation includes: Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) (‘TIA Act’) (relating to data retention obligations), the *Telecommunications Act 1997* (Cth), the *Intelligence Services Act 2001* (Cth), the *Surveillance Devices Act 2004* (Cth) and the *Australian Federal Police Act 1979* (Cth), s 60A(2) of which allows federal police recording and retaining of personal information. The AFP is legally permitted to collect facial images where it is ‘reasonably necessary to fulfil its policing functions’ and share them when it is ‘reasonably necessary for law enforcement purposes’ Attorney-General’s Department (Cth), ‘Face Matching Services’ (Fact Sheet) 3 .

⁴ Not covered are: the Office of National Assessments, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate, the Defence Intelligence Organisation, the Australian Geospatial-Intelligence Organisation. Office of the Australian Information Commissioner, “Which law enforcement agencies are covered by the Privacy Act?” at <https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement>.

⁵ Office of the Australian Information Commissioner, “Which law enforcement agencies are covered by the Privacy Act?” at <https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillancephotos/resources-on-law-enforcement>. It should be noted that the Australian Government Agencies Privacy Code (available at <https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacyaustralian-government-agencies-governance-app-code-2017>) was registered on 27 October 2017 and came into effect on 1 July 2018. It is a relatively short document which sets out specific requirements for government agencies to which the Privacy Act applies to assist them in adopting a best practice approach to privacy governance.

have privacy legislation that regulates use of personal information by State and local government agencies,⁶ in some cases involving criminal sanctions.⁷

- 1.9. Even where the Privacy Act does cover law enforcement agencies, there are many exemptions. And the Privacy Act provides for only limited civil redress, by way of complaints to the Australian Information Commissioner
- 1.10. ALHR submits that it is relevant to note the fact that Australia is the only Western liberal democracy without a federal Human Rights Act or Bill of Rights. Unlike Victoria, the Australian Capital Territory and Queensland, Western Australia does not yet have its own Human Rights Act. Western Australia does not therefore have a human rights framework to protect digital rights. Western Australians therefore live without the human rights protections established by the *The Charter of Human Rights and Responsibilities Act 2006 (Vic)*, the *Human Rights Act 2004 (ACT)* and the *Human Rights Act 2019 (Qld)*, and similar instruments that protect the human rights of others in comparable countries across the Western world.

2. Privacy and data sharing

- 2.1. Privacy is a fundamental human right recognized in the *UN Declaration of Human Rights*,⁸ the *International Covenant on Civil and Political Rights (ICCPR)*, the UN Principles on Personal Data Protection and Privacy and in many other international and regional treaties. Privacy is “at the heart of the most basic understandings of human dignity”,⁹ and is “known in all human societies and cultures at all stages of development.”¹⁰
- 2.2. As technology and data sharing capacities are constantly evolving, privacy “has become one of the most important human rights issues of the modern age.”¹¹
- 2.3. There are many aspects of privacy, and indeed it has been said that “in one sense, all human rights are aspects of the right to privacy.”¹²
- 2.4. “Information privacy” or “data protection” is a recognised subset of privacy¹³ and it is this type of privacy that is primarily affected by the proposed actions by the Western Australian Government

⁶ Privacy and Personal Information Protection Act 1998 (NSW); Information Privacy Act 2009 (Qld); Premier and Cabinet Circular No 12 (SA); Personal Information Protection Act 2004 (Tas); Information Privacy Act 2000 (Vic); Information Privacy Act 2014 (ACT); Information Act (NT).

⁷ Under s 62 of the Privacy and Personal Information Protection Act 1998 (NSW) the unauthorised or corrupt use or disclosure by a public official of personal information obtained through their official functions is an offence punishable by up to 100 penalty units or imprisonment for up to two years.

⁸ Article 12 states: “No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.”

⁹ Carly Nyst ‘Two sides of the same coin – the right to privacy and freedom of expression.’ Privacy International (February 2, 2018). Available at: < <https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression>>

¹⁰ United Nations Office of the High Commissioner Human Rights, ‘Report of the Special Rapporteur on the right to Privacy,’ (9 March 2016) Available at: < <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21248&LangID=E>>

¹¹ Privacy International, Privacy and Human Rights: an International Survey of Laws and Practice, available at Global Internet Liberty Campaign. Available at: < <http://gilc.org/privacy/survey/intro.html>>.

¹² Fernando Volio, ‘Legal personality, privacy and the family’ in Henkin (ed) *The International Bill of Rights*, New York, Columbia University Press, 1981, quoted in Privacy International, op cit. 6.

in its discussion paper titled “*Privacy and Information Sharing for the Western Australian Public Sector*” (**Discussion Paper**).

- 2.5. The general principles of data privacy adopted in the United States and most European countries include that personal information should be:
 - (a) obtained fairly and lawfully;
 - (b) used only for the original specified purpose, or for an ancillary purpose which is adequate, relevant and not excessive;
 - (c) kept accurate and up to date; and
 - (d) destroyed after its purpose is completed.¹⁴
- 2.6. While Australia is bound by the Commonwealth *Privacy Act* which contains the APPs, that legislation does not cover all the aspects of privacy. In particular, there is no tort of privacy and the common law provides minimal protection.¹⁵

3. General points about the Discussion Paper

- 3.1. The human right to privacy should be respected, protected and upheld by the Western Australian Government in developing responsible whole-of-sector approaches to information sharing.
- 3.2. Ideally, state privacy legislation would encourage transparency in the Western Australian Government’s use of information and provide privacy protections.
- 3.3. In a suboptimal situation, and in the absence of a human rights framework, privacy legislation can enable government intrusion into the privacy of individuals and the misuse of individuals’ data, including substantial infringements upon individuals’ privacy rights being given away by government in the name of security, and doors being left open for those same privacy infringements to be ‘monetised’ for commercial purposes (as is currently contemplated in some current Commonwealth legislation).
- 3.4. The Western Australian Government must act in good faith and consistently with Australia’s international legal obligations in enacting privacy legislation.. As many commentators have noted, it would be naïve to consider that all governments around the world will act in good faith once they have access to data pertaining to individuals, and act in the best interests of those individuals.¹⁶ It is therefore all the more incumbent upon the Western Australian Government to ensure appropriate human rights safeguards are built into legislation and policy that raises privacy issues.
- 3.5. Without information beyond what is contained in the Discussion Paper, it is difficult to assess whether the Western Australian Government’s approach within privacy legislation itself will accurately safeguard human rights. We refer to our discussion of the limitations of current protections in section 1 above.

¹³ <<https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/1-introduction-to-the-inquiry-5/the-meaning-of-privacy/>>

¹⁴ Op cit. 6

¹⁵ See further Tamsin Clarke, *Privacy Principles*, in Digital Rights Watch, ‘State of Digital Rights’ (2018), p. 14. Available at: <<https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Web.pdf>>

¹⁶ See further: Zeynep Tufekci and Seth Stephens-Davidowicz, ‘Privacy is Over’ (3 November 2018) talk presented at the University of New South Wales as part of the Festival of Dangerous Ideas. Recording available at: <<https://festivalofdangerousideas.com/ideas/privacy-is-over/>>

- 3.6. ALHR supports the idea that the human right to privacy also needs to be entrenched in other legislation beyond state privacy legislation.
- 3.7. Ideally, a right to privacy would be protected within a legislated Western Australian Human Rights Act which would provide protection, akin to the right to privacy in the *The Charter of Human Rights and Responsibilities Act 2006 (Vic)*, and the *Human Rights Act 2004 (ACT)* and the *Human Rights Act 2019 (Qld)*. 3.8The APPs themselves are limited in scope. Simply mirroring the APPs within state legislation, while providing national consistency, would not be sufficient to protect the human rights of individuals.
- 3.8. While data-sharing within the Western Australian public sector could prospectively promote human rights, particularly in identifying at-risk population groups and addressing inequity, this comes with very significant risks to individuals and to communities as a whole, particularly those communities who are socially and economically disadvantaged.
- 3.9. If the Western Australian Government is to use data in “creating a safer and fairer society for all”, as stated in the intended outcomes,¹⁷ meaningful consultation with, oversight by, and the explicit consent of, the groups experiencing inequity is essential and is the only way to ensure compliance with UN Principles on Personal Data Protection and Privacy (see further discussion below under headings **9** and **10**).
- 3.10. As the exchange of personal information, both identified and de-identified, has occurred freely in the Western Australian public sector in the absence of any overarching governing legislation, it is encouraging that the development and implementation of such is part of the WA Government’s Public Sector Reform Program.

4. What issues should be considered when developing privacy and information sharing legislation for Western Australia?

- 4.1. It is a fundamental aspect of the Australian Privacy Principles that individuals should know the reasons for collection of their personal information and that the information should be used only for that particular purpose or purposes.
- 4.2. Government bodies hold particularly sensitive personal information, the disclosure of which, even to other government bodies, can have a detrimental effect on an individual's access to finances, health services, or benefits. It is imperative that personal information with the potential to harm an individual's livelihood or reputation be closely monitored and subject to greater restrictions and not be used to penalise an individual attempting to access services to which they are entitled. For example, information as to criminal records, particularly in relation to children or other vulnerable groups, illicit drug use, or involuntary hospital admissions or issues related to mental illness, ought to be carefully considered before sharing to ensure the individual is not thereby deprived of their rights or entitlements.
- 4.3. For instance, ALHR submits that the ability to repurpose data can result in a complete failure of transparency in relation to the data matching process and is highly undesirable. Persons affected

¹⁷ Government of Western Australia, *Privacy and Information Sharing for the Western Australian public sector: discussion paper*. (hereafter “Discussion paper”), page 9. Available at: https://www.wa.gov.au/sites/default/files/2019-08/Discussion%20paper_Privacy%20and%20Responsible%20Information%20Sharing_1.pdf

need to be aware of the data being collected about them and should have to give a free and fully informed consent before that data can be used for a different purpose.

- 4.4. Further, there are problems around ensuring that any consent is both free and fully informed. To quote Anna Johnston¹⁸:

“There remains a problem with the ‘notice and consent’ model of privacy protection. As academic Zeynep Tufekci has noted, ‘informed consent’ is a myth: “Given the complexity (of data privacy risks), companies cannot fully inform us, and thus we cannot fully consent.”

Putting the emphasis for privacy protection onto the consumer is unfair and absurd. As Tufekci argues in a concise and thoughtful piece for the New York Times:

“Data privacy is not like a consumer good, where you click ‘I accept’ and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices. A more collective response is needed.”

The data is de-identified so there is nothing to worry about.

If you don’t like it, opt out. If you’ve done nothing wrong, you’ve got nothing to hide.

It’s time to put those fallacies to rest. The US model of ‘notice and consent’ has failed. Privacy protection should not be up to the actions of the individual citizen or consumer. It’s the organisations which hold our data – governments and corporations – which must bear responsibility for doing us no harm.

They could start by minimising the collection of personal information, storing data securely, and limiting its use and disclosure to only directly related secondary purposes within the subject’s reasonable expectations.

ALHR endorses those comments.

- 4.5. To ensure the security of data and uniform application of privacy legislation, government must continually develop and innovate technological infrastructure and ensure that data security and access to support is prioritised.
- 4.6. Government must ensure that third parties receiving information do not use such information for commercial purposes that may penalise an individual whether inadvertently or not (for example, . sharing information with insurers or financial institutions that may result in increased premiums or undue denial of financial products).
- 4.7. Appropriate and effective penalties and remedies for breach ought to be considered to encourage efficient and effective implementation of the legislation. This may be difficult where a breach is caused by a government department.

¹⁸ “Too much cyber, not enough privacy 101” by Anna Johnston, Salinger Privacy, 5 February 2018 at <https://www.salingerprivacy.com.au/2018/02/05/not-enough-privacy-101/>

4.8. Above all, privacy and information sharing legislation, policy and guidelines must be made available to as broad a range of the community as possible, and presented in a manner that is easily accessible, easily explained and understood, culturally appropriate, and available in foreign languages. Staff should be trained to ensure vulnerable groups, such as the elderly, disabled persons and their carers, children, people from culturally and linguistically diverse backgrounds, and those with low literacy, can understand their rights and remedies.

5. What privacy principles should WA adopt for regulating the handling of personal information by the public sector? Are any of the existing Australian Privacy Principles, or principles in other Australian jurisdictions, unsuitable for WA?

- 5.1. As explained above, ALHR does not consider that simply mirroring the APPs would be sufficient to protect the rights of individuals. Rather, a bespoke approach, is appropriate, taking into consideration the sort of highly sensitive information government departments hold and the purposes for which that information is used, and taking into account the UN Principles on Personal Data Protection and Privacy . The APPs themselves are also applicable to private commercial entities and so reflect the way those types of entities might be using personal information which is different to public sector use.¹⁹
- 5.2. The *Privacy and Personal Information Protection Act 1998* (NSW) contains a set of privacy standards called Information Protection Principles²⁰ that regulate the way New South Wales public sector agencies handle personal information (excluding health information which is regulated by the *Health Records and Information Privacy Act 2002* (NSW)).²¹ It may be more appropriate for Western Australia to implement these principles which have been specifically tailored to government agencies. Similarly, Victoria has implemented similar Information Privacy Principles to the APPs but tailored to government agencies.²² Victoria also excludes health information which is covered by the *Health Records Act 2001* (Vic).

6. What should the role of a Privacy Commissioner be, and how can this role best protect privacy and ensure public trust?

- 6.1. ALHR supports in principle the establishment of a statutorily appointed independent Privacy Commissioner to manage complaints and oversee development and implementation of the privacy legislation and policy guidelines.

¹⁹ For example, APPs 3 and 4 deal with soliciting information and APP 7 which deals with direct marketing. These APPs would not be appropriate for WA as government bodies should not be using engaging in direct marketing. Further APP

²⁰ See Part 2 Division 1 and Division 2 *Privacy and Personal Information Protection Act 1998* (NSW).

²¹ See s 4A *Privacy and Personal Information Protection Act 1998* (NSW).

²² See Schedule 1 of *Information Privacy Act 2000* (Vic).

- 6.2. The powers of the Privacy Commissioner should be enshrined in statute and open to administrative review where appropriate.²³
- 6.3. To ensure public trust, the Privacy Commissioner should be easily accessible and quick to respond to complaints, allegations or lack of compliance, and reported data breaches. This in turns means that this role would have to be sufficiently resourced.

7. How should breaches of privacy be managed, and what action should be taken in response to a breach?

- 7.1. As explained above, an effective penalties regime must be in place to encourage compliance. It should be mandatory for government bodies and authorised third parties to report data breaches to the Privacy Commissioner to ensure swift remediation and support may be provided to individuals affected. Random auditing of data security systems could be implemented as a check on compliance.
- 7.2. Careful consideration must be given to the effectiveness of the Privacy Commissioner's powers to quickly penalise and ensure remediation of data breaches. An effective and efficient complaints process is an essential part of this process. The Western Australian Privacy Commissioner should also be given the power to determine if a privacy breach has occurred and what action to take.²⁴
- 7.3. ALHR supports the adoption of similar data breach notification schemes as outlined by the Office of the Information Commissioner which detail the steps an entity must take where a notifiable data breach has occurred, that is, a breach that is likely to cause serious harm.²⁵
- 7.4. ALHR supports remedies for breaches implemented in other States such as seeking an apology, requiring structural change to an organisation's practices or procedures, directing staff training, directing compensation for financial or non-financial loss and imposing fines on the government body or even, in cases of extreme abuse, the individual public sector employee.²⁶

8. When should government agencies be allowed to share personal information? Are there any circumstances in which it would not be appropriate to do so?

- 8.1. It is a fundamental aspect of the Australian Privacy Principles that individuals should know the reason for collection of their personal information and that the information should be used only for that particular purpose or purposes.
- 8.2. ALHR supports in principle the use of an individual's personal information for the purposes of improving public service delivery and improving policy, where such consent has freely been obtained from the individual (although as to whether this is possible see the quotation in

²³ See e.g. Part 5 *Information Privacy Act 2000* (Vic) which deals with the complaints procedure and referral to the Privacy Commissioner or the Minister where the matter raises an issue of important public policy.

²⁴ Cf the Privacy Commissioner of Victoria who has no power to determine if a privacy breach has occurred.

²⁵ See <https://www.oaic.gov.au/privacy/notifiable-data-breaches/>

²⁶ See e.g. s 43 *Information Privacy Act 2000* (Vic) and ss 53 and 62 *Privacy and Personal Information Protection Act 1998* (NSW). Section 62 provides for penalties to be imposed against corrupt public sector officers.

paragraph 4.4 above) and provided there is a strict governance model to protect individual interests.

- 8.3. ALHR supports the Western Australian Government's suggestion to create special considerations or exclusions for particularly sensitive information (particularly in relation to criminal records and ongoing litigation) and specific prohibition of use of information for direct marketing or profiling of individuals for commercial or insurance purposes.²⁷ Where appropriate and practicable, personal information should be de-identified. Individuals should be allowed to opt out of having their data used in studies. The consent of individuals should always be sought before sharing sensitive personal information.²⁸

9. What should the role of a Chief Data Officer be? How can this role best support the aims of Government and the interests of the public?

- 9.1. ALHR supports in principle the appointment of a Chief Data Officer to provide guidance and best practice standards for the public sector in using and managing data.
- 9.2. A governance model that includes reporting obligations to an independently appointed Western Australian Privacy Commissioner would ensure that the best practice models adopted place adequate weight on the public interest and support individuals' rights to privacy.

10. Should the Western Australian Government facilitate sharing of information outside of the WA public sector? What should be considered when making a decision to share outside the WA public sector?

- 10.1. **Sharing with non-government entities:** The sharing of information outside the public sector should be approached with extreme caution and again should only ever occur with the consent of the individual. Once information, even in de-identified form, is shared outside of the WA public sector it would be difficult for the Western Australian Government to ensure that effective risk management frameworks were implemented in order to ensure the information was kept confidential. Even if third party agencies contracted or partnered with the government for the purposes of the delivery of public services, it would be difficult for the Western Australian Government to implement and maintain oversight by such non-government agencies of their use of personal data.
- 10.2. Where data is collected in partnership between agencies, or shared between data collection agencies, the standards around privacy and data protection may be different. This is a situation likely to arise if information were shared between Western Australian public sector agencies and private sector agencies, and indeed is likely to have happened already in the absence of regulation.
- 10.3. The United Nations Office of the High Commissioner for Human Rights has endorsed the approach in this situation to be that the practice of the agency with the strictest privacy and data

²⁷ See page 34 of the Discussion Paper.

²⁸ See e.g. Principle 10 – Sensitive Information *Information Privacy Act 2000* (Vic) and APP 3.3 *Privacy Act 1988* (Cth).

protection requirements should be adopted and upheld by all the agencies involved in the data-sharing project or exchange.²⁹

- 10.4. ALHR is strongly opposed to the prospect that information obtained through or used by Western Australian government sector agencies could or should be made available for commercial purposes.
- 10.5. There have already been uses of medical information at the federal level that have been questionable from a legal and ethical standpoint. Legal commentary has been made on the Department of Human Services (**DHS**) partnering with a non-government research institute to recruit participants into a study on bipolar disorder. In this instance, the research institute was provided by DHS with the details of 50,000 Australian who had been prescribed lithium, as gleaned from Medicare records, in clear breach of relevant Australian Privacy Principles.³⁰
- 10.6. **Sharing with individuals and third parties:** ALHR concedes that in very limited circumstances, it may be appropriate for information to be shared with dependents or third party assistants of individuals to enable the individual to have access to benefits and services. A 2010 report by the Australian Law Report Commission (**ALRC**) identified impeded access to benefits and services as a problem raised by many members of the community.³¹
- 10.7. The ALRC also identified that most of the concerns about impeded access could be facilitated by agencies and organisations having clear procedures in place to obtain the consent of individuals, rather than the governing legislation needing to be more prescriptive. For example, many of the access issues could have been avoided if the agencies involved had a clear procedure for partners, parents or third party assistants of individuals to gain the requisite consent from an individual.³²

11. What criteria should be included as part of a risk management framework such as the 'Five Safes'?

- 11.1. As pointed out in the Discussion Paper, the 'Five Safes' model of risk management would be a positive starting point for a risk management framework, although the Discussion Paper does not provide detail about how compliance with the Five Safes would be monitored.
- 11.2. While currently the 'Five Safes' model appears to be a well-regarded model that has been applied in other jurisdictions, the Western Australian Government should consider that the Five Safes model may need revision in the future with reference to the development of technology.

²⁹ See further the United Nations Human Rights Office of the High Commissioner, 'A Human Rights Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development.' (2018), p. 17. Available at: <<https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf>>

³⁰ Bruce Baer Arnold and Wendy Bonython, 'No, its Not OK for the government to use your prescription details to recruit you for a study.' July 31, 2019. <<https://theconversation.com/no-its-not-ok-for-the-government-to-use-your-prescription-details-to-recruit-you-for-a-study-121122>>. See further: <https://theconversation.com/after-the-medicare-breach-we-should-be-cautious-about-moving-our-health-records-online-80472>

³¹ Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' (ALRC Report 108). *Chapter: Problems with the Privacy Act*. Available at: <<https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/70-third-party-representatives/problems-with-the-privacy-act/>>

³² Op cit 25.

- 11.3. For example, assessments of what amounts to the “right level of security” and how de-identification can occur will need to be updated in line with current standards and practices.
- 11.4. Indeed, if even large corporations with almost unlimited resources and high technological capabilities are currently struggling to keep data de-identified, in safe settings and in the hands of safe people, as appears to be the case,³³ it is difficult to see how the Western Australian Government will be able to do so within normal resourcing limitations.
- 11.5. In developing legislation, the Western Australian Government should consider the United Nations’ human rights-based approach to data that forms a part of the United Nations’ (UN) 2030 Agenda for Sustainable Development³⁴ centred on the six guiding principles of participation, data disaggregation, self-identification, transparency, privacy and accountability.
- 11.6. This framework places more of an emphasis on the self-determination of individuals to participate in data-sharing projects, rather than building an external assessment of the ethics of data use into a risk assessment framework.

12. Under what circumstances would it be considered acceptable to share confidential information within the public sector?

- 12.1. ALHR acknowledges that once all risk management frameworks have been applied, information sharing within the public sector could assist vulnerable people. A careful balance needs to be struck between protecting vulnerable adults from unnecessary interference with their privacy and ensuring that they gain access to required services and benefits.
- 12.2. The ALRC notes that more effective information sharing between government agencies could facilitate meaningful responses to inequity and poor social and health outcomes in the community, some examples of which are given in the Discussion Paper.
- 12.3. Participation is one of the key guiding principles of data management in the United Nations’ human rights based approach to data, particularly with regards to disadvantaged groups in the community.³⁵
- 12.4. It is promising that the Discussion Paper points to the prospect of involving some groups in considering models for information sharing, in particular consulting with Aboriginal organisations such as the Western Australian Aboriginal Health Ethics Committee.³⁶
- 12.5. It is important that consultation with groups affected occurs in a meaningful rather than tokenistic way, particularly when the projects or data-collection initiatives involve sensitive information pertaining to health information and information relating to the wellbeing of children.

³³ Op cit 11.

³⁴ United Nations Human Rights Office of the High Commissioner, ‘A Human Rights Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development.’ Available at: <<https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf>>

³⁵ Op cit 28.

³⁶ Discussion paper, page 40.

13. What should the Western Australian government be doing to support successful implementation of privacy and information sharing?

- 13.1. The Western Australian Government should be placing the privacy interests and associated human rights of members of the community at the forefront of any information sharing framework. Some ways in which this can be achieved include:
- 13.2. **Treating data privacy as a fundamental human right rather than a privilege or a consumer good.** Governments should not treat data sharing and privacy like a “consumer good” and ALHR has some concerns about the Discussion Paper’s emphasis on the purported need to create ease for members of the Western Australian public and for service providers so that individuals do not have to provide their information multiple times to different entities. ALHR acknowledges that the sharing of information between service providers can facilitate holistic, trauma-informed service coordination and delivery so that vulnerable people are not re-traumatised by requirements to recount their trauma multiple times in order to access the supports they need. However, this can be accommodated within an information sharing framework via obtaining appropriate, specific, informed consent/s from the individuals involved. Outside of these situations, ALHR has serious concerns about measures that would prioritise ‘ease’ over the need for adherence to Australian Privacy Principles that require the informed consent, that individuals should know the reason for collection of their personal information, and that the information should be used only for that particular purpose or purposes.
- 13.3. As mentioned above, one New York Times writer has rightly commented that: “Data privacy is not like a consumer good, where you click “I accept” and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be regulated by trusting in the wisdom of millions of individual choices.”³⁷
- 13.4. Approaches need to be carefully planned and managed in consultation with the groups of people that they affect (see also discussion of informed consent at 4.4 above and 13.9 below) and ALHR notes the significant risk of paternalism and intrusiveness in the private lives of individuals under the guise of streamlined or improved service delivery, productivity or efficiency.
- 13.5. **Keeping information secure should be an upmost priority for the Western Australian Government in introducing data-sharing and privacy legislation.** The state public sector is composed of a large number of entities of different types. This presents not only vulnerability in managing datasets and databases but also opportunities for leakage and unintended sharing when information is exchanged between agencies.
- 13.6. The Federal Government has so far contravened the APPs in failing to keep personal and sensitive information secure, with a number of noteworthy examples in recent years including leaks related to the recently implemented My Health Record system,³⁸ inadequate encryption of

³⁷ Zeynep Tufekci, ‘Opinion: The Latest Data Privacy Debacle’ New York Times (January 2018), < <https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html>>

³⁸ Author unspecified, ‘Data breaches rise in My Health Record system,’ IT News, (January 1, 2019). Available at: < <https://www.itnews.com.au/news/data-breaches-rise-in-my-health-record-system-517394>>

- Medicare datasets,³⁹ and security breaches allowing the Medicare details of individuals to be accessed and sold on the dark web, two years after that information was accessed.⁴⁰
- 13.7. Given this failure at a national level, ALHR has serious concerns about the Western Australian Government's capacity to protect sensitive personal information.
- 13.8. It is not just the capacity of the Western Australian Government to protect and manage sensitive details that remains at large but rather their ability to keep up with the development of technology. The previous Australian Information Commissioner has described de-identification as akin to "rocket science" in difficulty, admitted that the risk of unauthorised entities re-identifying and using data is significant, and noted that de-identified data needs to be treated with as much care as identified data.⁴¹
- 13.9. **Ensuring informed consent and self-determination (see also discussion at 4.4 above):** ALHR is concerned if the new Western Australian legislation opens up the possibility of a data-sharing model which is an "opt-out" system similar to the Australian Digital Health Agency's My Health Record, where the default position leaves open the possibility of many members of the community not giving informed consent for the sharing of their data between agencies, particularly those from vulnerable communities.
- 13.10. Some commentators have even raised the point that an "opt-out" system is not capable of rendering consent at all, because under Commonwealth privacy law, an assertive acceptance is required for informed consent.⁴²
- 13.11. To adequately protect the right of privacy, it would be preferable to implement an opt-in system of information sharing where individuals are fully informed about what information will be shared between agencies and in what circumstances and for what purpose, with the possibility of customising these variables.

14. Conclusion

- 14.1. The Western Australian Government's approach to data sharing should not cause individuals to make *"simplistic, false choices between competing values: dignity or convenience; freedom or control; ... rights and freedoms, or security, modernisation and development."*⁴³
- 14.2. The Western Australian Government's approach to data sharing should not cause individuals to make *"simplistic, false choices between competing values: dignity or convenience; freedom or control; ... rights and freedoms, or security, modernisation and development."*⁴⁴

³⁹ Paris Cowan, 'Health Pulls Medicare dataset after breach of doctor details.' IT News (September 29, 2016). Available at: <<https://www.itnews.com.au/news/health-pulls-medicare-dataset-after-breach-of-doctor-details-438463>>

⁴⁰ Paul Karp, 'Australians' Medicare details illegally sold on darknet – two years after breach exposed,' The Guardian Australia (16 May 2019). Available at: <<https://www.theguardian.com/australia-news/2019/may/16/australians-medicare-details-illegally-sold-on-darknet-two-years-after-breach-exposed>>

⁴¹ Paris Cowan, 'Pilgrim warns data de-identification is "rocket science".' IT News (April 20, 2016) Available at: <<https://www.itnews.com.au/news/pilgrim-warns-data-de-identification-is-rocket-science-418387>>

⁴² Anna Johnston, 'Why Opt-Out Consent is an Oxymoron,' Salinger Privacy (November 29, 2018). Available at: <<https://www.salingerprivacy.com.au/2018/11/29/why-opt-out-consent-is-an-oxymoron/>>

⁴³ Op cit 4.

⁴⁴ Op cit 4.

- 14.3. Any legislation which threatens to impinge upon human rights must be narrowly framed, proportionate to the relevant harm or aim it seeks to address, and provide an appropriate contextual response which minimises the overall impact upon all human rights.
- 14.4. As Western Australia is lagging behind other states and territories in enacting both a Human Rights Act and privacy and data-sharing legislation, it is encouraging to see that such a legislative regime is part of the Western Australian Government's reform agenda.
- 14.5. ALHR urges that a human-rights based approach to privacy and data sharing be adopted by the Western Australian Government.
- 14.6. Privacy is a human right that the Western Australian Government is obliged at international law to uphold, and requires s protection within both a Western Australian Human Rights Act and a Federal Human Rights Act.
- 14.7. The challenge for the Western Australian government is the same challenge facing other governments in addressing privacy and data sharing –

“The challenge is to improve access to and understanding of technologies, ensure that policy makers and the laws that they adopt respond to the challenges and potentialities of technologies, and to generate greater public debate to ensure that rights and freedoms are negotiated at a societal level.”⁴⁵

- 14.8. As the Human Rights Law Centre has noted in comments on the use of biometric data, the use of people's private data:

“should be governed by laws with sufficient detail for Australians to understand what is being done with their information in their name, and adequate safeguards to protect against ‘function creep,’ misuse of data and inaccuracy. If we are to override requirements for individual consent in the public interest, we need to know what that interest is and what evidence justifies new powers.”⁴⁶


- 14.9. Citizen involvement, understanding of, and participation in, important decisions, is an essential element of democracy. The decision to share individuals' personal information with the Western Australian Government is a crucial decision with far-reaching consequences both now and for future generations. In order for government to work for the public good, to be democratic, and to be seen to be operating in a transparent and democratic manner, citizens need to be consulted by government in relation to important decisions of this nature and only legislation that fully reflects their privacy and other human rights should be implemented. 14.9 ALHR is happy to provide any further information or clarification in relation to the above.

⁴⁵ Op cit 4.

⁴⁶ Human Rights Law Centre Submission Inquiry into the provisions of the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 ('the NSW Bill') available at Inquiry Website. Submission 18 page 2.

If you would like to discuss any aspect of this submission, please email me at: president@alhr.org.au

Yours faithfully



Kerry Weste

President

Australian Lawyers for Human Rights

Any information provided in this submission is not intended to constitute legal advice, to be a comprehensive review of all developments in the law and practice, or to cover all aspects of the matters referred to. Readers should take their own legal advice before applying any information provided in this document to specific issues or situations.

Submission Contributors

Keely Liddle

Sarah Dunstan

Material drawn from ALHR Submissions:

[**Identity-matching Services Bill 2018 and the Australian Passports Amendment \(Identity-matching Services\) Bill 2018.**](#)

[**Inquiry into the provisions of the Road Transport Amendment \(National Facial Biometric Matching Capability\) Bill 2018 \('the NSW Bill'\)**](#)

By Dr Tamsin Clarke and Kerry Weste