Privacy and Responsible Information Sharing for Western Australia

INDEPENDENT COMMUNITY SUBMISSION

Prepared by:

Pip Brennan – Executive Director, Health Consumers' Council
Mark Fitzpatrick – CEO, Telethon Speech & Hearing
Juan Larranaga – Director, Save the Children WA
Vicki O'Donnell – CEO, Kimberley Aboriginal Medical Services
Maria Osman – Community member, Supporting Communities Forum
Carol Petterson JP – Community member, Supporting Communities Forum
Julia Powles – Associate Professor, University of Western Australia
Chris Twomey – Director of Policy, WA Council of Social Service
Ross Wortham – CEO, Youth Affairs Council of Western Australia

With expert guidance from Professor David Watts, former Victorian Privacy Commissioner, and Dr Bridget Bainbridge, whose inputs are kindly supported by the Minderoo Foundation

1. Introduction

The Western Australian government has produced a Discussion Paper entitled 'Privacy and Responsible Information Sharing for the Western Australian Public Sector'.[1] The Discussion Paper confirms the Western Australian government's commitment to introduce a whole-of-sector approach to:

- protecting individuals' information privacy;
- enabling safe and facilitated information sharing;
- harmonising standards for the responsible collection, management, and use of personal information; and
- introducing procedures to ensure accountability and public confidence (through independent oversight and clear pathways for resolving complaints),

within the Western Australian public sector and with authorised third parties.

The Discussion Paper seeks comments on its approach to implementing these initiatives into a legislative regime that is aligned to the contemporary needs and requirements of the Western Australian community.

This submission responds to the Discussion Paper's request for comments.

---

[1] Government of Western Australia, *Privacy and Responsible Information Sharing for the Western Australian Public Sector Discussion Paper,* at p14 (hereafter, *Discussion Paper*).

2. Executive summary

Western Australia has the opportunity to develop the most advanced and forward-thinking information privacy and sharing legislation in Australia. Although it has identified some of the key policy drivers for reform, this submission argues that the Discussion Paper does not provide an adequate contemporary approach to either protecting information privacy or establishing a suitable information sharing framework for the WA public sector.

The Discussion Paper's ambitions are needlessly limited for two main reasons.

The first is that it is overly influenced by the legislation of other Australian States and Territories, most of which were developed in an early digital era and before technologies such as advanced data analytics became widespread. Although these jurisdictional laws have been renovated, they have become complex and unwieldy. They lack clear and coherent information policy objectives. Although there are elements of other States and Territories' laws that can be adopted – and this is highlighted and recommended in this submission wherever possible – an overall 'cut and paste' approach will simply replicate their shortcomings.

The second limitation is that it is a mistake to assume that WA's information environment is localised to Australia. Privacy and information sharing issues are global. This means that WA's approach should align with international benchmarks – something that will, of necessity, also bring national harmonisation. One of the main reasons for reform in WA is to support and enable the State's world-class research capabilities. The privacy framework should empower WA's research sector with the regulatory foundations to enable researchers to participate in international research on an equal footing with international partners and competitors. This opportunity is not currently available to researchers in other Australian jurisdictions.

We urge the WA government to take a broader and more expansive approach to privacy and information sharing that aligns more closely with the international environment and which sidesteps some of the more problematic aspects of other jurisdictional legislation in Australia.

3. Information privacy and information sharing: two sides of the same coin

Information privacy laws have always been about striking a balance between providing individuals with a degree of control over the collection and handling of their personal information and ensuring the benefits that can accrue from information flow.

The foundation of privacy is in rights, but privacy is not an 'absolute' right. International human rights law confers privacy rights on individuals but permits these to be limited or restricted for legitimate public interests, such as for law enforcement and public health purposes.[2]

[2] *Universal Declaration of Human Rights 1948*, Articles 12 and 29(2); *International Covenant on Civil and Political Rights 1966*, Articles 4 and 17.

Information privacy – the right of individuals to exercise a degree of control over the way in which their personal information is collected, used, disclosed or otherwise handled – is a sub-set of privacy. It was first codified by the OECD in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980*, which established a series of principles designed to regulate the way in which personal data is both protected and shared, and aimed to "avoid the creation of unjustified obstacles to the development of economic and social relations".[3] The *OECD Principles* have served as the basis of all information privacy laws, including those of the Australian Commonwealth, States and Territories, as well as the European Union's privacy laws up to and including the *General Data Protection Regulation* (*GDPR*).

Information privacy laws also do more than just regulate the collection, use and disclosure of personal information. Through privacy principles, they invariably contain additional requirements that cover issues such as information openness and transparency, data quality, data security, access and correction rights, the use of unique identifiers, and transborder data flows. These principles serve an important role in protecting privacy by ensuring that individuals are confident that their personal information is properly safeguarded across a range of settings. For example, the data security principle found in all Australian information privacy laws is the only statutory information security[4] obligation that applies to the public sector.[5]

4. Australian privacy laws: a caution about crippling complexity

All of Australia's information privacy laws adopt privacy principles based on the *OECD Principles*, such as the *Australian Privacy Principles* in the Commonwealth *Privacy Act 1988*. Although there are some drafting variations between jurisdictions, in broad terms they are substantially similar. The main differences are the way in which privacy principles are implemented, that is, the way in which regulatory powers are conferred and exercised, the functions and powers of the regulator, penalties, remedies and exceptions.

These differences are most apparent in the federal *Privacy Act 1988.* The Commonwealth legislation was originally designed to cover the Commonwealth public sector but, since 1988, it has been extensively amended. Many of these amendments have been designed to deal with new technologies and particular areas of Commonwealth responsibility such as tax file numbers and credit reporting, as well as to cover the private sector.

Some, but not all, of these amendments include:

- in 1990 to cover spent convictions and tax file number data matching;
- in 1991 to cover credit reporting, Medicare and the PBS;
- in 1994 to cover the ACT;

[3] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. See especially Chapter II, Section A: Purpose and Scope.

[4] As distinct from confidentiality or secrecy obligations and offences.

[5] The only exception is the *Privacy and Data Protection Act 2014 (Vic)*, which establishes statutory security obligations for Victorian public sector data. The law applies to the Victorian public sector, with the exception of local government, Universities, and health information which is dealt with in separate state legislation.

- in 1997 to cover certain activities of telecommunications service providers;
- in 2001 to cover the private sector;
- in 2006 to cover anti money laundering and counter terrorism;
- in 2010 to cover healthcare identifiers;
- in 2012 to cover electronic health records;
- in 2014 to provide additional regulatory powers and to replace the *National Privacy Principles* with the *Australian Privacy Principles*[6]; and
- in 2018 to establish the Notifiable Data Breaches scheme.

The result of these successive amendments is highly complex legislation that is difficult to understand and apply by all but a small number of highly specialised lawyers and advisers. This complexity also means that it is almost impossible for individuals to understand and exercise their privacy rights. The Commonwealth *Privacy Act 1988* is now well over 300 pages long. It has recently been further amended to establish the Consumer Data Right (CDR), supplemented by additional regulation developed by the Australian Consumer and Competition Commission and the interim Data Standards Body to support the CDR. The Office of the Australian Information Commissioner recently issued *Draft Consumer Data Rights Privacy Safeguard Guidelines,* which are 180 pages long.[7] In 2020, the Commonwealth proposes to add to this already complex body of regulation by enacting Data Sharing and Release legislation.

Although State and Territory legislative frameworks have not undergone the same degree of change, they are also complex. For example, New South Wales, Victoria and the ACT have separate *health privacy* laws that set up parallel privacy principles (health privacy principles), parallel complaints and oversight mechanisms, and parallel bureaucracies.

New South Wales, Victoria and South Australia have also enacted *data sharing* laws that are designed to promote information sharing and data analytics.[8] These data sharing and analytics laws have the effect of overriding existing relevant privacy laws in those jurisdictions to the extent that they are inconsistent with them, and they contain powers to compel information to be shared, integrated and analysed. As will be seen in section 7 below, there is no evaluative evidence to suggest that these initiatives have succeeded.

This degree of complexity does not provide a regulatory framework that gives clarity to stakeholders. Associated disproportionate compliance costs and downstream inefficiencies impose burdens on the public sector and create uncertainty for individuals.

---

[6] The *National Privacy Principles* were first developed to support the extension of the *Privacy Act 1988* to the private sector in 2001. They were replaced by the *Australian Privacy Principles* in 2014 following the Australian Law Reform Commission's 2008 Report, *For Your Information: Australian Privacy Law and Practice,* ALRC 108. See https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/.

[7] Office of the Australian Information Commissioner, *Draft Consumer Data Rights Privacy Safeguard Guidelines*, 16 Oct 2019. See https://www.oaic.gov.au/engage-with-us/consultations/draft-cdr-privacy-safeguard-guidelines/draft-privacy-safeguard-guidelines/.

[8] *Data Sharing (Government information) Act 2015 (NSW)*; *Victorian Data Sharing Act 2017 (Vic)*; *Public Sector (Data Sharing) Act 2017 (SA)*.

The problematic nature of excessively complex regulation was highlighted in a different context in the final report of the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*:

> "… adding a new layer of regulation will not assist. It will add to what is already a complex regulatory regime. No doubt the financial services industry is itself complicated. That may be said to explain why the regulatory regime is as complicated as it is. But closer attention will show that much of the complication comes from piling exception upon exception, from carving out special rules for special interests. And, in almost every case, these special rules qualify the application of a more general principle to entities or transactions that are not different in any material way from those to which the general rule is applied."[9]

Although this statement was made about financial services regulation, it is just as relevant to information regulation and should, in our submission, inform Western Australia's approach to privacy and data sharing. A streamlined, cohesive, and coherent regulatory scheme with clear objectives that does not "pile exception upon exception" to cater for marginal special interests is not only desirable; it is imperative.

Recommendation 1
Western Australia should enact a single piece of privacy and data sharing legislation that has clear objectives and limited exceptions to avoid complexity. It should recognise that privacy is an enabler and not an impediment to responsible information flow.

5. Western Australia's opportunity

Western Australia has the opportunity to develop a public sector privacy framework from the ground up. It has the chance to learn from the experiences of other jurisdictions about what works and what does not. It also has the opportunity to inform its approach to privacy regulation by taking account of the most appropriate contemporary developments that reflect best practice, especially the European Union's *GDPR* – increasingly a standard in our region.

Western Australia has identified that one of its most useful assets is information which, if used wisely, "has the power to address the needs of our society now and into the future".[10] Using information wisely – particularly personal information – involves developing a regulatory approach that addresses the current deficits identified in the Discussion Paper:

- fragmented and unclear protections for those whose information is held in the WA public sector, with no specific avenue for complaints resolution;
- reduced public trust and confidence in how data is stored, used, and shared;
- an inconsistent and risk-averse approach to information sharing between agencies; and
- reduced collaboration and evidence-based decision-making.

[9] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, *Final Report Vol 1,* at p16.
[10] *Discussion Paper*, at p6.

This submission supports a legislative framework that addresses these issues, but argues that legislation is *only one* of the public policy approaches needed to reform Western Australia's information environment. It would be unrealistic to expect a legislative solution to completely resolve a risk-averse information sharing culture in the public sector.[11] Moreover, a legislative solution that fails to 'get the balance right' between protecting and sharing personal information is unlikely to increase the public's confidence in the Western Australian public sector's ability to function as trusted custodians of personal information. The government's acceptance of this reality is evident in the pressing need for legislation addressing privacy – in name but also in substance – as an essential precursor to anticipated reforms around data linkage and sharing. Establishing and maintaining trust in the WA public sector's information practices is crucial in an environment where trust in government has declined by fifty percent in the decade to 2018.[12]

5.1. Establish the regulatory framework to constitute Western Australia as a national, regional and international research hub

Western Australia has a long history of undertaking world-class health research through its Data Linkage System. This is overseen by the Data Linkage Branch, managed by WA Department of Health's Purchasing and System Performance Division. The work it has undertaken is internationally renowned. However, its potential for growth is hampered by the lack of a suitable privacy regulatory framework. As the WA Chief Scientist found in the report that motivated this privacy and information sharing reform opportunity: "… there is evidence to suggest that other States and countries are hesitant to share data with WA due to the lack of privacy legislation".[13]

Research can no longer be seen as being restricted to state or even national data initiatives. Increasingly, data-informed research involves multiple institutions operating collaboratively on an international basis.[14] What this means for Western Australia is that its research institutions will increasingly compete for opportunities, projects, funding, and expertise in a global research environment. Its competitors and collaborators will often be located in jurisdictions where statutory privacy protections apply to the research projects and the institutions that undertake them. Western Australia's inability to provide a robust privacy framework for research projects will put it at a competitive disadvantage.

Although the Discussion Paper acknowledges the need to develop a Western Australian privacy framework to support research initiatives, the *nature* of the framework is left open.

---

[11] This is an issue that is keenly felt within multiple policy domains. As just one example, the *Children and Communities Services Act 2004 (WA)* contains provisions to enable data sharing where children are at risk (e.g., s23 and s24) – but a culture of caution and reluctance reduces their use. See further in section 9.12 below.

[12] Museum of Australian Democracy and the Institute for Governance and Policy Analysis at the University of Canberra, *Democracy 2025.* See https://www.democracy2025.gov.au.

[13] Data Linkage Expert Advisory Group, *A Review of Western Australia's Data Linkage Capabilities*, at p16. See https://www.jtsi.wa.gov.au/what-we-do/science-and-innovation/chief-scientist-of-western-australia/data-linkage-review.

[14] See, for example, United Nations General Assembly, *Strengthening the Global Health Architecture: Implementation of the Recommendations of the High-Level Panel on the Global Response to Health Crises,* A/70/824. See https://www.un.org/ga/search/view_doc.asp?symbol=A/70/824.

Australian jurisdictions' existing privacy frameworks provide pathways by which *health* research can be undertaken. However, each was designed before Big Data, advanced data analytics, and Artificial Narrow Intelligence (ANI) technologies became broadly available to government and research institutions. None of these frameworks adequately address public interest research that extends beyond health research to more general categories of social and scientific research. Although some reference contemporary health research guidelines that are supported by privacy legislation,[15] such as the *National Statement on Ethical Conduct in Human Research*,[16] others, such as the *Guidelines on Health Research*[17] issued under the *Health Records Act 2001 (Vic)* are almost two decades old and are obsolete.

Health research, particularly research that focuses on public health and primary health risk analysis and prevention, is multi-sectoral and multi-dimensional. It needs to be anchored by appropriate evidence. Increasingly, as confirmed in WA's recent *Sustainable Health Review Final Report*, this evidence extends beyond health information to social, environmental, and other categories of data – these also being personal information – in order to examine linkages between, and to develop insights into, health outcomes and the causes of disease.[18]

To maximise Western Australia's capability to comprehensively participate in an international research environment, a privacy framework should include:

- provisions that enable public interest health and medical, social, and scientific research to be undertaken; and
- a supporting power to enable a nominated Privacy Commissioner to publish, following consultation, binding guidelines that support such research, subject to oversight and review by the Privacy Commissioner.

Recommendation 2
The privacy and data sharing legislation should support the growth and development of Western Australia's public interest research sector.

5.2. Align with international benchmarks

Increasingly the EU's *GDPR* is becoming an international benchmark for data protection. The reason for this is that it has extraterritorial reach under Article 3(2), and covers entities outside the EU who are processing data on people in the EU. In a research context, this means that research conducted by Western Australian organisations such as Universities may be required to comply with the *GDPR*.

[15] For example, Part IX of the *Privacy Act 1988 (Cth)* enables the Australian Information Commissioner to approve guidelines issued by the CEO of the National Health and Medical Research Council (see s 95A).
[16] National Health and Medical Research Council, *National Statement on Ethical Conduct in Human Research,* 2018 revision.
[17] See https://www2.health.vic.gov.au/about/publications/researchandreports/39Guidelines39--Health-Records-Act-2001-Vic-Statutory-Guidelines-on-Research-issued-for-the-purposes-of-Health-Privacy-Principles-11eiii-amp-22giii-February-2002.
[18] See https://ww2.health.wa.gov.au/Improving-WA-Health/Sustainable-health-review/Final-report, 2019.

Our view is that Western Australia has the opportunity to develop a regulatory regime that puts Western Australia's research institutions in a position where they are not required to develop and operate cumbersome, parallel information privacy compliance processes where they partner with European research institutions: in other words, compliance with Western Australian regulation would be the equivalent of compliance with the *GDPR*. The formal process by which this outcome could be achieved is by an 'adequacy' application under Article 45 of the *GDPR*.

Recommendation 3
Research is international. WA's privacy and data sharing legislation should align with international benchmarks to best support the public interest research sector – as well as the broader public interest in creating forward-thinking laws adapted to our context.

5.3. Create the conditions for seeking adequacy under the *GDPR*

Transfers of personal data from the EU to a third party are permitted where the European Commission "has decided that the third country, *a territory or one or more specified sectors within that third country…* ensures an adequate level of protection. Such a transfer shall not require any specific authorisation".[19]

A number of countries, including major trading partners *New Zealand, Japan,* and, within the privacy sector, *Canada* and the *USA*[20], but not Australia or any State or Territory of Australia, have information privacy laws that have been declared to be 'adequate' for the purposes of the *GDPR*. Regional partners such as South Korea are currently seeking 'adequacy' determinations.[21]

Western Australia has the opportunity to develop its privacy and information sharing regime to a standard that would provide it with the foundation for an 'adequacy' determination under the *GDPR*, facilitating the research activities of its institutions and Universities and their ability to engage in international collaborative projects where personal information is shared. This opportunity is not currently available in other Australian jurisdictions.

The approach to information privacy and information sharing that is outlined in the remainder of this submission has been designed to enable Western Australia to seek an 'adequacy' finding under the *GDPR*.

It seems clear that restrictions and barriers to the sharing of data will increasingly impact upon Australian businesses wanting to operate in and share data with the European Union, as well as across the Asia Pacific region as countries follow suit and adopt *GDPR* standards. The operation of the *GDPR* already limits Australian businesses, e.g., from sharing their own internal customer data across international boundaries, because of the lack of adequacy of WA privacy and data sharing protections. This reform presents an opportunity to respond to this situation.

---

[19] Article 45(1) *GDPR*. Our emphasis.
[20] Through what is known as the 'Privacy Shield'.
[21] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Recommendation 4
Alignment with international benchmarks creates an opportunity for Western Australia to seek an 'adequacy' finding under the *GDPR*. The privacy and data sharing legislation should be designed to enable Western Australia to successfully obtain an 'adequacy' finding.

6. The problem of information sharing

Both the Discussion paper and the WA Public Sector *Roadmap for Reform* recognise the need for better information sharing within the WA public sector. They identify two main problems.

6.1. Complexity, inconsistency, inefficiency

The first problem is that the lack of a clear privacy framework "has resulted in considerable complexity, inconsistency and inefficiency in how public sector agencies approach the management and use of information".[22]

Information within the WA public sector can be broadly classified into two categories: (1) information that is about, or which relates to, identified or identifiable individuals; and (2) other information that is not about, or related to, individuals.

It is worth noting clearly: the *absence* of WA privacy legislation cannot be claimed to be the sole reason for creating complexity, inconsistency, and inefficiency, or impeding the use and disclosure (i.e., the 'sharing') of personal, or any other, information in the WA public sector. Even when the Western Australian government has issued policy directions to the public sector, such as the *Policy Framework and Standards for Information Sharing between Government Agencies* and the *Whole of Government Open Data Policy,* public sector information sharing objectives have not been realised. As privacy has not entirely caused the problem, as a matter of logic the cause lies elsewhere.

The Discussion Paper suggests that the reluctance of the public sector to share information is attributable to other *legislative* barriers or deficiencies. The most obvious of these are confidentiality and secrecy provisions that prevent or restrict agencies from disclosing information to other agencies or enabling them to access it.

Although these may be contributing causes it is unlikely that they fully account for information sharing deficits. Many categories of public sector information are not subject to confidentiality or secrecy restrictions, but are not shared any more consistently.

Some confidentiality and secrecy provisions exist for the express purpose of preventing information from being shared and these *are* justified on public policy grounds. For example, those who notify children who are in need of protection are justifiably provided with confidentiality protections, as are whistleblowers and sensitive police sources.

[22] *Discussion Paper*, at p14.

Where confidentiality and secrecy restrictions apply, they can often be overcome where legal authority to disclose information is provided. In many cases this legal authority can be provided by a Minister, an agency head, or a chief executive: in other words, the current *legislative* sharing impediments identified in the Discussion Paper are overstated.

The Discussion Paper also – surprisingly – suggests that Western Australia's freedom of information legislation contributes to public sector information sharing failures. It states that water information from many "privately-developed expert reports provided by licensees and license applicants"[23] cannot be shared through the Department of Water and Environmental Regulation's Water Information portal because of "freedom of information processes".

Although the exact nature of these restrictions is not stated, privacy exemptions in the *Freedom of Information Act 1992* cannot be the reason. Water information is not personal information. If the (unspecified) restrictions are based around trade secret or confidentiality exemptions contained in freedom of information legislation, it seems incongruous that government accepted that such vital information should have been provided to it on that basis in the first place.

If the reports include some personal information such as the names and addresses of the experts, licensees or licence applicants, these can easily be redacted and/or anonymised.

It is equally incongruous to think that privacy and data sharing legislation could solve this problem unless the data sharing legislation is designed to abrogate government's third party trade secret or confidential information obligations. It is noted that information can always be released outside of freedom of information legislative requirements.[24]

6.2. Restrictive policies and practices

The second main information-sharing problem that has been identified in the Discussion Paper is that restrictive "… policies and practices designed to keep information confidential are sometimes extended to information that can be safely shared".

It is highly likely that these reasons more accurately account for the Western Australian public sector's information sharing failures. These arise out of internal public sector structural issues that disincentivise information sharing and include:

- cultural factors that discourage collaboration between agencies, due in part to a lack of leadership and accountability, inadequate policy development, as well as failing to reward or acknowledge multi-agency collaborative information sharing initiatives;
- funding arrangements that provide resources for agency-specific activities rather than for cross-agency initiatives;
- technical issues that prevent disparate public sector information resources such as databases being integrated and a lack of interoperability across public sector information systems and information assets;

[23] *Discussion Paper*, at p45.
[24] See s3(3) *Freedom of Information Act 1992 (WA)*.

- a reluctance to expose the errors and inadequacies of agency data collection, collated data sets, and performance more broadly, to third parties, including central agencies;
- a lack of clarity regarding information governance responsibilities for multi-agency information sharing programs and initiatives;
- proxy notions of privacy – often misinformed and unnecessarily restrictive – that have prevailed in a vacuum of authoritative privacy legislation;
- a lack of clarity about roles, responsibilities, and accountabilities for multi-agency information sharing programs and initiatives; and
- a lack of accountability for information sharing failures.

In our submission it is unlikely that the development of privacy and information sharing legislation will *of itself* address these root causes. Moreover, a complex legislative framework is more likely than not to exacerbate these problems.

It is noted that the Discussion Paper proposes a "permissive framework that agencies can use to meet community needs, rather than a mandatory one compelling the sharing of information".[25] A non-mandatory enabling legal framework is supported, but it is important to understand that the Western Australian government will need to rely on *a range* of other public policy approaches to address the reluctance of public sector agencies to share information where it is appropriate.

Recommendation 5
Privacy and data sharing legislation is a necessary but not sufficient public policy response to information sharing failures. It should be supported by other initiatives that address the cultural, structural and other impediments to information sharing.

7. The need for policy clarity: balancing privacy and sharing

As noted earlier, all privacy legislation strikes a balance between 'keeping personal information in' and permitting it to be used or disclosed – 'shared'. The balance is determined by assessing the extent to which public interest factors necessitate personal information to be shared for reasons that extend beyond the purpose for which personal information was collected in the first place and without the consent of the individual concerned.

There are recognised circumstances where other public interest rights 'trump' the public interest in privacy. These include:

- lessening or preventing threats to other individuals' life, health, safety, and welfare, or threats to public safety and welfare;
- research that is in the public interest and where it is impracticable to obtain individual consent;
- the evaluation, planning, monitoring, and improvement of government services;
- the reporting, detection, and investigation of unlawful activities; and
- to support national security activities.

[25] *Discussion paper*, at p25.

More recently, the governments of South Australia, Victoria, New South Wales, and the Commonwealth have thought it necessary to broaden these categories to permit any personal information to be shared with an office of data analytics to enable data integration and analysis for the purpose of informing government policy making, service delivery, and planning,[26] subject to the important restriction that the results of the data analytics can only be disclosed in de-identified form.[27]At this stage, there is no evaluative evidence that demonstrates that these initiatives have succeeded. Anecdotally, public sector organisations in these jurisdictions remain unwilling to 'share' information with an office of data analytics because of concerns about:

- the opacity of the analytic processes;
- the unaccountable nature of the data analytics offices that are invariably established within the Department of Premier and Cabinet and which report to the Secretary of that Department rather than the Department(s) whose data is subject to the analysis; and
- the inadequacy or erroneous nature of data sources.

It is difficult to see the value of these initiatives when privacy legislation *already* acknowledges and permits the sharing of personal information for public interest research, service evaluation, monitoring, and improvement purposes.

Recommendation 6
Existing exceptions to privacy are sufficient to enable Western Australia's data sharing objectives. It is unnecessary to create additional exceptions for policy development or service improvement through an office of data analytics.

7.1. Data sharing and the 'five safes'

Under privacy laws, *if* personal information is used or disclosed for purposes that individuals are not aware of, do not consent to, or if there is no other legal authority to use and disclose personal information, *then* an interference with privacy occurs.

The Discussion Paper suggests that "a structured, risk-based, decision-making process will be provided to enable agencies to assess whether information should be shared" and goes on to suggest that the decision-making framework will be based on the 'five safes' model.

The 'five safes' originated in work done in 2003 at the UK Office of National Statistics for its Virtual Microdata Laboratory, a confidential research enclave.[28] The elements that comprise the 'five safes' are: 'safe people', 'safe projects', 'safe settings', 'safe data', and 'safe outputs'.

[26] See s5, *Victorian Data Sharing Act 2017 (Vic)*.
[27] See s19, *Victorian Data Sharing Act 2017 (Vic)*.
[28] Tanvi Desai, Felix Ritchie and Richard Welpton, *Five Safes: Designing Data Access for Research,* University of the West of England, Faculty of Business and Law, Economics Working Paper Series 1601, at p5.

The framework has been used to a limited extent in certain, mainly health, applications in the UK,[29] and has gained popularity mainly in Australia and New Zealand.

Whether or not the five safes is an appropriate effective methodology is open to question. Although a range of materials have promoted its use, we have been unable to identify any independent evaluative material that assesses its efficacy.[30] Although it has been adopted by some jurisdictional governments,[31] and the Commonwealth is considering deploying it in its proposed data sharing and release initiative, enthusiasm for it is largely confined to Australia and, to a lesser extent, New Zealand. It is not regarded as an internationally-accepted benchmark. It has not been adopted or endorsed by the European Union, the USA, or by Canada. We have been unable to locate any material produced by any privacy regulator in the world that endorses it.

The five safes framework is not, and has never been, designed to constitute the legal authority to disclose personal information. It is intended as a methodology to address risk *where the preceding legal authority to disclose personal information has first been conferred.* As such, it is designed to assess risks to determine whether personal information can 'safely' be disclosed.

Although the five safes purports to be a risk management framework, *it is not*. It assumes that the disclosure of personal information is 'safe' where each of the five 'safe' criteria apply. It mistakenly assumes that these five factors can be crystallised at the inception of a project that seeks to disclose personal information where an individual has not consented to the disclosure or where some exception to privacy is available. As such, it assumes that information risk across information sharing projects is static and fixed. This assumption is wrong because disclosure risks are dynamic. They vary on an information lifecycle basis.

For example, the five safes provides no assistance in determining what 'safe people' are. If the people are 'safe' at the inception of an information disclosure project, how will an agency determine that they are 'safe' across the lifecycle the project? How will an agency go about assessing whether 'data' (i.e., personal or sensitive information) is safe to share? At the inception of an information disclosure project it might seem that disclosure risks are minimal, but the disclosed information may be linked by the recipient with other data at some time in the future in a way that is highly intrusive and uncontrolled.

At best, the five safes is a decision-making framework, albeit a resource intensive and expensive one. At each stage of a personal information disclosure project, *all* of its elements must be consistently applied on an end-to-end and whole-of-system lifecycle basis. To provide public confidence in it as a decision-making tool it will be necessary for

[29] See, for example, Victoria Moody, *Access to Sensitive Data for Research: 'The 5 Safes'*, UK Data Service, Data Impact Blog, 5 May 2015. See http://blog.ukdataservice.ac.uk/access-to-sensitive-data-for-research-the-5-safes/.

[30] For example, there is no material provided by the Commonwealth Department of Prime Minister and Cabinet to assess or review the 'five safes' in the material it has published about its proposed Data Sharing and Release legislation. See https://www.pmc.gov.au/sites/default/files/publications/australian-government-data-sharing-release-legislation_issues-paper.pdf.

[31] For example, the *Public Sector (Data Sharing) Act 2016 (SA),* Part 4.

comprehensive operational records to be kept and maintained and mechanisms built-in for independent oversight and scrutiny through review and audit processes maintained by an independent privacy regulator. Where the five safes is misapplied or fails to support proper decision-making, individuals should be able to complain to, and seek compensation through, the privacy regulator.

Although we acknowledge that the Western Australian government is under some pressure to 'follow the leader' to adopt the five safes, we do not believe that it provides a reliable, proven, and trustworthy framework to manage the disclosure of personal and sensitive information. In our submission, the 'five safes' should *not* be adopted by or under Western Australia's proposed privacy and responsible information sharing framework.

Recommendation 7
The 'five safes' is not an exception to privacy. It is a largely untested and unevaluated decision-making framework that is of limited value to Western Australia's data sharing objectives.

7.2. Advanced data analytics

Advanced data analytics relies on the availability of large quantities of data. The use of advanced data analytics is claimed to discern patterns of behaviour in order to help make faster and better decisions based on predictions – a power that is sold as "having a superpower".[32] That said, a number of risks have been identified ranging from erroneous and incorrect results, the development of individual profiles that can be used for surveillance, behaviour 'nudging' and modification, opaque and unaccountable 'black box' decision-making, bias, and discrimination.[33]

Any advanced data analytics capability established by the Western Australian government must provide the legal authority to undertake data analytics and to account for these risks and mitigate or eliminate them. This will involve developing safety and quality requirements, effective safeguards against intrusive targeting and profiling of individuals, the provision of effective remedies, rigorous oversight and accountability mechanisms, and open and transparent disclosure of analytic processes and procedures.

Models and methodologies are being developed to facilitate this new form of risk analysis and oversight such as New Zealand's recently published draft Algorithm Charter[34] and its Algorithm Assessment Report.[35] These should be taken into account in building WA's data sharing framework and consideration should be given to embodying them, or their equivalent, into the privacy and data sharing framework from the outset.

[32] PWC, *Data: Your New Superpower.* See https://www.pwc.com.au/consulting/data-and-analytics.html.
[33] For a detailed account of these, see Frank Pasquale, *The Black Box Society,* Harvard, 2015.
[34] Statistics New Zealand, *Algorithm Charter,* October 2019. See https://data.govt.nz/assets/Uploads/Draft-Algorithm-Charter-for-consultation.pdf
[35] Statistics New Zealand, *Algorithm Assessment Report,* October 2019. See https://data.govt.nz/assets/Uploads/Algorithm-Assessment-Report-Oct-2018.pdf

Recommendation 8
The privacy and data sharing framework should include provisions that support the transparency and accountability of decision-making that uses advanced data analytics.

7.3. Data analytics: roles and responsibilities

The Discussion Paper foreshadows the appointment of a Chief Data Officer whose responsibilities would include:

- standard-setting for data sharing;
- providing tools, guidance, and expertise;
- resolving information sharing disputes between agencies;
- performing data analytics work for the public sector;
- advising on best practices for data analytics, cyber security, and privacy protection; and
- regulating a data sharing system and legislation.[36]

Some of these roles and responsibilities appear to conflict with the responsibilities that are to be conferred on the Western Australian Privacy Commissioner.

In our submission there is no compelling need to establish a *separate* office of Chief Data Officer with these functions and powers. Other than undertaking data analytics work for the public sector, each of these nominated activities are normally undertaken by an independent privacy regulator. Our view is that all of these functions could and *should* be performed by the Privacy Commissioner, with the exception of the data analytics work (a function that we regard could be undertaken by the Office of Digital Government).

Recommendation 9
The functions of the Chief Data Officer should be limited to performing data analytics work, and could likely be absorbed into the Office of Digital Government, working in a cross-government fashion. Any data analytics work should be subject to the oversight of the Privacy Commissioner.

8. Indigenous data sovereignty

The Discussion Paper acknowledges that the "… rights of Aboriginal people as custodians of their cultural information are vital in considering a model of information sharing",[37] and points to the need for Western Australia's privacy and information sharing framework to "… recognise and reflect the importance of involving individuals or communities in the way

[36] *Discussion Paper*, at p36.
[37] *Ibid,* at p40.

information is collected, managed, used and shared".[38] These objectives can be addressed in the Western Australian privacy and data sharing framework based on global and Australian activities that seek to establish, maintain, and advance Indigenous data sovereignty rights (ID-Sov) and data governance (ID-G) frameworks.

What is particularly powerful about WA taking a leadership role with respect to ID-Sov and ID-G is that these frameworks provides working use-cases for the realisation of *collective interests* in information, through placing stewardship of data – and community-driven solutions – with those most directly affected.

The global movement to develop approaches to Indigenous data sovereignty is derived from the *UN Declaration on the Rights of Indigenous Peoples 2007*[39] and seeks to ensure that Indigenous Peoples govern "… the creation, collection, ownership and application of their data."[40] The establishment of the Global Indigenous Data Alliance[41] highlights the increased interconnectivity of international networks committed to establishing mechanisms in support of ID-Sov principles across data platforms and data supply chains.

Indigenous data is data which is about and may affect Indigenous people both collectively and individually. *Indigenous data sovereignty* is considered to be:

> "… the right of Indigenous peoples to determine the means of collection, access, analysis, interpretation, management, dissemination and reuse of data pertaining to the Indigenous peoples from whom it has been derived, or to whom it relates. Indigenous data sovereignty centres on Indigenous *collective* rights to data about our peoples, territories, lifeways and natural resources."[42]

Indigenous data sovereignty is conferred and implemented through *Indigenous data governance*:

> "Indigenous data governance is decision-making. It is the power to decide how and when Indigenous data are gathered, analysed, accessed and used. It is the ability to construct a data framework that reinforce[s] [and does] not restrict Indigenous goals and ambitions."[43]

A significant body of work has been undertaken by Australian and other Indigenous peoples across the world to develop a systematic and evidence-based approach to ID-Sov and ID-G.

---

[38] *Id*.

[39] UN General Assembly Declaration *A/61/L.67 and Add.1.* See https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf. Rights to Indigenous data sovereignty flow from Articles 3, 4, 5, 15(i), 18, 19, 20(i), 23, 31, 32, 33, 38 and 42.

[40] Australian Indigenous Governance Institute, *Indigenous Data Sovereignty Communique,* 20 June 2018. See https://www.aigi.com.au/wp-content/uploads/2019/10/Communique-Indigenous-Data-Sovereignty-Summit.pdf.

[41] See https://www.gida-global.org/.

[42] Australian Indigenous Governance Institute, *Indigenous Data Sovereignty, Data for Governance: Governance of Data, Briefing Paper: June 2018,* Our emphasis. See https://static1.squarespace.com/static/5b3043afb40b9d20411f3512/t/5b70e7742b6a28f3a0e14683/1534125946810/Indigenous+Data+Sovereignty+Summit+June+2018+Briefing+Paper.pdf.

[43] *Id*.

This work includes producing a taxonomy of traditional knowledge and biocultural labels[44] that assist in identifying and ascribing rights to labelled data in cultural heritage and biological/genomic resource contexts. Institutions such as the US Library of Congress have adopted the traditional knowledge labels.[45]

In Western Australia, the Roebourne 6718 project provides a practical example: the local community wanted to have access to public sector data that was being claimed as the basis for policy interventions and specific program investments, and to be able to provide their own local analytic capacity to inform their engagement with government. This was picked up in the Yule River meeting of Aboriginal people from the Pilbara, who are motivated to develop and extend this approach. Indigenous data sovereignty also informs the work of Just Reinvest NSW, a coalition aimed at reducing the number of Aboriginal children and young people in prison. It does this by helping local communities access government-held data for the purpose of building data analytic tools to develop, implement, and evaluate local strategies reallocating public finances from criminal justice to other areas.

Our view is that this practical work could serve as the foundation for the development of a Western Australian legislative approach to providing Western Australian Indigenous peoples with increased control and governance over traditional knowledge that falls within the concept of 'personal information'. Although further consultation is required to fully establish the elements of both ID-Sov and ID-G, the Western Australian privacy and information sharing initiative can be designed to include a framework that both facilitates and is capable of implementing both. This can be achieved in the first instance by empowering the Privacy Commissioner to develop specific ID-Sov and ID-G codes in partnership with a representative Indigenous data working group. The conferral of a such a code-making power is discussed at the end of this submission. It should be emphasised that situating ID-Sov and ID-Gov in a code is an endeavour to provide flexibility to the process of enacting realisable rights and frameworks.

Recommendation 10
The privacy and data sharing legislation should include a framework that enables special rules or codes to be developed to address Indigenous data sovereignty and Indigenous data governance issues, in consultation with Indigenous peoples.

9. What would strong contemporary privacy and information sharing legislation look like? Key components

9.1. Privacy principles

[44] These are set out and explained in greater detail at http://localcontexts.org/tk-labels/.
[45] See: https://www.loc.gov/item/2015655578/ and for information about this work: https://www.loc.gov/collections/ancestral-voices/about-this-collection/.

In Australia as in other jurisdictions, privacy legislation is *principles-based*, so as to enable privacy protections to be sufficiently flexible to cover both current and future information practices, typically driven by new technologies.

The Discussion Paper states that the WA government's preference is to use the Commonwealth's *Australian Privacy Principles* (APPs) as the basis for its privacy principles.

Although consistency between the Commonwealth, other jurisdictions, and WA is desirable, the Commonwealth's APPs are designed to cover the Commonwealth public sector, the private sector on a national basis, and particular sectors such as direct marketing. As a result they include some features – for example, credit reporting and direct marketing – that are irrelevant to the functions and activities of the Western Australian public sector.

A 'fit for purpose' set of public sector privacy principles that is better adapted to Western Australia's public policy objectives can be taken from other State or Territory legislation. The most recently refreshed set of public sector privacy principles is the Territory Privacy Principles (TPPs) in the *Information Privacy Act 2014* (ACT). These reflect the most recent public sector relevant updates to the APPs including explicit openness and transparency requirements (APP1/TPP1) and requirements for dealing with unsolicited personal information (APP4/TPP4). Other State and Territory privacy principles have not been updated to reflect these improvements. We recommend that the Western Australian government adopt these principles.

Recommendation 11
The Commonwealth's *Australian Privacy Principles* are unsuitable for Western Australia's public sector. The ACT's *Territory Privacy Principles* are a more suitable model.

9.2. Information sharing under privacy principles

It is crucial to reiterate that the ACT TPPs and all of the other privacy principles that have been adopted by Australian jurisdictions already permit the use and disclosure (i.e., the 'sharing') of personal information in a variety of circumstances. In all cases, personal information can be shared (i.e., disclosed) if the individual *consents.*

Typically personal information can be used and disclosed by public sector organisations for *'secondary' purposes* (i.e., purposes that are not the primary purpose for which the personal information was collected) where the secondary purpose is 'related' to the primary purpose and the individual would 'reasonably expect' that the personal information would be used or disclosed for that secondary purpose.[46] Where sensitive information, such as health information, is concerned, the secondary purpose must be 'directly related' to the primary collection purpose.[47]

Privacy principles also permit the sharing of personal information without individual consent for research and the compilation and analysis of statistics in the public interest. For example,

[46] See, for example TPP 6.2.
[47] See, for example, TPP 6.2(a)(i).

IPP 2.1(c) of the Victorian *Information Privacy Principles* permits the use or disclosure of personal information for secondary purposes:

> "… if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual—
>
> (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
>
> (ii) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information."

Privacy principles can also enable the sharing of personal information for evaluative purposes. An example is in *Health Records Act 2001 (Vic) Health Pricy Principles* (HPPs). HPP 2.1(f) permits the sharing of personal health information for:

> (i) "funding, management, planning, monitoring, improvement or evaluation of health services; or
>
> (ii) training provided by a health service provider to employees or persons working with the organisation."

As discussed earlier, other common examples where information sharing is permitted include to enable law enforcement agencies to undertake their law enforcement functions; to investigate unlawful activity; to lessen or prevent the threats to an individual's health, safety, or welfare; and to prevent or reduce serious threats to public health, safety, or welfare.

On their face, these exemptions to the use and disclosure of personal information provide a wide latitude for appropriate information sharing that supports research, evaluation, benchmarking, and design of public sector services.

Recommendation 12
Existing and well-recognised exceptions to privacy protections cover all of the proposed data sharing activities contemplated by the Western Australian government. Further exemptions to enable data analytics to assess service delivery or to inform public policy are unnecessary.

9.3. Health information

Although the *Privacy Act 1988* covers the privacy of health information in the Commonwealth public sector and the private sector on a national basis, New South Wales, Victoria, and the ACT have developed separate health privacy legislation: the *Health Records and Information Privacy Act 2002 (NSW),* the *Health Records Act 2002 (Vic)*, and the *Health Records (Privacy and Access) Act 1997 (ACT).* Each of these enactments cover the public *and* private sectors and thus potentially conflict with the Commonwealth legislation.

There seems to be little justification for Western Australia to establish separate legislative regimes for personal and sensitive information on the one hand and another for health information.

It is submitted that the WA legislation should deal comprehensively with each of personal, sensitive, and health information within the one piece of legislation. This is consistent with the Commonwealth's approach in the *Privacy Act 1988.* There appears to be no compelling reason to establish separate privacy and health privacy regulators.

Recommendation 13
Western Australia's privacy and data sharing legislation should cover health information privacy within the one piece of legislation.

9.4. Additional rights not covered by existing jurisdictional privacy principles

Recent developments in deploying Big Data, advanced data analytics, and forms of artificial narrow intelligence (ANI) – in this submission collectively referred to as AI – have highlighted a range of privacy risks to individuals. These technologies rely on the availability of large data sets and algorithmic analysis, often employing machine-learning techniques.

Western Australia's stated commitment to greater information sharing and public sector data analytics serves as a basis for the deployment of AI to assist in service delivery and better government decision-making.

However, a range of AI-related risks have been identified. These include concerns that automated decision-making based on AI is not consistent with normal legal rules that require reasons for decisions,[48] the profiling of individuals,[49] and many documented instances where AI has made mistakes[50] or has produced decisions that are biased[51] or discriminatory.[52]

Western Australia's privacy and information sharing framework should provide for minimum protections to mitigate these risks. Some of the provisions of the *GDPR* provide a starting point.

The first is *a right to know about and to object to automated individual decision-making* (being a decision based solely on automated processing) in Articles 21(1) and 22(1) of the *GDPR*.

---

[48] s 13 *Administrative Decisions (Judicial Review)* Act 1977. See also, Ombudsman WA, *Guidelines: Giving Reasons for Decisions,* 2019, http://www.ombudsman.wa.gov.au/Publications/Documents/guidelines/Giving-reasons-for-decisions.pdf.

[49] 'Profiling' is defined in A4(4) of the *GDPR*.

[50] See, for example, Peter Fussey and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Facial Recognition Technology,* Human Rights Centre, University of Essex, July 2019. See https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

[51] For example, racial bias in healthcare algorithmic decision-making see Ziad Obermyer, Brian Powers, Christine Vogelli and Sendhil Mullainathan, *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations,* Science, Vol. 366, Issue 6464, at p447.

[52] For example, discriminatory algorithmic sentencing recommendations in the justice system: Andrew Lee-Park, *Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing,* UCLA Law Review, Law Meets the World, 19 February 2019. See https://www.uclalawreview.org/injustice-ex-machina-predictive-algorithms-in-criminal-sentencing/.

The second is *a right to meaningful information about the logic involved in automated decision-making, and the ability to seek human intervention and to contest the decision,* which is located in Articles 13(2)(f), 14(2)(g), 15(1)(h) and Article 22(3) of the *GDPR*.[53] 'Meaningful' has to be interpreted through the general information rules, Article 12 *GDPR*, and must be understandable and comprehensible for the person concerned. It also must be functional and meaningful enough to facilitate intervention, contestation, and the exercise of rights.

Recommendation 14
The privacy and data sharing legislation should incorporate some of the rights conferred by the *GDPR*, namely a right to know and to object to automated decision-making, as well as a right to a meaningful explanation that facilitates the exercise of rights.

9.5. Privacy by design

Privacy by design is a methodology for embodying privacy compliance and risk management into information systems and processes. It enables privacy to be 'built-in' and reduces the (expensive) risk of retrofitting privacy into established systems. What this means is that ICT systems are built to embody functionality that is compliant, rather than non-compliant, with privacy requirements. For example, this could include system controls that require the legislative authority for the collection of personal information to be nominated in an agency-enabled drop-down menu before personal information is collected.

Privacy by design is recommended by the Office of the Australian Information Commissioner:

> "'*Privacy by design*' is a process for embedding good privacy practices into the design specifications of technologies, business practices and physical infrastructures. This means building privacy into the design specifications and architecture of new systems and processes.
>
> It's more effective and efficient to manage privacy risks proactively, rather than to retrospectively alter a product or service to address privacy issues that come to light." [54]

It is also mandated in Article 25 of the *GDPR* as 'privacy by design and by default':

> "(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

[53] See AD Selbst and J Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233.
[54] See https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design/.

> (2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed… "[55]

Privacy by design and by default approaches to privacy risk identification, management and mitigation have become standard 'business as usual' practices throughout the jurisdictions covered by the *GDPR* and assist in ensuring that compliance issues are dealt with methodically.

Both Australian and *GDPR* approaches also recommend that public sector agencies actively manage privacy risks through undertaking privacy management programs and the use of privacy impact assessments to help agencies identify, manage, and mitigate privacy risks.

This submission recommends the inclusion of a 'privacy by design and by default' requirement into the WA legislative framework in a manner that is consistent with the *GDPR* approach.

Recommendation 15
The privacy and data sharing legislation should include a 'privacy by design and by default' requirement modelled on the equivalent *GDPR* provision.

9.6. Privacy engineering

The concept of *privacy engineering* as a means to manage and mitigate privacy and security risks has developed separately from *privacy by design and by default* and is specifically designed to address systems engineering aspects of privacy and security.

Privacy engineering is an approach to privacy and security that has been developed by the US National Institute of Science and Technology (NIST). Privacy engineering:

> "…means a specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII (personal information)… Moreover, this outcome-based focus provides the frame of reference that can facilitate translation of privacy principles into system privacy requirements."[56]

Privacy engineering is meant to 'bridge the gap' between policy and lawmakers on the one hand, and systems architects and engineers on the other. It addresses these requirements by establishing a set of engineering objectives – predictability, manageability, and disassociability—to help system engineers focus on the types of capabilities the system needs in order to demonstrate how an agency's privacy policies and system privacy requirements have been implemented.

---

[55] See Article 25 *GDPR*.

[56] National Institute of Science and Technology, *An Introduction to Privacy Engineering and Risk Management in Federal Systems,* NISTIR 8062, January 2017, at p10-12. See https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

Privacy engineering provides a basis from which ICT engineers can 'translate' the high-level principles embodied in privacy principles:

> "They [information privacy principles] are value statements rather than recipes, however. System planners often encounter difficulties when trying to operationalize them, particularly when assessing privacy risks and when establishing privacy requirements for designing and developing systems and technologies. Those activities require a well-articulated set of privacy objectives and a privacy risk assessment approach, from which privacy risks can be evaluated and implementation requirements can be developed."[57]

There is sufficient scope to embody this approach into a 'privacy by design and by default' legislative requirement along the lines of Article 25 of the *GDPR*.

Recommendation 16
As part of a 'privacy by design and by default' approach, the privacy and data sharing legislation should establish a structure within which the Privacy Commissioner can provide guidance to public sector agencies to adopt a 'privacy engineering' approach to the design and development of information systems and processes.

9.7. Organisational coverage

The Discussion Paper indicates that the 'right' organisations are covered by the legislation, that this would extend more broadly than the definition of the public sector in s3 of the *Public Sector Management Act 1994* (WA), and that it could include entities included in Schedules 1 and 2 of that Act.

The approach taken in most privacy legislation is to cover public sector organisations in the broadest sense. At a State and Territory level, this means that important components of the public sector such as *local government* are covered as well as organisations established to undertake public functions and activities that are constituted as separate entities under statute or some other mechanism. Local government plays a significant role in the day-to-day lives of Western Australians. It collects and handles large amounts of personal information, largely for the purposes of service provision. Unless it is covered by the proposed information privacy law, there will be a significant gap in the coverage of the legislation.

Privacy legislation normally also extends to cover *Universities* and other educational institutions established under statute.[58] Given that the development of public sector privacy legislation has been at least partially driven by the acknowledged need to provide an appropriate privacy underpinning for research activities in WA Universities, including health research using techniques such as data linkage, it is our submission that Universities should also be covered.

Police are subject to privacy laws in the exercise of their law enforcement functions and activities both under Commonwealth and Victorian law. Other jurisdictions exempt police law

[57] *Ibid*, at p11.
[58] See, for example, s13(1)(i) of the *Privacy and Data Protection Act 2014 (Vic)*.

enforcement functions from some or all of the privacy principles embodied in their information privacy legislation.[59]

However, information privacy laws and principles cover more than just the collection, use, and disclosure of personal information. They require that personal information held is up to date and accurate (data quality) and that it must be held securely (data security). It would seem incongruous for police to be exempt from such requirements. In our submission, police should be covered by the WA privacy and data sharing legislation but exempt from those of the privacy principles that would substantially impede their operational activities. Section 15 of the *Privacy and Data Protection Act 2014 (Vic)* provides a suitable model for such an exemption.

Community service organisations and other non-governmental entities contracted to deliver public services are generally covered within privacy and data sharing legislation under the category of 'authorised third parties', with responsibilities and protections written into funding contracts, as discussed in the section on 'Outsourcing' below.

Recommendation 17
The privacy and data sharing legislation should cover the Western Australian public sector broadly. It should extend to local government and Universities as well as to police (noting that some exceptions to collection, use, and disclosure privacy principles will be necessary to enable police to undertake their law enforcement functions).

9.8. Security

Information security has become one of the most problematic issues of the information age. The Australian Criminal Intelligence Commission estimates that the direct cost of cyber crime to the Australian economy is $1Billion annually.[60] Other estimates suggest that economic loss attributed to security breaches in Australia amount to $29Billion annually.[61] The average cost of a cyber security incident for an Australian business is estimated as $276,323.[62]

In Western Australia, the Auditor General's *Information Systems Audit Report 2019* highlighted security deficits in key business applications at four public sector entities *"…the most common of which related to poor contract management, policies, procedures and information security."*[63] The Discussion Paper recognises the need for Western Australia to improve its security posture and resilience, and outlines a series of initiatives it is undertaking to address public sector security issues.

---

[59] See, for example, ss 23 and 24 of the *Privacy and Personal Information Protection Act 1998 (NSW)*.

[60] Australian Criminal Intelligence Commission, *Cybercrime,* 2019. See https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime.

[61] Microsoft, *Direct Costs Associated with Cybersecurity Incidents Costs Australian Businesses $29 billion per Annum.* See https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/.

[62] https://www.staysmartonline.gov.au/sites/default/files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf.

[63] Office of the Auditor General Western Australia, *Information Systems Audit Report 2019,* at p4.

It also highlights the reluctance of other jurisdictions to share information with Western Australia. One of the reasons for this is because Western Australia has comparatively weak protective security policies and arrangements. In the case of sensitive law enforcement data, the Commonwealth has required Western Australia to comply with its *Protective Security Policy Framework* (PSPF) through contractual arrangements before sharing law enforcement data with Western Australian law enforcement agencies. This *ad hoc* approach to security means that parts of the Western Australian public sector that have law enforcement roles and responsibilities must contractually implement the Commonwealth's comprehensive security policy, whereas other parts need only comply with Western Australia's more limited security policies. As security threats – particularly cyber security threats – escalate, our submission is that Western Australia should respond to these by taking steps to strengthen the public sector's security posture and resilience.

More sharing of personal and sensitive information means more security risks. The development of privacy and information sharing legislation presents an opportunity to address these issues.

As noted earlier, all privacy legislation includes obligations to take *'reasonable steps'* to protect personal information from misuse and loss from unauthorised access, modification, or disclosure. These obligations have had limited effect because organisations have been uncertain about what steps are 'reasonable' and, at least at a State and Territory level, government security policy has lagged behind national policy initiatives.

In response to increasing concerns about the security of both personal information and of public sector information more generally, Victoria legislated for the inclusion of explicit protective data security in the *Privacy and Data Protection Act 2014.*[64]

Under the Victorian legislation, the Information Commissioner is empowered to develop a protective data security framework and to issue protective data security standards that bind the Victorian public sector. The legislation requires Victorian public sector organisations to comply with the standards and to develop protective data security plans, putting in place security controls that are proportionate to the security classification or labelling of public sector information to ensure that it is safeguarded. These protective security requirements apply to all public sector information.[65]

Both the *Victorian Protective Data Security Framework* (VPDSF) and the *Victorian Protective Data Security Standards* (VPDSS) take a risk-based approach to protective security. They are aligned to and consistent with the Commonwealth *Protective Security Policy Framework* (PSPF),[66] draw on guidance from the Commonwealth's *Information Security Manual* (ISM),[67] and include guidance and supporting material for the Victorian public sector.

---

[64] See Part 4 – Protective Data Security, *Privacy and Data Protection Act 2014 (Vic)*.

[65] For more detailed information, see Office of the Victorian Information Commissioner, *Victorian Protective Data Security Standards,* June 2018, https://ovic.vic.gov.au/wp-content/uploads/2018/07/VPDSS-Standards-v1.1-March-2018.pdf.

[66] See https://www.protectivesecurity.gov.au.

[67] See https://www.cyber.gov.au/ism.

The lack of an appropriate, proportional, and risk-based protective security framework in the Western Australian public sector jeopardises the public policy outcomes identified in the Discussion Paper. Additional public sector information sharing as proposed by the Discussion Paper increases the risk that information security is compromised.

In our submission, the security arrangements set out in the Discussion Paper do not effectively manage information sharing risks and do not provide adequate security benchmarks for the WA public sector. We recommend that the WA government incorporate into its privacy and information sharing legislation explicit risk-based legislative protections for protective data security, using the Victorian approach as a model.

Recommendation 18
The privacy and data sharing legislation should include explicit provisions that cover the security of all government information using a risk-based approach to strengthen the Western Australian public sector's protective security resilience.

9.9. Data breach notification

A data breach notification scheme is an essential component of a statute-based protective data security framework and should be included in the Western Australian legislation. It is an essential part of the oversight of security breaches within the Western Australian public sector and will enable the compilation of statistics to assist agencies to identify common security risks, to develop security strategies and practices, and to provide accountability so that the public are aware of risks to their personal information.

In our submission, the Commonwealth's Notifiable Data Breaches scheme would serve as an appropriate model for a Western Australian scheme.

Recommendation 19
In order to underpin enhanced protective security measures across the Western Australian public sector, a data breach notification scheme should be established under the privacy and data sharing legislation.

9.10. Outsourcing

The Discussion Paper suggests that information sharing should occur between the Western Australian public sector and '*authorised third parties*'.

All jurisdictional privacy legislation includes provisions that enable agencies to require outsourced (sometimes referred to as contracted) service providers to government, such as child protection or homelessness services or cloud computing providers, to comply with the agencies' privacy obligations to the same extent as if they were the agency. The source of the outsourced service provider's obligations is based on contractual provisions that are incorporated into the outsourcing contract.

An example of this type of approach is to be found in s 95B (and related provisions) of the *Privacy Act 1988.*

Coverage of outsourcing is necessary so as to ensure that privacy obligations are not avoided by the outsourcing of government-related functions and responsibilities to third parties and should be included in the Western Australian legislation. This is particularly important to address heightened public concern around corporate collection, use, and exploitation of personal data. Both in this respect, and in the case of community service delivery that is funded by charitable donations, philanthropy, or source income rather than by government, it is crucial to assess whether the coverage provided by outsourcing requirements is adequate and inclusive.

Recommendation 20
The privacy and data sharing legislation should enable public sector organisations to require that outsourced third party service providers comply with the legislative requirements to the same extent as the outsourcing agency.

9.11. Sharing data with community services

Not-for-profit community service providers are increasingly a source of information and support for Western Australian citizens, particularly for the most vulnerable and disadvantaged members of our community. Community members that are vulnerable and disadvantaged are more reliant on public and community services, in turn making them more likely to be of interest to researchers and policymakers. However, the community sector's capacity for data collection and analysis is often limited, and little or no provision is made in service commissioning to support and enable more effective data collection and reporting. Further, while State policy (the *Delivering Community Services in Partnership* policy[68]) commits in principle to outcome-based service contracting, in practice little or no work has been done to develop outcome frameworks, measurement tools and practices, and data protocols to ensure consistent and meaningful data collection and reporting.

Contract reporting places a significant administrative burden onto community services, and the resources dedicated to collecting, compiling, and reporting outputs detract from the time dedicated to delivering frontline services. This would be a worthwhile sacrifice if the information collected and reported was meaningful and was being effectively used and integrated by the Western Australian government or the services themselves to evaluate service delivery, improve service targeting and quality, better understand changing community need, develop best practice, and inform policy development.

However, in practice, community services report frustration that there is little or no evidence the data they provide is used by government, and it is rarely made available to those services in a composite or comparable form to enable effective service improvement. Further, digital government practices increasingly require community services to directly input reporting

68 See https://www.wa.gov.au/government/multi-step-guides/buying-community-services/getting-started-community-services-procurement/introducing-the-delivering-community-services-partnership-policy.

data into government portals that preclude subsequent access and use of data that those community services generate – often requiring them to develop parallel data systems, undertake double entry of data, or develop their own manual workarounds to maintain access to their own data.

The community service sector wants to see an evidence-driven approach to policy development, service commissioning, and funding. Investing in developing community sector capacity for better data collection and evaluation should enable us to better understand social need, design better service systems, and be better able to demonstrate the return on social investment. Information sharing cannot be a one-way street.

In our submission, the Western Australian government should commit to a principle of meaningful data collection and sharing such that the government only collects and reports service data that directly contributes to delivering better outcomes and that reflects agreed priorities (i.e. the services that individuals and the community identify as their life and wellbeing priorities). That data should be compiled and shared back with services in a usable fashion to enable better understanding of need and service improvement, and it must be shown to be used in evaluating government policy and driving funding decisions. We note that this principle has strong connections to Indigenous data sovereignty, and offers a further practical mechanism for ensuring trust and social licence for data-informed decision-making in the public sector.

Recommendation 21
The privacy and data sharing legislation should ensure that the WA government only demands and collects data from contracted social services that is meaningful for the purposes of policy development and service improvement, and it should ensure that any such data collected is compiled and shared with services in a useful and accessible fashion that demonstrably supports service improvement.

9.12. Privacy and consent among vulnerable populations

There are particular challenges in protecting the privacy rights and advancing the best interests of vulnerable individuals seeking support from public and community services. While some approaches have focused on the need to secure informed consent at the point of service delivery, information collection, or service referral, there are real questions about how 'informed' consent can truly be, when it is secured from individuals in distress and in urgent need of support. The capacity of children and young people, individuals experiencing mental health issues, or those experiencing shock or extreme distress to understand and *consent* at the point of service engagement is questionable.

Existing legislation (such as the *Children and Community Services (CCS) Act 2004*) often has provisions that relate to 'the best interests' of the child, which leaves open the question of how to determine what these best interests are. Similarly, there are provisions to enable sharing of private information when a child is at imminent risk of harm, but inquiries into child protection and harm often find information that *would* have made a difference was not shared in a timely and appropriate fashion.

These issues present particular challenges for information sharing in relation to individuals as the basis for service support or referral where they need to be *specifically identified* and personal and sensitive information needs to be shared between services to prevent harm. For example, the WA government is currently examining how it tackles this issue to meet its commitments to deliver the recommendations of the *Royal Commission into Institutional Responses to Child Sexual Abuse*. Current processes requiring information to be shared between frontline services through the Department of Communities have been found to be blocking effective information sharing, and the state is considering whether some service providers need to be defined as "authorised entities" under *the CCS Act 2004*.

A similar challenge exists in relation to the delivery of more effective and joined-up services to homeless people under the *Zero Homelessness* model developed in the US and being trialled in some Australian cities. This model necessitates sharing information about specific street-present homeless people across services so that services can quickly identify and respond to people in crisis.

A more nuanced and enduring approach to information sharing governance and service evaluation involves the active and informed participation of people with lived experience of hardship directly in the *oversight* of service systems. While it may prove problematic to get informed consent and meaningful engagement from people in crisis or distress at the point of first engagement, supporting and enabling a range of people with a diversity of lived experiences of those problems and services to inform and evaluate decision-making can provide stronger governance, greater insights, and more legitimacy to the ultimate process.

Recommendation 22
The Western Australian government should develop effective governance mechanisms that involved people with lived experience in the governance of public service design and evaluation, as well as oversight of information sharing in as many sectors as possible.

9.13. Oversight

The establishment of an Office of Privacy Commissioner is strongly supported on the basis that the Commissioner would be an independent governor-in-council appointment and that the functions and activities of the office are appropriately funded by government.

10. Functions and powers of the Privacy Commissioner

10.1. Role

The Privacy Commissioner's role should encompass activities that include promoting an understanding and acceptance of the privacy and information sharing regime; to provide general advice about privacy issues to the public sector; and to undertake the functions and activities set out in this section.

10.2. Complaints

A conciliation-based complaints-handling function with associated powers to require the production of documents is supported to ensure that those who claim that their privacy has been interfered with by a public sector organisation have access to a low-cost and effective dispute resolution process. Where conciliation fails, complainants should have a right to pursue their claim in the State Administrative Tribunal. Corresponding provisions should be included to confer this new jurisdiction on the State Administrative Tribunal. A suitable model can be found in Division 8 of the *Privacy and Data Protection Act 2014 (Vic).*

10.3. Compliance notices

The Commissioner should, on her or his own motion, have the power to serve a compliance notice where a public sector organisation breaches a privacy principle (or an applicable code of practice) and the breach is serious or flagrant. The jurisdiction to make and serve a compliance notice should enable the Commissioner to require a public sector organisation to take specified action within a specified time for the purpose of ensuring compliance with the privacy principles or a code.

In determining whether to exercise compliance notice powers the Commissioner should have the power to require the production of documents and to require a person to attend before the Commissioner to answer questions relevant to the decision to issue a compliance notice so as to ensure that she or he is properly informed of all relevant evidence and to provide the necessary powers to exercise appropriate oversight and accountability. A suitable model can be found in Division 9 of the *Privacy and Data Protection Act 2014 (Vic).*

10.4. Public interest determinations

Many Australian privacy laws empower the Commissioner to make a public interest determination.[69] This power is designed to enable the Commissioner to permit departures from compliance with privacy principles where there is a substantial public interest in doing so. In order to ensure that such departures are properly overseen by the parliament, public interest determinations should be of limited duration (e.g., 6-12 months) and, where it is considered that they should become permanent, amending legislation should be developed.

10.5. Codes of practice

The Commissioner should have the power to develop codes of practice as a flexibility mechanism to modify the application of privacy principles but only to the extent that, in aggregate, the modifications are at least as rigorous as the privacy principles.

The power to develop a code of practice should also empower the Commissioner to determine issues that may assist public sector organisations to manage privacy obligations and thus support the objectives set out in the Discussion Paper. An example of such a code is

[69] For example, Division 5, Sub-division 1, *Privacy and Data Protection Act 2014 (Vic)*.

the Office of the Australian Information Commissioner's *Australian Government Agencies Privacy Code*[70] which, for example, requires agencies to develop a privacy management plan, appoint a Privacy Officer and undertake Privacy Impact Assessments for high privacy risk projects or initiatives that involve new or changed ways of handling personal information.

[70] See https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code/.