28 October 2019

Public Sector Reform Unit
Department of the Premier and Cabinet
Locked Bag 3001
WEST PERTH WA 6872

Dear Sir / Madam,

Privacy and Responsible Information Sharing: Discussion Paper – AIIA Submission

Thank you for the opportunity to provide feedback on the Privacy and Responsible Information Sharing: Discussion Paper released for public comment by WA Department of Premier and Cabinet.

About the AIIA – WA Chapter

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, and AIIA membership fees are tax deductible. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:

- providing a strong voice of influence
- building a sense of community through events and education
- enabling a network for collaboration and inspiration; and
- developing compelling content and relevant and interesting information.

We represent technology organisations of all shapes and sizes all around Australia, including:

- Global corporations such as Apple, Adobe, Avanade, EMC, Deloitte, Gartner, Google, IBM, Infosys, Intel, Lenovo, Microsoft and Oracle
- Multinational companies including Optus and Telstra
- National organisations including Data#3, ASG and Technology One; and
- a large number of small and medium businesses, start-ups, universities and digital incubators

Some 92% of AIIA members are small and medium Australian businesses and 8% of AIIA members are large Australian companies and multinational corporations

The AIIA has six State and Territory Councils, including the WA State Council. Membership of the WA Council is representative of the wider AIIA profile and includes both large multinationals, small to medium businesses and start-ups.

At present the AIIA WA State Council includes representatives from the following sectors:

- Start-ups
- Scaleup companies
- ASX-listed and/or Multinational companies
- CRC research organisations
- ICT industry service providers
- South Australian public sector

AIIA Response:

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

   Digitisation is establishing an entirely new dynamic between the consumer, collector and custodian of data. Whilst this has enabled citizens to obtain access to services in exchange for data with relative ease, the degree of risk that such data capture entails has grown exponentially. In this context, the AIIA determines that a key consideration should be balancing individual rights to privacy against the benefits that information sharing can afford to consumers in terms of service access and provision. Every citizen should be fully informed on their data privacy rights including, but not confined to detailed information on data collection processes, including collection and retention processes, how data is shared and under what circumstances. Additionally, due consideration should also be given to citizens' rights to access personal data and the right to be forgotten.

   Another key consideration should be the ease by which individuals can assess how their privacy rights have changed over time. This will be dictated by how obligations in relation to privacy and information sharing are drafted. In relation to each new obligation it needs to be clear:

   - who has responsibility for the obligation;
   - what triggers the obligation; and
   - the content of the obligation.

   In examining these issues, the AIIA notes that due consideration will also need be given to legislative reforms at a Federal level. At the time of writing the Federal Government is currently in the process of developing legislation aimed at streamlining how public data is shared and released within the Australian Public Sector and with trusted users[1]. Additionally, the Federal Government will also be required to respond to the recommendations arising from the final

[1] Department of the Prime Minister and Cabinet – Data Sharing and Release Legislative Reforms – Discussion Paper (2019).

report of the Australian Consumer and Competition Commission (ACCC) Digital Platforms Inquiry[2]. The ACCC has recommended the Federal Government consider strengthening existing protections under the *Privacy Act*[3] and implement broader reform of Australian privacy legislation[4]. Accordingly, it is in the interests of the WA Government to ensure that any privacy and information sharing legislation enacted within its jurisdiction aligns with Commonwealth legislation.

The AIIA recommends that any legislation governing data sharing and access be consistent with those enacted in Federal and State jurisdictions and should not result in an unreasonable compliance burden or duplication of requirements.

2. *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?*

   The AIIA recommends that the OAIC Australian Privacy Principles (APPs) form the basis for any principles that may be under consideration by the WA Government. The APPs are the foundation of the privacy protection framework, and are sufficiently comprehensive to ensure they encompass multiple facets of personally identifiable information (PII) data.

   As WA is one of only two states that does not currently have a legislative framework to support these practices, the AIIA considers those successfully introduced in other jurisdictions to be pertinent examples for the WA public sector. In implementing a system which is consistent across jurisdictions it is anticipated that this will reduce any associated compliance burden and will be fit for purpose in the longer term.

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

   The AIIA affirms that a Privacy Commissioner should be empowered to fulfil its obligations and enforce legislation that affords equal protection to individuals, organisations and Governments with respect to privacy. Further, in addition to enforcement, a primary part of the Privacy Commissioner's role should be helping organisations to comply with their obligations by providing guidance and answering questions. In this capacity, the position of Privacy Commissioner should be constituted as an independent statutory office-holder, and whose roles and responsibilities would be outlined in any state privacy legislation.

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

   The AIIA recognises the inherent complexity that accompanies privacy breaches and recommends that any infringement be investigated on a case-by-case basis, so as to ensure that

[2] Australian Competition and Consumer Commission (ACCC) Digital Platforms Inquiry – Final Report (June 2019).
[3] Australian Competition and Consumer Commission (ACCC) Digital Platforms Inquiry – Final Report (June 2019) – Recommendation 16.
[4] Australian Competition and Consumer Commission (ACCC) Digital Platforms Inquiry – Final Report (June 2019) – Recommendation 17.

due consideration is given to the nuances and characteristics of individual incidents. Accordingly, the AIIA recommends that a dedicated process be developed to enable individuals and organisations to report privacy breaches directly to the Office of WA Privacy Commissioner. This process should include ongoing liaison in relation to the management of privacy breaches, including methods to ensure breaches are contained and mitigate against further incidents. Additionally, it is also recommended that privacy breaches be resolved via a conciliation process with an independent expert to act as mediator between the relevant parties.

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

The AIIA is subject to the *Privacy Act 1988 (Cth)*, which imposes limits on the manner in which organisations can use and disclose information. The Australian Government is subject to its own set of regulations in this context, the *Information Privacy Principles* (IPPs), which clearly state how public sector agencies must manage personal information. The guidance provided by the IPPs on information disclosure stipulates that a Government agency who has possession or control of personal information should not use this for any other purpose unless:

- the individual concerned has consented to use of the information for that other purpose;
- the record-keeper believes on reasonable grounds that use of the information is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
- use of the information for that other purpose is required or authorised by or under law;
- use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
- the purpose for which the information is used directly relates to the purpose for which the information was obtained.

In this context, the AIIA states that it is important to ensure that any legislation or other regulatory provisions that are enacted do not function as a barrier to information sharing. Instead, the circumstances in which personal information can be shared and with whom must be clearly defined and communicated.

Due consideration must also be given to the risk posed by data aggregation, as in agencies sharing data there is a risk of creating alternative views or insights through bringing separate datasets together that may be contrary to public interests. Data aggregation should not be at the expense of individual citizens.

6. *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?*

In a private sector organisation, the Chief Data Officer (CDO) is responsible for the utilisation of data as a company asset. This includes responsibility for determining the type of information an organisation will capture, retain and employ in its operations. Accordingly, the CDO also assumes responsibility for managing any governance and risk surrounding data use and retention. As

public sector entities have progressively transitioned to become data-driven entities, it has become necessary for them to consider the role they need to assume in creating greater public value from data, and how best to manage privacy and data usage.

Within the public sector, the role of the CDO would be similar as the position holder would still need be responsible for data management. However, the scope of this role increases to an unprecedented scale due the immense quantity of data retained by public sector entities. Whilst a Government CDO will be responsible for safeguarding public data, it will also need to be proactive in assisting agencies to make effective use of their data, provide oversight in managing privacy and protections for personal information and, most importantly, ensure that individual citizens can access public data. In order to accomplish this, it will be necessary for CDOs to work across Government departments and coordinate activities with relevant officers (i.e. Privacy Commissioner, CIOs and CTOs, FOI departments, etc.) to effectively support and manage public sector data assets. However, if the role of the CDO is to ensure that public data is used in the interests of citizens, this will need to form a core aspect in developing this position.

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

In principle, the AIIA is open to information sharing outside the WA public sector. However, in addressing issues relating to information sharing outside the WA public sector, this would need to be supported by a comprehensive data sharing framework. Such a framework would need to guide data sharing with both the private sector, as business will continue to have a role in assisting the public sector in service provision and systems development, and associated public sector agencies in other state jurisdictions. At a fundamental level, data sharing should be encouraged where:

- it provides tangible benefits to citizens (i.e. service provision and access, improved public safety, etc.);
- reduces costs and resources allocated for public service delivery; and
- does not expose data to unnecessary risk.

Additionally, it is important to emphasise the need for transparency in data sharing practices and the need to ensure citizens are fully informed of any relevant sharing frameworks and, where possible, be afforded the right to opt out.

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

The Five Safes has proven to be a useful risk assessment framework for data access and has been effective in communicating an agency's approach to ensuring privacy, confidentiality and data security. The practice of assessing each of the five risk dimensions separately and then as a whole enables data custodians to take necessary and reasonable steps to manage disclosure risks. It broadens the approach to data confidentiality by considering not just the treatment of data, but also the manner and context in which data is released.

The AIIA recommends the WA Government consider the adoption of the Five Safes as the basis for its own risk management framework.

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

   The Sharing of confidential and non-confidential information should be treated with the same respect as to consent, process and privacy controls. The only variation that should affect this is having necessary access controls in place to ensure that any information exchanged remains confidential (i.e. encryption, policies addressing sharing of confidential or sensitive information, etc.)

10. *What should the WA Government be doing to support successful implementation of privacy and information sharing?*

    The AIIA recommends that the WA Governments give consideration to three core commitments in developing a privacy and information sharing framework:

    1. **Transparency** – ensure that privacy and information frameworks are communicated to the public, and in such a way that it outlines the framework's intent and can be easily accessed and understood.
    2. **Access** – develop necessary systems to ensure that citizens are able to view any publically-held data that directly relates to them, and introduce administration process to address any requests to edit or remove personal information.
    3. **Security** – ensure there are ongoing security and governance assessments for all publically-held data, and that this is in alignment with relevant legislative and regulatory obligations.

Concluding Remarks

The AIIA recognises the importance of addressing this issue within a public sector context, as the benefits that can be derived from information sharing have the ability to enhance public service provision and can be used to develop new initiatives. However, it is essential that any strategy where public data is used for these purposes that this is complimented by a legislative framework that protects privacy and public interest.

The AIIA would welcome further opportunities to engage with the WA Government in the development of information sharing and privacy frameworks that support both the public and private sectors.

Yours sincerely,

Ms Sharon Brown
Chair, Australian Information Industry Association – WA Chapter