WA Privacy and Responsible Information Sharing

Submission – Christina Weeden

28 October 2019

Please find below my submission on WA Privacy and Responsible Information Sharing. I have read the discussion paper and attended a public information forum.

In addition to being an interested member of the WA community, I have extensive experience as an Information Management professional across public and private sectors, including defining, developing and implementing Information Management / Data Governance and Data Privacy frameworks and programs of work.

I would be very interested in further involvement in the development of WA Privacy and Responsible Information Sharing legislation and practices. For now, I offer the following observations and suggestions.

- The individual providing personal information to a WA agency is not viewed as the central actor to privacy considerations as in contemporary privacy legislation within other Australian and international jurisdictions. The discussion paper is silent on the rights of the individual and it appears that individuals will have no direct control over their personal data once collected and all decisions on its future use will rest with government staff, guided by the legislation and frameworks. This is counter to the fundamental privacy tenet - Ownership of personal information remains with the individual.
    - OECD privacy tenet
    - GDPR is based on this
    - ACCC Digital Platform Inquiry Report – Chapter 7 also calls this out

  WA Privacy legislation should align to that of other jurisdictions and explicitly acknowledge that ownership of personal information remains with the individual. At a minimum, WA should adopt the Australian legislation as well as any changes that may be made to it. (Note: the ACCC Report has suggested strengthening Australian Privacy legislation.)

- The rights of individuals have not been addressed, including consent considerations for secondary uses of personal information. Whilst collection of personal data may be required for specific primary purposes, individuals will not have direct control on whether their data is used for other purposes. If individuals have concerns about the use of their data they must work through a sophisticated complaint process.
    - The discussion paper gives examples for using data:
        - Improving government services

          How will individuals know how their data is used? What level of detail will be provided to the individual? What transparency measures will be in place?

Who will monitor agencies use of data? Will individuals actually use the sophisticated complaint processes described?

- Sharing data with relevant agencies so that individual provides data once

  If agencies need to share personal data to support primary purposes, perhaps it is more an indicator that service provision needs to be restructured/rationalised rather than sharing the data across agencies. Agencies should investigate the real problem and look for solutions other than sharing personal data.

- Research on giving consent for using personal data shows *95% of Australians surveyed want to be able to opt-out* (ACCC Report)

Privacy legislation should support Government's responsibility to educate individuals and enhance individual control over their personal information in the digital world / data economy.

Mechanisms are required to give the individual control over their personal information such as for handling requests to correct, delete, etc.; asking for consent for secondary uses of data; etc.

Use of personal data to improve government services needs many safeguards in place. The Australian government recognises this. WA government must learn from other jurisdictions.

Individuals should be able to 'opt out' of their personal data being used, at the very minimum.

Agencies should investigate the real problems/opportunities and look for solutions other than sharing personal data e.g. it may be that services may need restructuring across agencies and be delivered through 'one service organisation' e.g. Services WA.

- It appears that privacy and data sharing will be addressed in the same piece of legislation. Sharing non-personal data still needs policies, standards, protocols, etc. but should be addressed separately.

  Privacy legislation should be clear on handling personal information and not confused with data sharing in general. Otherwise misuse of personal information is likely.
  - **Keep usage of personal information separate from usage of other sorts of information**
  - **Make it simpler to interpret legislative requirements**
  - **Make it easier and more transparent for individuals to understand what is being done with their personal information**
  - **Enable future proofing of legislation – technology changes e.g. AI and privacy**

- The discussion paper takes account of WA government agencies consuming personal data from other jurisdictions (national / international); but does not acknowledge the territorial reach of other privacy legislation such as GDPR and proposed Californian Act. The implementation of privacy requirements in agencies will be unnecessarily complex if the WA legislation does not align to common privacy principles.
    - WA Public Sector is a consumer of data from other jurisdictions, thus must comply with their requirements!
    - WA Public Sector is a collector of personal information from EU residents, Californian individuals, those from Asia, etc. thus, must comply with their very strict privacy requirements!

  WA privacy legislation must align to common privacy principles otherwise agencies will have overly complex privacy implementations. At a minimum, WA should adopt the Australian legislation as well as any changes that may be made to it in order to facilitate using personal data from other jurisdictions.

- The discussion paper does not take account of the fact that WA agencies are transitioning to cloud services i.e. third party provision of ICT infrastructure and information systems. Handling of personal information will involve third party service providers.
    - Many of these service providers must comply with Australian Privacy requirements and GDPR.
    - WA agencies are still responsible for the data and must work with their third party suppliers, therefore a common privacy framework is needed.

  WA privacy legislation must align to common privacy principles otherwise agencies will have overly complex third party relationships. At a minimum, WA should adopt the Australian legislation as well as any changes that may be made to it in order to facilitate a common framework with service providers e.g. the handling of data breaches needs to be clearly articulated and aligned to common practice.

- The discussion paper does not take account of any risks, such as data breaches and unintended consequences to vulnerable individuals through poor analysis, algorithms, use of AI, etc.

  WA must align to best practices in other jurisdictions.

- There are a number of other issues that should be considered:
    - WA government should not take control away from the individual in regard to using their personal information – the government should build trust by educating individuals in how their personal information may be used and seek their permission (or, at a minimum, allow them to opt out). This approach will assist the WA community to operate safely and make good decisions in the broader digital world.
    - An individual should have a choice in how their personal information is used, beyond its primary purpose of collection. It will be difficult to address the power imbalance

between government and the individual if the individual does not agree with the government decisions and practices around the use of their personal information.

- Some elements of personal information are more sensitive requiring different levels of privacy protocols e.g. health details. Although practices may be in place to safeguard this sensitive personal information, it is important that individuals are made aware of these practices and can have a direct input or 'opt out' as the case may be. Control needs to be placed back with the individual.
- Many individuals don't have the ability to assess adverse impacts relating to uses of their personal information. Individuals should be fully informed of any proposed use of their personal information, including any risks that may be associated with that use. Individuals should be able to 'opt out'.
- Individuals should be informed about: Location tracing, online tracking, disclosure to third parties, what is inferred from internet behaviour or site behaviour. The Government should be fully transparent in what it is collecting and doing with personal information.
- De-identification of personal data still carries real risks of reidentification
- Implementation of privacy legislation can learn a lot from organisations who implemented GDPR requirements – among other matters, a comprehensive Information Management / Data Governance Program was fundamental to understanding the personal information held and how it was managed and used – many WA agencies have not yet initiated or are only just starting their Information Management / Data Governance journey.