

# **Government of Western Australia's Privacy and Responsible Information Sharing**

Discussion Paper

November 2019

## 1 Background

We provide our submissions in response to the Government of Western Australia's *Privacy and Responsible Information Sharing – Discussion Paper* (the **Discussion Paper**).

These submissions have been prepared by the Data Privacy and Cybersecurity Practice of Squire Patton Boggs (AU). Squire Patton Boggs is a full-service global law firm providing insight at the point where law, business and government meet. The Data Privacy and Cybersecurity Practice Team has substantial experience advising a broad client base, including government and local government, along with domestic and internationally publicly listed companies, large privately owned companies, not-for-profits and small business. The team acts on the forefront of advancing regulatory measures in data privacy and cybersecurity and these submissions are part of an ongoing commitment to advise on and contribute towards best practice regulatory standards and compliance across the privacy and cybersecurity space in Australia, and in particular within Western Australia.

## 2 Responses to Questions in Discussion Paper

We have addressed select questions below. Our decision not to comment on other questions should not be taken as agreement or disagreement to those propositions.

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

- 3.1 There is an inherent tension in the nature of data privacy legislation – competing interests between privacy and data use, which requires balance between maintaining individual privacy and promotion of the safe use of personal information.
- 3.2 Similar difficulties were identified during the introduction of substantive amendments to the *Privacy Act 1988* (Cth) in 2012 (the **Privacy Act**). In the course of the second reading speech for the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), Senator Wright stated that “we need to be careful that we strike the right balance between privacy rights and the free flow of information”.<sup>1</sup>
- 3.3 The Discussion Paper appears to have given detailed consideration to the benefits of data sharing between WA Government agencies and departments and even with third parties. Our recommendation is that any privacy and information sharing legislation also, and in equal measure, focusses on the maintenance of individual privacy.
- 3.4 For comparison, we refer to the objects of the Privacy Act set out in section 2A of the Privacy Act, which relevantly include (among others):
  - “(a) to promote the protection of the privacy of individuals; and
  - (b) to recognise that the protection of privacy of individuals is balanced with the interests of entities in carrying out their functions and activities”.
- 3.5 We recommend that any draft legislation put forward by the WA Government adopts analogous objects as those set out in paragraph 3.4, as a minimum.

---

<sup>1</sup> Commonwealth of Australia, Official Hansard, No. 15, 2012 page 9871.

- 3.6 Privacy legislation that acknowledges the needs and concerns of individuals will ensure that public trust and engagement is retained. The Discussion Paper identifies the public's concern as to how their information is shared and accessed. This concern is a key barrier to policy expansion where individual privacy is concerned and refer to recent examples where the Australian public has shown a general unwillingness to surrender is privacy.
- 3.7 Notably, the implementation of the Australian Government's My Health Record project culminated in significant issues on the final day to opt-out of the system. High user-traffic of individuals looking to "opt-out" lead to the website crashing, forcing the Government to extend the deadline for an additional ten weeks to meet demand.<sup>2</sup> This response was no surprise, given recent reports of government distrust from multiple sources. Figures out of Edelman's 2018 Trust Barometer global report indicates that trust in government bodies in Australia fell 2% to 35%, the lowest trust level across the previous five years.<sup>3</sup> Additionally, a report commissioned by the Unisys Corporation found that 49% of Australians did not trust the government to keep their data safe, expecting a data breach to occur within the next 12 months.<sup>4</sup>
- 3.8 To ensure that the Western Australian public is satisfied with the WA Government's privacy frameworks and trusts the Government enough to willingly provide their personal information, individual privacy concerns should be a primary focus of any proposed legislation.

**4 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?**

- 4.1 The Discussion Paper has stated that the WA Government intends to use the Australian Privacy Principles (the **APPs**), contained with the Privacy Act, as the basis for establishing regulation for the collection and use of personal information.
- 4.2 The APPs are the benchmark privacy legislation in Australia, while also representing one of the most balanced privacy frameworks currently present in an international context.
- 4.3 We support the development of new legislation with reference to the APPs and consider that doing so will promote a straightforward transition to new privacy standards in Western Australia.

**5 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?**

- 5.1 One of the objects of privacy legislation is the protection of individual. In light of data breaches, malicious use of personal information by insiders and inappropriate use of information generally – personal information can be misused regardless of the

---

<sup>2</sup> McCauley, Dana, 'My Health Record opt-out deadline extended after system crash', *Sydney Morning Herald*, 14 November 2018, <<https://www.smh.com.au/politics/federal/my-health-record-opt-out-deadline-extended-after-system-crash-20181114-p50g01.html>>

<sup>3</sup> Edelman, *2018 Edelman Trust Barometer Global Report*, <[https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018\\_Edelman\\_Trust\\_Barometer\\_Global\\_Report\\_FEB.pdf](https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf)>

<sup>4</sup> Unisys, *Australians believe telcos and government organisations more likely to suffer a data breach than other industries, Unisys research finds*, <<https://www.unisys.com.au/offers/security-solutions/news%20release/australians-believe-telcos-and-government-organisations-more-likely>>

legislative system in place or the internal controls that are implemented. To this end, the protection of individual privacy is promoted by the collection and ongoing storage of as little personal information as possible. However, as the Discussion paper has addressed, information is valuable and its use can promote innovation and discovery for public sector agencies.

5.2 We recommend that, when disclosing information outside the public sector, all reasonable efforts should be undertaken to ensure that personal information is de-identified or anonymised where possible and practical. Doing so will limit the amount of personal information that is disclosed while retaining the benefit of large data sets for use in research and development.

1.2 However, we note that de-identification of information is not infallible and should not be treated as a catch all exclusion from general privacy protections. It is well established that the de-identification of information, while effective on a superficial basis, often fails when scrutinised either internally by an individual within the organisation or externally by third parties. In summary, a number of mundane facts, when taken together, often suffice to isolate an individual. The most prominent example of this is provided as a case study in the Office of the Australian Information Commissioner (**OAIC**)’s guidance note on ‘What is Personal Information’, this example is outlined below:

- *“In 2006, AOL, a search engine provider, released apparently anonymous web search records for 658,000 users. However, some journalists working for the New York Times were able to link the search terms to identify users and contacted them. For example, “Subscriber 4417749” was able to be identified as a 62-year old woman, through her searches for local real estate agents and gardeners, her use of dating sites, health queries she had about her ‘numb fingers’ and questions about her dog’s behaviour”.*<sup>5</sup>

5.3 This example indicates that with a number of connected data points, it is possible to identify an individual without common identifying information such as that person’s name, date of birth or address. We consider that in substantial data sets, a consistent anonymised (or pseudonymised) data set will inherently disclose the identity of individuals when subject to sufficient scrutiny regardless of the de-identification process adopted.

5.4 However, the issues around de-identifying personal information only apply to ‘connected data’ sets that is data that is connected to a particular pseudonym or is connected by multiple interconnected data points. As indicated above, the more data points available for analysis, the more likely it is that an individual can be identified from such data. In contrast, the less data points available for analysis, the less likely it is that an individual can be identified.

5.5 We recommend that the WA Government adopts an approach that limits the disclosure of ‘connected data’ (i.e data connected to a government identifier or data portraying a particular individual even without an identifier) where possible and focusses on the disclosure of abstract data points which are more suitable to de-identification procedures. We consider that doing so will reduce the amount of personal information

---

<sup>5</sup> Example extracted from Michael Barbaro and Tom Zeller Jr, 2006, ‘A Face is Exposed for AOL Searcher No. 4417749’, New York Time <<http://www.nytimes.com/2006/08/09/technology/09aol.html>> , as referenced in Office of the Australian Information Commissioner, 2017, ‘What is personal information?’ <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/what-is-personal-information.pdf>

disclosed, ensure individual privacy and reduce the risk associated with cybersecurity events or data breaches by third parties.

## 6 About Squire Patton Boggs

Squire Patton Boggs is a global law firm providing insight at the point where law, business and government meet. With 44 offices across 19 countries, we offer access to expertise and invaluable connections both locally and across the world.

We provide legal and strategic advice to clients engaging with regulatory bodies at all levels and across all judicial and administrative forums. Our advice is grounded in a comprehensive and extensive understanding of the law, industry and how governments operate, including how to engage with policy makers and policy enforcers at all levels. We also help clients to assess, in advance or in real time, what government policies could affect their business interests and how to respond to those policies.

### Margie Tannock | Partner & Head of the Cyber Security & Data Privacy Team in Australia



T: [number withheld]  
E: [email withheld]

*Margie's practice focuses on advising clients from all sectors on statutory approvals, corporate governance, compliance and public law. She works closely with clients to resolve regulatory risk across all aspects of corporate decision making.*

### Connor McClymont | Associate



T: [number withheld]  
E: [email withheld]

*Connor advises clients on data privacy and cybersecurity regulatory compliance and best practice. He works with clients to implement bespoke compliance frameworks and offers advice grounded in understanding the nature of their operations.*