Office of the
Information Commissioner

Freedom of information for Western Australia

Our Ref: 07/005/01

1 November 2019

Ms Robin Ho
A/Deputy Director
Public Sector Reform Unit
Department of the Premier and Cabinet
Locked Bag 3001
WEST PERTH WA 6872

By priority post and email to: [redacted]

Dear Ms Ho

SUBMISSION IN RESPONSE TO PRIVACY AND RESPONSIBLE INFORMATION SHARING FOR THE WESTERN AUSTRALIAN PUBLIC SECTOR DISCUSSION PAPER

My office is pleased to provide the enclosed submission to the Department of the Premier and Cabinet in response to the *Privacy and Responsible Information Sharing for the Western Australian Public Sector Discussion Paper*.

While matters of policy are entirely a matter for the Government and the Parliament, my office strongly supports the Government's initiative to introduce privacy and data sharing laws in Western Australia.

I have no objection to my office's submission being made public.

If you have any questions about my office's submission, or if my office can be of further assistance, please contact me directly on [redacted] or by email at [redacted]

Yours sincerely

Catherine Fletcher

Catherine Fletcher
INFORMATION COMMISSIONER

Albert Facey House, 469 Wellington Street Perth WA 6000
Telephone: (08) 6551 7888
Freecall (WA country): 1800 621 244
Email: info@oic.wa.gov.au
Web: https://www.oic.wa.gov.au

SUBMISSION OF THE OFFICE OF THE INFORMATION COMMISSIONER (WA) TO THE DEPARTMENT OF THE PREMIER AND CABINET IN RESPONSE TO THE PRIVACY AND RESPONSIBLE INFORMATION SHARING FOR THE WESTERN AUSTRALIAN PUBLIC SECTOR DISCUSSION PAPER

On 5 August 2019 the Western Australian Department of the Premier and Cabinet (**DPC**) released the *Privacy and Responsible Information Sharing for the Western Australian Public Sector Discussion Paper* (**Discussion Paper**) and invited public comment by 1 November 2019.

The ten questions for consideration are summarised on page 47 of the Discussion Paper.

This submission is made by the Office of the Information Commissioner (WA) (**OIC**) and relates to Questions 1-6 and 10. Some of the comments made in relation to Questions 1 and 5 also relate to other questions.

In providing this submission, the OIC has sought feedback from other Australian privacy regulators on certain issues as referred to in this submission.

Q 1	**What issues should be considered when developing privacy and information sharing legislation for Western Australia?**
Q5	**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 comments below relate to Questions 1 and 5.

On 18 February 2019, the OIC gave DPC and the Attorney General an issues paper prepared by the OIC which highlighted some key issues for the Western Australian Government (**the Government**) to consider in the area of privacy and data sharing law reform (**OIC Issues Paper**). A copy of that Issues Paper is attached at Appendix 'A'. While a considerable amount of the material in that paper is contained in this submission, the OIC Issues Paper should be read as part of this submission.

The key points arising from the OIC Issues Paper were as follows:[1]

- While matters of policy are entirely a matter for the Government and the Parliament, the OIC considers that the Government should enact privacy legislation as separate stand-alone legislation to data sharing legislation.

- It is generally accepted that the protection of privacy under the common law is inadequate and that privacy legislation in Western Australia is long overdue.

- Community trust is critical to the success of data sharing legislation.

- Privacy laws should be viewed as an enabler instead of a barrier to information sharing.

---

[1] See page 2 of the OIC Issues Paper

- Data sharing models in other Australian jurisdictions may provide useful insight when designing data sharing legislation.

- Issues raised by other Australian Information Commissioners in response to the proposed Commonwealth Data Sharing and Release Legislation should be closely examined.

- Oversight of privacy laws in the majority of models in Australia sits with the Office of the Information Commissioner.

Lessons learned from other Australian privacy and data sharing laws

As observed on page 4 of the Discussion Paper, WA has the opportunity to learn from the legislative models and experiences of other jurisdictions that already have privacy and information sharing arrangements.

All Australian states and territories, other than Western Australia and South Australia, have privacy legislation governing the handling of personal information at state/territory and local government level. The *Privacy Act 1988* (Cth) (**Privacy Act**) governs the handling of personal information by Australian Government agencies, as well as certain other entities.

Three Australian jurisdictions have enacted data sharing legislation – Victoria, New South Wales and South Australia[2] – and the Commonwealth Government is currently developing and designing a new Data Sharing and Release Bill.[3] The OIC observes that the latter is timely and that the issues and concerns arising from that process can inform the development of the proposed WA legislative framework for privacy and data sharing.

In its submission in response to an issues paper released for consultation on 4 July 2018 by the Department of the Prime Minister and Cabinet (**DPMC**) on the 'New Australian Government Data Sharing and Release Legislation'(**the Cth Data Sharing Issues Paper**) the Office of the Australian Information Commissioner (**OAIC**) relevantly observed that:[4]

> [T]*here are a number of other legislative data sharing models operating across other Australian (and international) jurisdictions, all in the early stages of implementation... The OAIC notes that these models are narrowly drafted, and generally restrict the purposes for which data may be shared to those which may inform government policy making, service planning and design....They also generally provide that, unless otherwise expressly provided for, the relevant legislation does not override other relevant obligations, and in particular privacy or data protection legislation....The OAIC would recommend that the Department consider the design of these schemes as part of its design and implementation of the DS&R Bill.* [footnotes omitted]

Data sharing legislation in Victoria and New South Wales operates in the context of existing privacy legislation, as is proposed at the Commonwealth level.

---

[2] See *Data Sharing Act 2017*(Vic), *Data Sharing (Government Sector) Act 2015* (NSW), and *Public Sector (Data Sharing) Act 2016* (SA)

[3] See https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation

[4] See page 4 of OAIC submission at https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20720.pdf

The OIC notes that the newly established Office of the National Data Commissioner (**ONDC**) is 'embedding a privacy-by-design approach in how [they] develop the [proposed Commonwealth] legislation'.[5] This includes commissioning an independent Privacy Impact Assessment (**PIA**) on the proposed legislative framework that identifies its strengths and weaknesses [6] and adopting recommendations from the PIA into the framework to minimise risks while maximising benefits.

The OIC considers that the same approach should be considered by the Government in the development of the WA legislation. The OIC also submits that the Government should consider the issues, findings and recommendations contained in the PIA of the proposed Commonwealth legislation. For example, the finding on page 17 of the PIA relating to 'Social Licence' which said:[7]

> *It is likely to be difficult, but not impossible, to develop community trust, confidence and acceptance – known as a social licence – for the Data Sharing & Release Bill.*
>
> *The main obstacle is that the overall approach of the Bill imposes a mandatory scheme (for consumers) with no consent provisions. This will need to be balanced by a significant public benefit and strong privacy protections – and the successful communication of these.*
>
> *The key factors in determining a social licence will be:*
>
> *1) The extent to which compliance is included as an allowable purpose;*
>
> *2) The extent to which commercial access is allowed;*
>
> *3) The treatment of sensitive data; and*
>
> [4)] *The extent to which other privacy and security measures can counter concerns regarding the lack of consent.*

The OIC also notes that the requirement in the proposed Commonwealth data sharing laws that State and Territory users are covered by the Privacy Act, or a State or Territory law that provides equivalent protections to the Privacy Act,[8] makes the introduction of privacy laws in Western Australia essential [OIC emphasis].

Privacy and data sharing laws should be in separate pieces of legislation

The OIC's understanding is that it is currently contemplated by DPC that privacy and data sharing laws could be included together in one omnibus piece of legislation.

As observed on page 1, the OIC considers that the Government should enact privacy legislation as separate stand-alone legislation to data sharing legislation. In our view, this is a

---

[5] https://www.datacommissioner.gov.au/media-hub/privacy-design-approach
[6] Conducted by Galexia, see https://www.datacommissioner.gov.au/sites/default/files/2019-09/PIA_Proposed%20DS%26R%20Framework_2019June.pdf
[7] See above, n 6
[8] See page 31 of the *Data Sharing and Release Legislative Reforms Discussion Paper* at https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf

critical and overarching issue that needs to be decided in the development of privacy and information sharing legislation for Western Australia.

The OIC has sought feedback from other privacy regulators on whether privacy and data sharing laws should be in separate pieces of legislation. In his letter to the OIC dated 18 September 2019 (attached at Appendix 'B'), the Victorian Information Commissioner, Mr Sven Bluemmel – the former WA Information Commissioner between 2009 and 2017 – expressed the view that privacy and data sharing laws should be in separate pieces of legislation, for the reasons set out in his letter, which he advised were based on the Victorian experience of privacy and data sharing laws.

In summary, those reasons were as follows:

- Having the respective functions of the privacy regulator and Chief Data Officer set out in separate legislation signals to the public sector and the community that the work of the privacy regulator is performed independently of government.

- If the privacy regulator has oversight of the activities of the Chief Data Officer (or equivalent), incorporating both schemes under the one piece of legislation may have the perception that the privacy regulator is not independent of government.

- By creating a single law to cover privacy protection and data sharing, the two concepts may become conflated, and the protection of privacy may be viewed as having significance in respect of data sharing, but not more broadly.

- Creating stand-alone data sharing legislation would provide an express authority for public sector organisations to share data (which may include personal information) for specific purposes, signalling Parliament's intention that data be shared and used across government. In Victoria, the *Victorian Data Sharing Act 2017* has created a clear pathway for data sharing to take place, by separating the authority for data sharing from privacy law and reshaping cultural attitudes.

The OIC agrees with the views expressed by the Victorian Information Commissioner and encourages the WA Government to consider those views.

The OIC is concerned that the importance of privacy will be diluted if privacy and data sharing laws are in the same piece of legislation and that the implementation of the laws will be more confusing to public sector officers.

The OIC submits that the Government consider the reasons why all other Australian jurisdictions have introduced, or are introducing (in the case of the Commonwealth), data sharing laws as separate legislation instead of incorporating them into existing privacy legislation.

As observed by the Victorian Information Commissioner in his letter of 18 September 2019 referred to above, privacy laws around Australia and internationally provide privacy protections for individuals beyond when information about them is shared. That is, privacy laws relate to more than just the sharing of personal information. Conversely, data sharing laws relate to the sharing of information beyond merely personal information.

Privacy issues identified in OIC submission to Data Linkage Advisory Group

A summary of the privacy issues identified by the OIC in its submission to the Data Linkage Advisory Group in June 2016 can be found at pages 8, 9 and 17 of the enclosed copy of the OIC Issues Paper. They include that:

- Modern Australian privacy legislation is designed to enable the trusted collection, use and disclosure of personal information in a way that is transparent and secure.
- Privacy legislation has the potential to facilitate information sharing that respects the reasonable privacy expectations of individuals.
- Data-driven innovation requires trust, even where the data being used is not personally identifiable.
- The *Australian Privacy Index 2016* (**Privacy Index**) published by Deloitte found that 94% of consumers believe that trust is more important than convenience. The Privacy Index also noted that the most common type of privacy complaint made against public and private sector organisations was about information being used inappropriately, followed by organisations failing to secure personal information.
- Modern data analytics can allow data to be re-identified in more cases than was previously thought. This further highlights the importance of building trust in all information handling practices.
- The Australian Privacy Commissioner has consistently encouraged the concept of 'privacy by design'. Designing privacy compliance capability into information systems at the outset is likely to be more efficient than having to retrofit such capability at a later stage. Privacy legislation would provide a stable platform upon which such systems can be designed.

Building a social licence for greater data use and sharing

It is commonly observed that community trust is vital for the success of data sharing legislation.

In its submission, in response to the Cth Data Sharing Issues Paper, the Office of the Victorian Information Commissioner (**OVIC**) observed:[9]

> *Community trust is crucial for the success of* [data sharing legislation]. *To ensure community trust, the scheme should draw on principles developed in privacy law to balance the potentially competing interests of data subjects and data users.*

To this end, the OIC agrees with the following comments made by the Victorian Information Commissioner in the above submission:

[9] See https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20713.pdf, at page 1

OVIC acknowledges the need for a simple and effective mechanism for sharing government data and is supportive of using government data for evidence-based policy design.

However, such a scheme must be established in a way that accords with community expectations. If a data sharing scheme does not align with the manner in which members of the public expect their personal information to be used, it will not be met with community acceptance. Without this, the existing social license that data users such as researchers and government rely on in carrying out their current activities will be compromised. The Productivity Commission correctly stated that building community trust is a critical part of enhancing data sharing and release [Productivity Commission, Data Availability and Use: Productivity Commissioner Inquiry Report, Overview and Recommendations, No. 82, 31 March 2017, p. 2, available at: https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf]. *A data sharing and release scheme must be consistent with community expectations in order for it to be successful.*

Existing privacy law seeks to reconcile the interests of data subjects and data users. Privacy has developed mechanisms and principles to handle the tension between these potentially diverging interests. For example, the objects of the PDP Act [under section 5(a); see also section 5(b)] *expressly acknowledge the need to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information. I suggest that the proposed scheme should consider and incorporate similar principles where appropriate, including notions of necessity, proportionality, and transparency.*

In its submission in response to the Cth Data Sharing Issues Paper, the OAIC noted[10] that the OAIC's Australian Community Attitudes to Privacy Survey 2017 'highlighted that some in the community may be uncomfortable with secondary uses of information, but that people are more likely to support data sharing for some purposes [more] than others'. It also observed that the figures it quoted 'suggest that there is still some work for the Australian Government to do to build an informed community confidence in government's planned secondary uses of personal information' and referred to the concerns expressed in recent community debate in relation to the secondary uses of data collected for the purposes of the My Health Record system.[11]

Some useful observations from a number of articles from the *Mandarin* are set out in pages 14-16 of the enclosed OIC Issues Paper. They include the following:

- Information has never been easier to share than today… And thanks to advances in areas like analytics and AI, it has never been more valuable, with commentators grandly proclaiming from time to time that data is 'the new oil' of the 21st century.

- The flipside of this 'new age of information' lies in maintaining privacy without creating unnecessary barriers.

[10] See above, n 4, page 5
[11] Ibid, page 6

- Any public servant introducing new technologies in government must grapple with complexity or uncertainty surrounding privacy. This is driven by the extremely context-specific nature of applying privacy principles, and may be exacerbated by differing standards across jurisdictions, the proliferation of new technologies and international developments. However, these drivers may also assist in creating more universal privacy standards, which ensures privacy is embedded from the start of the process - rather than as an afterthought.

- A Privacy by Design approach ensures privacy is built into the process at the start, rather than being an afterthought.

- Gaining and maintaining the trust of citizens and consumers over the use of their data will be critical to realising the social and economic value from data. Trust is a complex concept and it is often said that it takes years to build up trust and only seconds to destroy it.

- To gain greater licence, both private and public organisations need to be transparent in how they manage data and how effectively they communicate its value. Trust needs to be earned and maintained. How business and government deal with privacy, security and control by an individual over their data will be pivotal to building this trust and gaining social licence.

Relevantly, the then Australian Information Commissioner and Australian Privacy Commissioner, Timothy Pilgrim said as follows, in a speech given in May 2016:[12]

> ***Simply put, a successful data-driven economy needs a strong foundation in privacy.***
>
> *Our experience and community research shows that by and large people do want their personal information to work for them, provided that they know it is working for them.*
>
> *When there is transparency in how personal information is used, it gives individuals, choice and confidence that their privacy rights are being respected.*
>
> ***Accordingly, good privacy management and great innovation go hand in hand.***
>
> *Because when people have confidence about how their information is managed, they are more likely to support the use of that information to provide better services.*
>
> *In fact, their expectations often become entirely supportive.*
>
> *Most people do expect organisations to use their information where it's necessary to provide them with the services they want or to improve on those services.*
>
> *They do expect law enforcement agencies to use information resources to stop crime and to keep people safe.*

[12] See https://www.oaic.gov.au/media-and-speeches/speeches/privacy-data-de-identification

However, people also want to know how their information is being used, who has access to it, and what that means for them in terms of their personal identity.

Accordingly, privacy law - often misunderstood to be about secrecy, is really underpinned by transparency and accountability.

And by ensuring organisations are transparent and responsible when handling personal information, privacy management strengthens customer trust.

Building this trust is key to our big data challenges - whether sought in the form of customer confidence or political mandate.

Australian Government Data Sharing and Release Draft Legislation

The submissions provided to DPMC[13] in response to the Cth Data Sharing Issues Paper include submissions from Information and Privacy Commissioners around Australia.[14] The OIC recommends that the Government considers the issues raised in those submissions, including the following, which are summarised.

Office of the Australian Information Commissioner

In its submissions the OAIC observes:

> [T]*he Australian Government also holds a vast wealth of data that is personal information about its citizens, which when linked together, can paint a rich and detailed picture of who we are as individuals....As such data is usually collected on a compulsory basis (as authorised or required by law), with individuals having little choice or control over whether to provide it, the Australian Government carries a unique responsibility when making decisions about how it should be used and disclosed.*
>
> *It is particularly important then, for any policy proposals which would use and disclose personal information for purposes beyond those originally intended at the time of collection, to have a strong public interest purpose and minimise any privacy impacts. Further, the social licence and level of community support for data sharing activities under a new scheme will need to be considered carefully throughout the design and implementation of the scheme. Ensuring that the privacy impacts of the scheme are minimised will help to build this social licence and trust [OIC emphasis].*[15]

The OAIC's key recommendations, in summary, were:

1. Data sharing should occur on a de-identified basis wherever possible, to minimise the privacy impacts of the scheme for individuals.

2. The scope and purpose of data sharing legislation should be defined as clearly and narrowly as possible in order to minimise the impact on privacy.

---

[13] Available at https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms/submissions
[14] This office did not make a submission.
[15] See above, n 4, pages 1 and 2

3. The existing privacy protections for Commonwealth-held data should be maintained as far as possible, including the preservation of the OAIC's regulatory remit as the national, independent privacy regulator. This will help ensure accountability, and also avoid duplication, inconsistency and regulatory burden. The standards set out in the Commonwealth Privacy Act should remain the baseline, and any new arrangements under data sharing legislation should be developed in a way that ensures consistency with the existing regulatory requirements under the Privacy Act [OIC emphasis].[16]

The OAIC also noted that '[t]here is significant complexity and risk involved with the publication of unit record level data derived from personal information'.[17] The OAIC expressed the view that 'open data environments are generally only appropriate for information that is either not derived from personal information, or information that has been through an extremely robust de-identification process…that ensures…that no individuals are reasonably identifiable'.[18]

Office of the Information Commissioner, Queensland

The Office of the Information Commissioner Queensland (**Qld OIC**) noted in its submission[19] that:

> *Striking the right balance between greater data availability and use and the protection of an individual's privacy and personal data is critical to realising the benefits of data, achieving greater openness and transparency and enhancing levels of trust in government.*

On the issue of de-identification, the Qld OIC noted that '[i]n October 2017, the UN Special Rapporteur on the Right to Privacy presented to the General Assembly the interim report of the work of the Taskforce on Big Data Open Data - the first of the thematic reports to be presented to the General Assembly'. The Qld OIC noted that the Special Rapporteur was considering a range of recommendations regarding publication of data about individuals; that 'the recommendations contained in the final report may have implications for the public release of de-identified data'; and that 'there is ongoing debate about the effectiveness of de-identification due to the increased risk of re-identification as more data becomes available'. [20]

Information and Privacy Commission New South Wales

In its submission,[21] the Information and Privacy Commission New South Wales observed that:

> *From a privacy perspective, the community expectation is that any datasets that contain personal or health information will be handled in accordance with privacy legislation. Many citizens would have significant concerns should their personal and/or health*

---

[16] Ibid, pages 3 and 4
[17] Ibid, pages 6 and 7
[18] Ibid
[19] See https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20706.pdf at page 2
[20] See page 3 of the submission. The final report of the UN Special Rapporteur was submitted to the General Assembly on 17 October 2018 and is available at https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/Issues/Privacy/SR_Privacy/A_73_45712.docx&action=default&DefaultItemOpen=1
[21] See https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20726.pdf at pages 4 and 5

data, often compulsorily collected by government in exchange for access to payments or services, ...be made available to other government agencies or private sector organisations for purposes separate to that for which it was collected, or to conduct research which may commercially benefit private entities, in circumstances where they have not consented to, or been notified of, that disclosure. More broadly, individuals may not support their data being used for secondary, unspecified purposes which they view as having no clear personal or public benefit.

It is clear from recent media coverage of the commencement of the "opt-out" period for the My Health Record, and the strong concerns expressed about the use of, and access to, health information by other government agencies, that the community has concerns about certain types of government use and sharing of information. To build trust and support, governments must be transparent about the intended uses of data, particularly when there is the ability for personal or health information to be used for purposes beyond those for which it was collected.

Taking a proactive 'privacy-by-design' approach, which aligns data sharing frameworks with privacy requirements from the outset, will assist in building trust in the community and between public sector agencies [OIC emphasis].

Office of the Victorian Information Commissioner

In addition to OVIC's submissions already noted at pages 5 and 6 of this submission, OVIC submitted, among other things, that '[r]elying on de-identification of personal information carries with it significant challenges and risk and is unlikely to be appropriate in a data release context'. [22]

Australian Government Data Sharing and Release Legislative Reforms Discussion Paper

Following consideration of submissions made in response to the Cth Data Sharing Issues Paper and further consultations, in September 2019 DPMC released for public comment the 'Data Sharing and Release Legislative Reforms' Discussion Paper (**the Cth Discussion Paper**). The OIC submits that the Government should consider the issues and concerns raised in the Cth Discussion Paper which include the following:

- Any public data sharing arrangements should be underpinned by enhanced safeguards, privacy and security protections.[23]

- Transparency of activities enabled by data sharing legislation is key to building trust.[24]

- The office with oversight of the new data sharing system – the ONDC – should have a dual role: championing greater data sharing while promoting safe data sharing practices. This office should also be empowered to apply strong penalties to intentional or negligent

[22] See above, n 9, page 1. For further information on the limits of de-identification of personal information, see OVIC's publication 'Protecting unit-record level personal information - The limitations of de-identification and the implications for the Privacy and Data Protection Act 2014' available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf

[23] See page 1 of the Cth Discussion Paper

[24] Ibid, page 35

misuse and should cooperate with other regulators, including the Australian Information and Privacy Commissioner[25] [this point also relates to Question 6 regarding the role of the Chief Data Officer].

- The risks of eroding individuals' privacy, the importance of protecting the personal information government collects compulsorily, and the expectation that government be accountable and transparent in its data use.[26]

- Concerns about the legislation overriding existing data secrecy provisions.[27]

- Broad support for cooperation between the Australian Information and Privacy Commissioner and the National Data Commissioner to address the 'grey areas' between freedom of information, privacy and data sharing laws.[28]

- Stakeholders warned against duplication of roles with existing regulators and asked for consistent definitions to reduce possible confusion with the Privacy Act.[29]

- Frequent and recurring debates about de-identification and the difficulty of ensuring information is appropriately de-identified, leading some to suggest the term be retired entirely.[30]

- Competing views on the issue of consent and the importance of being clear on how consent is understood and integrated into a data sharing scheme 'to ensure the public is not taken by surprise'.[31]

- A considered approach to Indigenous data is important.[32]

- Concerns about the purposes for sharing data, with general consensus around the use of public sector data for improving policy, program evaluation, service delivery and research and development, with opinions divided in relation to compliance and commercial purposes.[33]

- Strong support for the publication of Data Sharing Agreements to increase the transparency of how public sector data is used.[34]

- Anyone handling personal information under the Data Sharing and Release legislation is required to meet the Privacy Act or equivalent obligations, including the Australian Privacy Principles relating to privacy notification requirements and security standards.[35]

---

[25] Ibid, page 5
[26] Ibid, page 6
[27] Ibid, page 7
[28] Ibid, page 7
[29] Ibid, page 7
[30] Ibid, page 7
[31] Ibid, page 7
[32] Ibid, page 7
[33] Ibid, page 8
[34] Ibid, page 9
[35] Ibid, page 32

- The Notifiable Data Breaches Scheme in the Privacy Act will continue to apply to personal information shared under the Data Sharing and Release legislation.[36]

- Existing mechanisms to make a complaint to the OAIC under the Privacy Act will apply to the suspected mishandling of personal information under the Data Sharing and Release legislation.[37]

The OIC also suggests the Government consider the issues and concerns raised in submissions made by other Australian Information and Privacy Commissioners or regulators in response to the Cth Discussion Paper, noting that the closing date for submissions was 15 October 2019. A copy of the submissions published by the OAIC and OVIC on their respective websites are attached at Appendix 'C' and 'D'. Some of the issues and concerns raised in those submissions are set out below.

From the OAIC's submission dated 17 October 2019:

- It is important to ensure that there is a strong public interest case for a policy proposal that authorises the use and disclosure of personal information for purposes beyond those originally intended at the time of collection. Laws that authorise acts or practices that may otherwise breach privacy laws must be necessary, reasonable and proportionate to achieving a legitimate policy objective.

- Privacy safeguards should be consistent, clear and enforceable.

- A key safeguard to minimise privacy impacts of the proposal will be to ensure that the scope and purpose of the authorising legislation is clearly and narrowly defined.

- A constrained purpose test will assist in ensuring that any subsequent impacts on individual privacy are reasonable, necessary and proportionate to achieving a legitimate policy objective with a strong public interest purpose. Additional consideration could be given to the purpose test through the Explanatory Memorandum, to clearly set out the rationale of the test, any operational limitations and provide examples as appropriate.

- The use of government held personal information for commercial purposes raises additional privacy impacts that would warrant a cautious and thorough consideration through a separate Privacy Impact Assessment and further public consultation, to ensure that community trust in the system is maintained.

- The OAIC's Australian Community Attitudes to Privacy Survey 2017 indicated that 86% of Australians considered a secondary use of their personal information (use for a purpose other than the original purpose it was provided for) to be a misuse of their personal information, but 46% of Australians were comfortable with government agencies using their personal details for research or policy-making purposes.

- Data safeguards and protections introduced by the Data Sharing and Release legislation should at least be commensurate with those under the Privacy Act, which provides the

[36] Ibid, page 37
[37] Ibid,page 51

basis for nationally consistent regulation of privacy and the handling of personal information.

- Data sharing should occur on a de-identified basis where possible, to minimise the privacy impacts of the scheme for individuals. Where it is not possible to use de-identified information, consideration should be given to whether it is reasonable and appropriate to seek consent.

- A consent-based model may be appropriate in relation to the proposed service delivery purpose. This would be in line with the objective of providing individuals with greater control over the handling of their personal information.

From the OVIC's submission dated 15 October 2019:

- While a purpose test is valuable to ensure that data shared is used for the benefit of the community, in deciding whether the purpose test is satisfied, consideration should also be given to other potentially competing public interests, such as the public interest in protecting individuals' privacy.

- Sharing for commercial purposes should be in the public interest and, importantly, meet community expectations; DPMC should consider additional safeguards where data sharing for commercial purposes is enabled under the Data Sharing and Release legislation.

- A key message to promote in any guidance issued to entities is that the Data Sharing Principles do not displace entities' obligations to adhere to privacy principles under any applicable privacy legislation; rather, it should be promoted that the Data Sharing Principles complement, not replace, privacy principles relating to information sharing under the Privacy Act or State or Territory privacy legislation.

Data Sharing models in other jurisdictions

While not recommending any particular model, the Government may wish to consider the following features of the *Victorian Data Sharing Act 2017* (**VDS Act**):

- The VDS Act promotes data sharing across government by:
    - Creating a clear framework for sharing and using data for policy making, service planning and design
    - Establishing the Chief Data Officer (**CDO**) who leads the Victorian Centre for Data Insights (**VCDI**) in working to transform how government uses data.
- The VDS Act provides a range of protections and safeguards, including:
    - Requiring all data to only be used for informing policy making, service planning and design
    - Providing for how identifiable data should be handled

- Annual reporting and notifying of possible breaches to the OVIC and the Health Complaints Commissioner (**HCC**)
- Providing that existing obligations under privacy laws continue
- New offences for unauthorised access, use or disclosure of information.[38]

- The VCDI employs a number of privacy-enhancing techniques including:
  - express privacy and data security safeguards under the VDS Act, including mandatory breach notification and annual reporting requirements to OVIC;
  - an additional layer of protection for data analytics conducted in a controlled environment, ensuring that reasonable steps have been taken to ensure that data no longer relates to an identifiable individual or an individual who can reasonably be identified before data analytics work commences;
  - the provision of a clear legislative framework for the sharing of public sector data only, as distinct from the release of public sector data; and
  - the employment of the Five-Safes Framework in the context of a secure environment to conduct data analytics.[39]
- The VDS Act interacts with privacy laws in the following way:
  - Privacy laws allow identifiable data to be shared where this is authorised by another Victorian law.
  - The Act works within privacy laws by providing a new 'authorisation by law' for sharing and using identifiable data (in addition to existing privacy exceptions). Otherwise, obligations under privacy laws (including the information and health privacy principles, and the Victorian Protective Data Security Framework and Standards) continue to apply. This means that the sharing of data that is already allowed under privacy laws is not affected.
- The OVIC plays an express oversight role over the VCDI:
  - The interaction between the VDS Act and the *Privacy and Data Protection Act 2014 (Vic)* (**PDP Act**) is clearly outlined under section 24 of the VDS Act.
  - The CDO must report annually to Victoria's privacy regulators: the OVIC and HCC. This report must include matters, such as the steps taken to ensure compliance with privacy laws, the data projects that have been undertaken, details of data requests and refusals, and the issues and challenges that have arisen.

---

[38] See '*Victorian Data Sharing Act 2017, Guidance for departments and agencies*' available at: https://www.vic.gov.au/system/user_files/Documents/vcdi/Victorian%20Data%20Sharing%20Act%202017%20Web%20Guidance%20UPDATE%20as%20at%2020%20Feb%202018.pdf

[39] See above, n 9, page 3

- The VDS Act also requires the CDO and departments (as data analytics bodies) to report any breach of privacy laws to the privacy regulator (OVIC and HCC) and the original data provider.

- In order to strike a balance between data sharing and privacy considerations, the VDS Act creates two new offences:

  - a general offence for unauthorised access, use or disclosure of data or information (with a penalty of 2 years imprisonment or 240 penalty units or both)

  - a more serious offence where the person knows or is reckless that the data or information may be used to endanger life or safety, assist in committing an offence or impede justice (with a penalty of 5 years imprisonment or 600 penalty units or both).

The OVIC has combined oversight of privacy, data protection and freedom of information in Victoria, and administers the PDP Act and *the Freedom of Information Act 1982* (Vic). The Victorian Information Commissioner's legislative responsibilities include commenting on matters affecting the personal privacy of individuals, and ensuring that the objects of the PDP Act are upheld.

Notifiable Data Breach Scheme

The OIC submits that the Government should consider the inclusion of a mandatory reporting scheme for data breaches in the Western Australian privacy legislation.

As observed earlier, proposed Commonwealth data sharing laws will require that State and Territory users are covered by the Privacy Act, or a State or Territory law that provides equivalent protections to the Privacy Act[40] [OIC emphasis]. Equivalent privacy protections are stated as including data breach notification requirements. The OIC agrees with the observation made by OVIC in its submission to DPMC (see Appendix D), that it is difficult to see how this requirement will operate in practice if State privacy legislation does not contain mandatory data breach notification requirements similar to the Notifiable Data Breaches Scheme under the Privacy Act.

As noted in the OIC's comments in response to Question 4 of the Discussion Paper, the NSW government is currently looking at whether a more robust reporting scheme is needed in NSW. In July 2019, the NSW Department of Communities and Justice released a discussion paper titled 'Mandatory notification of data breaches by NSW public sector agencies', [41] which sought feedback on whether a mandatory reporting scheme for data breaches should be adopted under the *Privacy and Personal Information Protection Act 1998* (NSW). The Government may wish to consider the issues raised in that discussion paper and the submissions made in response (noting that submissions closed on 23 August 2019).

---

[40] See page 31 of the *Data Sharing and Release Legislative Reforms Discussion Paper* at https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf

[41] See https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/mandatory-data-breach-notification.aspx

Privacy Code

The OIC submits that the Government should consider the introduction of a privacy code similar to the Australian Government Agencies Privacy Code (**the Code**) which commenced on 1 July 2018. In summary:

- The Code sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2.
- The Code requires all Australian Government agencies subject to the Privacy Act (except for Ministers) to:
    - have a privacy management plan
    - appoint a Privacy Officer, or Privacy Officers, and ensure that particular Privacy Officer functions are undertaken
    - appoint a senior official as a Privacy Champion to provide cultural leadership and promote the value of personal information, and ensure that the Privacy Champion functions are undertaken
    - undertake a written Privacy Impact Assessment (**PIA**) for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information
    - keep a register of all PIAs conducted and publish this register, or a version of the register, on their websites
    - take steps to enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information.[42]

Application of laws to local government

Page 26 of the Discussion Paper notes that the WA legislation could apply to local government, among other entities. The OIC has asked other privacy regulators whether their respective jurisdictions privacy and/or data sharing laws apply to local government. The responses received confirmed that privacy laws in Queensland, Victoria and New South Wales apply to local government. As observed by the OVIC, [43]

> *Councils often have a very direct relationship with their constituents, perhaps more so than any other level of government. The personal information held and used by local government can directly affect people's lives. Ensuring that this information is appropriately protected is an important component of privacy law and a critical function of a privacy regulator, and I would encourage the extension of a WA privacy law to local government.*

---

[42] See https://www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/
[43] See OVIC's letter dated 18 September 2019 at Appendix B

The OIC agrees that it is important that privacy laws in WA apply to local government. The inclusion of local government in any legislative privacy or data sharing regime will give local government agencies greater clarity regarding the circumstances in which the sharing of information with other government agencies is appropriate.

Consequential amendments to the FOI Act

The OIC notes that a significant issue that will need to be addressed in the development of privacy and data sharing laws in Western Australia is how those laws will intersect with and affect the operation of the *Freedom of Information Act 1992* (WA) (**the FOI Act**). This includes the issue of whether the rights to access and amend personal information will remain in the FOI Act or be transferred to the new privacy legislation. The OIC welcomes the opportunity to be consulted further on those issues.

Q 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 starting point for the operation of privacy protection is to identify the kind of information about an individual, to which a regulatory regime will apply. The term 'personal information' is defined in the Glossary to the *Freedom of Information Act 1992* (WA) (**FOI Act**) to mean:

> [I]*nformation or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead –*
>
> *(a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or*
>
> *(b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.*

That definition makes it clear that any information or opinion about an individual whose identity is apparent – or whose identity can reasonably be ascertained from the information or opinion – is, on its face, personal information.

The definition of 'personal information' in the FOI Act is used in the Discussion Paper. That definition should be retained in (or at least kept consistent with) privacy legislation to ensure the effective operation of both the principles governing access to information and the principles governing the protection of privacy.

In the Commonwealth, and in most states and territories (WA and SA being the exceptions), the protection of personal information (or 'privacy') is regulated through a legislative framework that incorporates statutory information privacy and health records laws.[44] In nearly all of those jurisdictions there is a separate (but, arguably, complimentary) access to information legislative framework (such as FOI or RTI). Only in the NT is there an

[44] Moira Paterson, *Freedom of Information and Privacy in Australia Information Access 2.0,* 2nd edition, LexisNexis Butterworths, 2015, at p.28.

'omnibus' single piece of legislation which has combined information privacy, FOI and public records laws into one Act.[45]

The Privacy Act states in section 3 that:

> *It is the intention of the Parliament that this Act is not to affect the operation of a State or Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer personal information.... and is capable of operating concurrently with this Act.*

According to the Australian Law Reform Commission, the above provision makes it clear that the Commonwealth Parliament did not intend to 'cover the field' and to override state and territory laws relating to the protection of personal information if such laws are capable of operating alongside the Privacy Act.[46]

The objects clause in the Privacy Act [47] refers to the following list of objectives:

a) to promote the protection of the privacy of individuals;

b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities;

c) to provide the basis for nationally consistent regulation of privacy and the handling of personal information;

d) to promote responsible and transparent handling of personal information by entities;

e) to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected;

f) to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected

g) to provide a means for individuals to complain about an alleged interference with their privacy; and

h) to implement Australia's international obligations in relation to privacy.

The Privacy Act applies the Australian Privacy Principles (**APPs**) as the basis of the regulation of protection of personal information held by federal government agencies and some private bodies (collectively referred to as an 'APP entity'). These obligations arise where an APP entity collects or holds personal information. These principles are said to establish 'fair information-keeping practices'.

---

[45] The *Information Act 2002* (NT).
[46] *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, accessed at https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/.
[47] Section 2A *Privacy Act 1988* (Cth)

According to the OAIC:[48]

> *The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988 (Privacy Act). They apply to any organisation or agency the Privacy Act covers.*
>
> *There are 13 Australian Privacy Principles[49] and they govern standards, rights and obligations around:*
>
> - *the collection, use and disclosure of personal information*
> - *an organisation or agency's governance and accountability*
> - *integrity and correction of personal information*
> - *the rights of individuals to access their personal information*
>
> *The Australian Privacy Principles are principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies.*
>
> *A breach of an Australian Privacy Principle is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.*

The APPs are the result of an amalgamation in 2012 of the previous public sector Information Privacy Principles (**IPPs**) and the private sector National Privacy Principles (**NPPs**). Some privacy advocates take the view that the re-wording of the NPPs has resulted in a lower level of protection than was previously available.[50]

Whilst it is also the case that there are various exemptions that operate to limit the application of the APPs they may, on the other hand, also be supplemented by approved APP Codes.[51] An actionable interference with the privacy of an individual occurs if the entity breaches one or more of the APPs, unless it is subject instead to an approved APP Code. The federal Privacy Commissioner also has the power to waive the application of one or more of the APPs through a public interest determination.[52]

Most of the APPs apply to entities generally, but some impose specific obligations only on particular federal government agencies[53] or certain private sector organisations.[54]

---

[48] https://www.oaic.gov.au/privacy/australian-privacy-principles/

[49] Refer to the *Australian Privacy Principles quick reference.* Accessed at https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/

[50] Moira Paterson, *Freedom of Information and Privacy in Australia Information Access 2.0,* 2nd edition, LexisNexis Butterworths, 2015.

[51] Paterson suggests that reference should be had to the APP Guidelines which explain the operation of the APPs and provide a detailed examination of the exceptions to the APPs.

[52] Paterson says that the public interest determination is subject to Parliamentary disallowance and this is an important safeguard.

[53] For example, see APP clause 3.4 (d)(i) which refers to the " Immigration Department".

[54] For example, see APP clause 7.5 (a) which refers to "..a contracted service provider for a Commonwealth contract.."

The OAIC provides significant guidance around the interpretation and application of each of the APPs.[55]

Other jurisdictions in Australia have also based their own privacy principles on the APPs. Some of these have modified the APPs to suit their local laws and provide relevant state based exemptions. This submission will not attempt a comparison of all the various state and territory laws. A useful comparison of some of the jurisdictions is provided by Moira Paterson in her 2015 text '*Freedom of Information and Privacy in Australia Information Access 2.0*'. [56]

After an extensive review of the operation of the privacy laws and associated privacy principles (which Paterson collectively refers to as "the Information Privacy Acts") she says:[57]

> *The Information Privacy Acts share a number of similar features. They are based on sets of information privacy principles loosely derived from the OECD guidelines, they are administered by a Commissioner, and they provide for enforcement procedures that emphasise conciliation but also allow for the making of legally binding orders, including orders for the payment of compensation. They also create offences for corrupt conduct.*
>
> *None of the Information Privacy Acts contain an explanation of why the protection of personal data is important. The* [Victorian] *Act differs from the others in that it contains such an objects clause, but this simply refers to the 'responsible' collection and handling of information.*
>
> *The failure to clearly articulate the significance of privacy as a means of protecting individuals against abuse of power and as a precondition for the exercise of other important rights, such as freedom of expression, creates the danger that it will be allowed to give way to other competing interests, including commercial interests. This is significant, as the collection, matching and analysis of large quantities of personal data enhances the efficiency of both governments and private sector bodies. While privacy needs to be balanced against other competing interests, it is important that it should be given appropriate weight when finding the appropriate balance. The current drafting of each of these Acts arguably gives insufficient precedence to values that underlie the concept of privacy, and fails to ensure that the decision is interpreted so as to further the objective of preserving individual privacy*
>
> ....
>
> *A further shortcoming that is common to all of the Information Privacy Acts is the extent to which they are limited in their application to publicly-available information. That exclusion arguably has the potential to considerably undermine their potential to protect information, given the extent of information that is potentially available from public sources*
>
> ....
>
> *Another issue of concern is the fact that these laws do not form part of a broader Australia-wide privacy regime. Modern technology makes it possible for information to*

---

[55] Refer to the OAIC website at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/.

[56] Moira Paterson, *Freedom of Information and Privacy in Australia Information Access 2.0*, 2nd edition, LexisNexis Butterworths, 2015.

[57] Paterson, at pp.38 - 39.

be transferred quickly and at low cost across the boundaries of different jurisdictions and between the private and public sectors. However, the handling of personal information is subject to different rules in the private and public sectors, and there are parts of Australia that lack such rules altogether. There are also significant parts of the private sector and significant categories are private sector information that remain outside the scope of the private sector provisions in the Privacy Act.

Paterson provides further comparative commentary concerning the protection afforded for privacy under the Commonwealth,[58] NSW[59] and Victoria[60] Acts. She says:

> *Privacy protection under the* [NSW] *Act compares unfavourably with that available under the APPs in the Privacy Act. This is in part due to the large number of exceptions that* [the NSW Act] *contains and in part due to specific shortcomings with the* [Information Privacy Principles in that Act][61] ....
>
> *The* [Victorian Act] *compares favourably with the other Information Privacy Acts. It is not subject to the same broad exceptions and it has a comprehensive set of* [Information Privacy Principles].[62]

Based on the above commentary and a reading of the various Information Privacy Acts, this office submits that Western Australia's privacy framework should adopt a set of privacy principles along the lines of either the APPs in the Commonwealth Act or the IPPs in the Victorian Act. The Victorian IPPs (which apply to Victorian agencies) are perhaps more readily transferred to the Western Australian context. There is also an added attraction that the Victorian Act, having been enacted in 2014, is more recent (and therefore more contemporary) than the most recent amendments made to the Commonwealth Act (in 2012).

In any discussion of what principles of protection are appropriate for data and personal information in Western Australia, it is also appropriate to consider the possible application of the EU's General Data Protection Regulation (**GDPR**) which came into effect in May 2018. This law aims to harmonise data privacy laws across Europe and replace the data protection rules that existed up to that time. As an overview of the GDPR it has been written that the:

> *....data privacy principles of the GDPR are fairly straightforward. The law asks you to make a good faith effort to give people the means to control how their data is used and who has access to it. To facilitate this, you must transparently and openly provide them with the information they need to understand how their data is collected and used. And you have to make it simple for your customers and users to exercise the various rights (of access, of erasure, etc.).*[63]

The GDPR and APPs share many common features, however there are also some significant differences between the two regimes. Some important differences include added protections under the GDPR such as rights relating to data portability, automated decision-making and the erasure of personal data.

---

[58] *Privacy Act 1988 (Cth)*
[59] *Privacy and Personal Information Protection Act 1998* (NSW)
[60] *Privacy and Data Protection Act 2014* (Vic)
[61] Paterson, at p. 146.
[62] Paterson, at p. 151.
[63] *A Guide to GDPR Data Privacy Requirements*. Accessed at https://gdpr.eu/data-privacy/.

The GDPR is also designed to have extra-territorial reach. As explained by the Queensland Office of the Information Commissioner:

> *Although the GDPR is a European privacy law, it could apply to Australian businesses and government agencies that offer goods or services to, or monitor the behaviour of, individuals in the EU.*[64]

There have been recent calls in this country for the standards of privacy protection to be lifted to a standard even higher than that offered by the GDPR due to the risks that digital technology and artificial intelligence pose to the security of personal information. Fiona McLeod SC, former President of the Law Council of Australia and also former chair of Transparency International, in her Solomon Lecture Address given in Brisbane in August 2019[65] said:

> *At a minimum we should be adopting EU standard terms for data protection which focus on information related to identity, including information that is "identifiable". The inadequacies of the GDPR are already being revealed, so we have an opportunity to refine those regulations and set the benchmarks here.*

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

Privacy legislation in other jurisdictions provides guidance in determining the role of the Privacy Commissioner. As noted in these submissions, all Australian States and Territories, other than Western Australia and South Australia, have privacy legislation governing the handling of personal information.

Victoria, New South Wales and South Australia also have data sharing legislation and the Commonwealth is developing and designing a new data sharing regime.

The primary function of the Privacy Commissioner should be to regulate the handling of personal information and to protect the privacy of individuals. Please also refer to the submissions under Question 10 for further discussion on the powers of the Privacy Commissioner.

The role of the Privacy Commissioner should include similar general functions to other state jurisdictions. For example, section 36 of the *Privacy and Personal Information Protection Act 1998* (NSW) sets out the particular functions of the Privacy Commissioner in New South Wales.[66]

---

[64] Office of the Information Commissioner of Queensland website page, *GDPR & Queensland Government Agencies*. Accessed at https://www.oic.qld.gov.au/about/news/gdpr-and-queensland-government-agencies.

[65] The 2019 Solomon Lecture hosted by the Office of the Queensland Information Commissioner, presented by Fiona McLeod SC. Transcript accessed at https://www.oic.qld.gov.au/__data/assets/pdf_file/0003/40746/2019-Solomon-Lecture-transcript.pdf.

[66] https://www.legislation.nsw.gov.au/#/view/act/1998/133/part4/div2/sec36

Broadly, the Privacy Commissioner should have the following functions:

- To receive, investigate and conciliate complaints from individuals about alleged breaches of privacy by an agency in order to protect privacy rights.
- To promote an understanding and acceptance of privacy principles and responsibilities and the objects of the privacy laws in Western Australia in order to bring about cultural change and best practice associated with privacy requirements.
- To conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate.
- To identify and report on breaches of privacy.
- To oversee information handling in the public sector, including oversight of the activities of the Chief Data Officer (**CDO**). For example, in Victoria, under the *Data Sharing Act 2017* (Vic)(**VDS Act**), the CDO, and data analytics bodies, are required to report annually, to the Information Commissioner, on the projects conducted under the VDS Act that relate to personal information. The CDO and data analytics bodies are also required to give notice of any breaches of the *Privacy and Data Protection Act 2014* (Vic).
- To prepare and publish guidelines relating to the protection of personal information and other privacy matters, and to promote the adoption of such guidelines.
- To promote the adoption of, and monitor compliance with, information protection principles.
- To make public statements about any matter relating to the privacy of individuals generally.
- To initiate and recommend the making of privacy codes of practice.
- To provide assistance to agencies in adopting and complying with information principles and privacy codes of practice.
- To conduct education programs and disseminate information for the purpose of promoting the protection of the privacy of individuals.
- To have a leadership role on privacy related issues, which would include having responsibility to prepare and publish reports and recommendations about any matter that concerns the need for, or the desirability of, legislative, administrative or other action that would improve the administration of privacy legislation and enhance the privacy of individuals.
- To report serious and/or repeated interferences with privacy to a Minister responsible for an agency involved in such serious and/or repeated interferences who would then, in turn, be required to present the Commissioner's report to the Parliament or, alternatively, the Privacy Commissioner would provide that report directly to the Parliament.
- To conduct research, and collect and collate information, about any matter relating to the protection of personal information and the privacy of individuals.

- To refer a privacy complaint to another entity that may be able to more appropriately deal with that complaint (such as where it is assessed as not being a valid privacy complaint by the Privacy Commissioner).

In a submission in response to the NSW discussion paper referred to under Question 1 of these submissions, the NSW Privacy Commissioner submitted that the Privacy Commissioner should be given the following additional powers:

- The power to investigate agency systems, policies and practices and conduct audits. See for example, Division 3 of Part 3 of the *Government Information (Information Commissioner) Act 2009* (NSW) (**GIIC Act**).

- The power to accept enforceable undertakings, like the Australian Information Commissioner (**AIC**), which are enforceable in the Federal Court and Federal Circuit Court. The undertakings may be published on the OAIC website and require an entity to refrain from undertaking a specified action, comply with the Privacy Act 1988 and not to interfere with the privacy of an individual.

- The power to share information with other key regulators, such as Cyber Security NSW, State and federal law enforcement and the AIC. See for example Division 5 of Part 3 of the GIIC Act.

- The power to make recommendations to agencies. See for example section 95 of the *Government Information (Public Access) Act 2009* (NSW).

Determinative powers

Under the *Freedom of Information Act 1992* (WA) (**FOI Act**), in addition to conciliating complaints, the Western Australian Information Commissioner has power to determine complaints. A right of appeal lies to the Supreme Court on any question of law arising from certain decisions of the Information Commissioner.

Except for the Commonwealth, privacy regulators in other jurisdictions do not make determinations in relation to complaints. However, the Victorian Information Commissioner expressed the view in his letter dated 18 September 2019[67] that a Privacy Commissioner have power to make decisions in respect of privacy complaints. That letter sets out the advantages to the Privacy Commissioner having determinative functions.

Privacy oversight could sit with the Office of the Information Commissioner (OIC)

Commonwealth privacy legislation governs the handling of personal information by the Australian public service and by much of the private sector. All states and territories, other than Western Australia and South Australia, have privacy legislation governing the handling of personal information at state/territory and local government level. In most other state jurisdictions, oversight of privacy laws sits with the jurisdictional counterpart of the OIC.

[67] See OVIC's letter dated 18 September 2019 at Appendix B.

Although Western Australia has not had a legislative privacy regime, the OIC through its responsibilities under the FOI Act has considerable experience with the protection of personal information since the establishment of the OIC in 1993. This is because the WA FOI Act provides some privacy protections in the form of the exemption in clause 3 of Schedule 1 (which protects personal information from disclosure subject to exceptions) and the right to apply to amend personal information held in government records. Such provisions are an essential part of FOI laws in Western Australia in the absence of standalone privacy protection.

The OIC is therefore well placed to deal with privacy protection. Successive Information Commissioners' have consistently, in the absence of specific WA privacy legislation, stated in published decisions that the purpose of the exemption in clause 3 is to protect personal privacy.

Part 3 of the FOI Act also deals with applications for amendment of personal information. These provisions provide a means of ensuring that personal information held by State and local government is accurate, complete, up to date and not misleading. As observed in the Second Reading Speech of the *Freedom of Information Bill 1992* (**FOI Bill**) (see Hansard, Legislative Assembly, 1 September 1992, 4156), the provisions in Part 3 were originally intended for inclusion in privacy legislation proposed at the time but were included in the FOI Bill when privacy laws were not enacted. Similar provisions are found in most privacy legislation in other states/territories and the Commonwealth.

However, the FOI Act does not provide for privacy regulation or create rights or remedies when privacy is breached.

As the OIC administers the FOI Act, and the Information Commissioner makes binding determinations about whether personal information is exempt from disclosure and in relation to an agency's decision not to amend personal information, the OIC's view is often sought by agencies and members of the public in privacy related matters, despite it not having a specific privacy remit.

The OIC currently receives communications and jurisdictional updates from Privacy Authorities Australia, which is a group of Australian privacy authorities that meet regularly to promote best practice and consistency of privacy policies and laws.

The OIC promotes a model of resolving complaints under the FOI Act by conciliation. Officers of the OIC have the necessary skills and experience to resolve matters by conciliation. The Annual Report of the OIC 2018/2019 shows that 82% of complaints were resolved by conciliation in that reporting period.

The OIC sought a response from privacy regulators in other jurisdictions about whether the privacy oversight should sit with the OIC.

Mr Sven Bluemmel was appointed as the Victorian Information Commissioner in 2017. He was the Western Australian Information Commissioner from 2009 to 2017. In his letter to the OIC dated 18 September 2019,[68] Mr Bluemmel states as follows:

[68] See Appendix B to this submission

In my view, oversight of privacy law is well placed within an Information Commissioner's office, combining information privacy and FOI functions.

The establishment of OVIC in 2017 saw the privacy regulator functions merge with those of the former FOI Commissioner, bringing the two areas under the remit of a single Information Commissioner. This approach had already been adopted in other Australian states before Victoria followed suit, leveraging off the success of this approach in other jurisdictions, particularly New South Wales and Queensland. The experiences of the New South Wales Information and Privacy Commission, Office of the Information Commissioner Queensland and OVIC have demonstrated that combined oversight of FOI and privacy has the potential to provide a coherent, consistent regulatory approach to governance and enforcement of information rights.

Despite the seeming tension between the notions of public access to government information and information privacy, in practice, it is rare for privacy law and FOI law to conflict. Where there is potential for inconsistencies between the two laws, it is my view that having a sole regulator for both areas is likely to result in a better outcome when seeking to resolve tensions, in contrast to two regulators who approach their respective jurisdictions from a single perspective.

As a former WA Information Commissioner, and having continued to work with [OIC WA] *in my role as Victorian Information Commissioner, I am of the view that the Office of the Information Commissioner for WA* ***(OIC)*** *would be well placed to take on the role of privacy regulator. As an office that already receives and responds to complaints and reviews relating to information rights, the receipt of privacy complaints would be a natural extension for the OIC. Given the existing structures and processes in place at the OIC, an expansion into oversight of privacy law would offer an effective and efficient model for implementing the regulation of privacy rights in WA. I offer this view on the assumption that the OIC would receive appropriate funding and resourcing for the expansion of its remit to oversight of information privacy.*

On 25 September 2019, in correspondence to the OIC, the Queensland A/Privacy Commissioner, Ms Susan Shanley, observed as follows:

While privacy oversight models vary across jurisdictions, it is OIC's view that privacy oversight should sit with the Office of the Information Commissioner. Having privacy and right to information functions in the one entity provides a number of advantages. For example, there is synergy between all functions of the OIC, as the activities of one function support and complement the work of another. For example, OIC's monitoring and assistance functions improve the quality of agency practice in the collection and handling of personal information which minimises demand for our external review and privacy complaints services. This combination works well and is a proven model in jurisdictions nationally and internationally. Notably Canada, British Colombia, the UK, New Zealand (for personal Information) Australia's OAIC, NSW IPC, NT and more recently Victoria.

The close relationship between the regulation of privacy and the regulation of access to information has a historical legacy. This is illustrated by the following quote from the former

New Zealand Privacy Commissioner who in 2005, in relation to the interface between privacy and access to information at that time in that jurisdiction, noted as follows:[69]

> *The NZ experience of the Privacy Act/FOI interface is that they have two Acts,* [the Official Information Act 1981(**OIA**)] *and the Privacy Act; two independent review bodies, a Privacy Commissioner for the Privacy Act and the Ombudsmen for the OIA. Requests made by individuals for information about themselves must be dealt with under the Privacy Act (even though it is also, technically, official information). All other official information (that is, government-held information that is not personal information about the requester), must be considered under the OIA. This includes personal information about identifiable individuals other than the requester, or which otherwise affects the privacy of individuals. Privacy gets considered - but it gets considered under the privacy withholding grounds of the OIA. Reviews of decisions to withhold on the grounds of protecting privacy operate through a consultative process between the Privacy Commissioner and the Ombudsman. If it's unclear whether a matter falls within the Privacy Act or the OIA, then we discuss it. If necessary, we'll transfer complaints from one office to the other, to assist the requester. Ultimately, the decision on release or otherwise lies with the Ombudsman. But my view as Privacy Commissioner is of considerable assistance to the Ombudsman in making that decision. Where there are common but contentious issues, such as naming fines defaulters, it is helpful if the Ombudsman and the Privacy Commissioner can present a considered opinion. If this is a joint opinion, all well and good. If it isn't, then this too is useful.*

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

Relevant legislation in other jurisdictions provides guidance on how breaches of privacy should be managed.

Overview of privacy enforcement in Queensland, New South Wales, Victoria, and Commonwealth

Queensland

- Privacy complaints are made to agencies in the first instance; if not satisfied with the response, the complainant can lodge a privacy complaint with the Queensland Office of the Information Commissioner (**OIC**).
- The OIC encourages agencies to notify the OIC of a privacy breach, although there is no mandatory requirement to do so under the *Information Privacy Act 2009* (**IP Act**).
- The Queensland Information Commissioner has privacy functions under the IP Act.
- However the IP Act also establishes the additional office of the Privacy Commissioner whose role is that of the deputy to the Information Commissioner with particular responsibilities for matters relating to the Information Commissioner's privacy functions under the Act.

[69] Former NZ Privacy Commissioner, Marie Shnaff's presentation at the FOI Live 2005 Conference 16 June 2005, London entitled 'The Official Information Act and Privacy: New Zealand's Story': http://www.privacy.org.nz/assets/Files/67725421.

- The Information Commissioner has a mediation role and does not have power to make a determination, order or recommendation concerning a privacy complaint. If the complaint is not resolved, the complainant can ask the OIC to refer the complaint to the Queensland Civil and Administrative Tribunal (**QCAT**).

- QCAT has power to hear and determine the privacy complaint. QCAT can make orders such as restraining an agency from repeating any act or practice or ordering the agency to carry out certain acts, award compensation to the complainant not exceeding $100,000 and/or make further orders against the agency.

- The Information Commissioner does not have a right to appear and be heard in privacy matters before QCAT. However a 2017 submission by the OIC[70] recommended that the IP Act be amended to give the Information Commissioner and Privacy Commissioner a right to assist the court in a role such as an amicus curiae, where the OIC considers it appropriate, and with the leave of the court. This would be in line with the function of the Privacy Commissioner in other privacy jurisdictions including NSW and Victoria.

- The Information Commissioner has power to issue a compliance notice (e.g. to take a stated action within a set period) where there has been a serious or a flagrant breach of the obligation to comply with the privacy principles, or a breach which has occurred five times in the preceding two years. An agency must comply with a compliance notice, but can appeal against the decision to issue the compliance notice to the QCAT.

- The Information Commissioner also assesses Bills for their potential to impact on privacy rights and makes submissions to Parliamentary Committees on these issues if appropriate.

- The Information Commissioner has the power to waive or modify the privacy principles. An agency can apply to the Commissioner for approval to not comply with the privacy principles or to comply in a different way; approval is only granted where the Commissioner is satisfied that the waiver or modification is more strongly in the public interest than compliance with the principles.

  Note: no applications for waivers or modifications of the privacy principles were received by the Commissioner during 2017–18.[71]

New South Wales

- Broadly speaking, the NSW Privacy Commissioner deals with privacy complaints, oversees privacy complaint handling by the NSW public sector, assists the NSW Civil and Administrative Tribunal (**NCAT**) in their judicial review of public sector privacy complaints, and reports on the investigation of privacy complaints and broad systemic privacy issues.

- The Privacy Commissioner has an oversight role in how agencies handle privacy complaints. A complainant is initially required to ask the agency to conduct an internal review of their complaint. Agencies must keep the Privacy Commissioner informed about

[70] see: https://www.oic.qld.gov.au/__data/assets/pdf_file/0008/34199/submission-2016-consultation-on-review-of-the-rti-and-ip-acts.pdf

[71] see page 27 of annual report 2017-18: https://www.oic.qld.gov.au/__data/assets/pdf_file/0006/37581/oic-annual-report-2017-18_web.pdf

the internal review application and its progress until finalised - including informing the Privacy Commissioner of the findings of the review and any action proposed to be taken.

- If the review is not completed within 60 days, or a person is not satisfied with the action taken in relation to internal review, the complainant can apply to NCAT for external review of the conduct concerned.

- The Privacy Commissioner does not represent the parties at NCAT but has the right to attend and be heard at a hearing, to assist in the legal interpretation of NSW privacy legislation in the role of amicus curiae.

- NCAT can make orders including awarding compensation (damages) of up to $40,000 for any financial loss, or psychological or physical harm, because of conduct of the agency or body; or requiring the agency or body to make an apology, change their practices or stop any conduct or action which contravenes an Information Privacy Principle or Health Privacy Principle. Orders made by NCAT must be followed by an agency and are enforceable.

- There is a voluntary scheme for reporting data breaches to the Information and Privacy Commission (which the Privacy Commissioner is part of) - while not required by law, the Privacy Commissioner encourages agencies to voluntarily notify the Commissioner of data breaches - the NSW government is looking at whether more robust reporting scheme is needed in NSW.[72]

- The Privacy Commissioner's functions extend to dealing with complaints concerning the private sector handling of health information in NSW.

- The Privacy Commissioner has the power to formally investigate certain privacy complaints and to investigate and report on general issues concerning rights to privacy.

  Note: complaints involving private sector use of personal health information comprise a large proportion of matters dealt with by the Privacy Commissioner.[73]

- Public sector agencies are required to prepare and implement a privacy management plan and provide a copy to the Privacy Commissioner.[74]

Victoria

- Privacy complaints should be made to the agency directly in the first instance. If not satisfied, the complainant can lodge a complaint with the Victorian Office of the Information Commissioner (**OVIC**).

- The OVIC is headed by the Information Commissioner (now Sven Bluemmel, former WA Information Commissioner) who is supported in his privacy related functions by the Privacy and Data Protection Deputy Commissioner.

---

[72] see pages 9 and 10 of 2017/2018 annual report: https://www.ipc.nsw.gov.au/sites/default/files/file_manager/IPC_2018_Annual_Report__WEB.pdf

[73] https://www.ipc.nsw.gov.au/privacy/privacy-resources-public-sector-agencies/privacy-reports-and-investigations/privacy-investigations

[74] see page 36 of 2017/2018 annual report: https://www.ipc.nsw.gov.au/sites/default/files/file_manager/IPC_2018_Annual_Report__WEB.pdf

- Although there is no obligation under the *Privacy and Data Protection Act 2014* (**PDP Act**) for public sector organisations to notify OVIC or affected individuals of data breaches, OVIC encourages voluntary reporting of data breaches to OVIC, including those reported to the OAIC under the Notifiable Data Breaches scheme (given that an eligible data breach involving a VPS organisation would also likely involve a breach of the PDP Act).[75]

- OVIC has power to conciliate complaints however if conciliation is unsuccessful a matter may be referred to Victorian Civil and administrative Tribunal (**VCAT**) for hearing and determination.

- Among other things, VCAT can order the respondent to stop the acts complained of or take action to redress any loss or damage suffered by the complainant and order the respondent to pay a complainant compensation of up to $100,000 for loss or damage suffered by the complainant.[76]

- The Information Commissioner, although not a party to the VCAT proceedings, may join privacy proceedings before VCAT with leave from VCAT. Even in the exceptional circumstances where the Commissioner is a party to proceedings, he will act as an independent and expert participant, making submissions on questions of law, policy and the public interest as they relate to privacy and the PDP Act.

  Note: the number of breach notifications to OVIC increased from 13 to 65 annually over the last four years, which OVIC considers is attributable to a broadening appreciation among regulated organisations of the importance of actively managing privacy incidents and the value in proactively engaging with their office.[77]

- OVIC conducts privacy impact assessments upon request by organisations.

- OVIC reviews draft legislation that has an impact on privacy when requested.

- OVIC is consulted by organisations about initiatives that have an impact on privacy.

- OVIC has an oversight role under the *Data Sharing Act 2017*.

Commonwealth

- *The Privacy Act* 1988 (Cth) (**Privacy Act**) confers a range of regulatory powers on the Australian Information Commissioner, including investigation and enforcement powers, which are based on an escalation model.

- Enforcement and regulatory powers[78] include powers to:

  - direct an agency to give the Commissioner a privacy impact assessment;

---

[75] https://ovic.vic.gov.au/wp-content/uploads/2018/07/OVIC-NDB-scheme-guidance.pdf
[76] https://ovic.vic.gov.au/resource/guide-to-the-handling-of-complaints-under-the-privacy-and-data-protection-act-2014-by-the-victorian-civil-and-administrative-tribunal/
[77] see page 22 of 2017/2018 annual report: https://ovic.vic.gov.au/wp-content/uploads/2018/09/OVIC-2017-18-Annual-Report.pdf
[78] See: https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/privacy-regulatory-action-policy.pdf

- monitor, or conduct an assessment of, whether personal information is being maintained and handled by an entity as required by law;
- conciliate a complaint;
- investigate a matter (either in response to a complaint or on the Commissioner's own initiative), and various related powers including to decline to investigate a complaint, to refer the matter and discontinue an investigation where certain offences may have been committed, and to refer a complaint to a specified alternative complaint body;
- report to the Minister in certain circumstances following an investigation, monitoring activity or assessment;
- accept an enforceable undertaking and, if necessary, bring court proceedings to enforce an enforceable undertaking.

  Note: an enforceable undertaking is a written agreement between an entity or person and the Commissioner, which is provided under either the Privacy Act or the My Health Records Act and is enforceable against the respondent in the courts. An enforceable undertaking is an important enforcement tool for use in situations where there has been or appears to have been an interference with the privacy of an individual and the OAIC considers an agreed change to future behaviour offers the most appropriate regulatory outcome in the particular circumstances.[79]
- make a determination and, if necessary, bring court proceedings to enforce a determination.
- seek an injunction.
- apply to the Federal Court or Federal Circuit Court for a civil penalty order if an entity is alleged to have breached a civil penalty provision in the Privacy Act, including for serious or repeated interferences with privacy.

  Note: the penalty is paid by the entity to the Commonwealth, but there is provision for an individual to recover compensation or other remedies where a civil penalty order is made against an entity for a contravention of a civil penalty provision contained in Part IIIA (Credit reporting) of the Privacy Act. Penalties are expressed in 'penalty units'.
- direct an entity to make a notification under the Notifiable Data Breaches scheme, or declare the notification is not required or can be delayed.

- A party may apply to Administrative Appeals Tribunal (**AAT**) to have a decision or determination by the Commissioner reviewed by the AAT (merits review) and/or apply to the Federal Circuit Court or the Federal Court of Australia for judicial review of a determination.

[79] see 3.1 and 3.12: https://www.oaic.gov.au/resources/about-us/our-regulatory-approach/guide-to-oaic-s-privacy-regulatory-action/oaic-regulatory-action-guide.pdf

Notifiable Data Breaches scheme (NDB scheme)

- The *Privacy Amendment (Notifiable Data Breaches) Act 2017* inserted Part IIIC into the *Commonwealth Privacy Act 1988* to establish the Notifiable Data Breaches scheme (**NDB scheme**).

- The NDB scheme came into force on 22 February 2018 and requires entities captured by the scheme to notify the OAIC and affected individuals of any eligible data breaches.

- The NDB scheme applies to entities that have obligations to protect the personal information they hold under the Privacy Act 1988. This includes Australian Privacy Principle (APP) entities, credit reporting bodies, credit providers and tax file number (TFN) recipients.

- State public sector agencies who receive or collect TFNs are subject to the scheme – both Victoria and NSW have produced publications to assist their respective states on this subject.[80]

Note about New Zealand

- A new privacy bill was introduced in March 2018. The Bill enhances the role of the Privacy Commissioner and requires agencies to report data breaches/notify the people affected and the Commissioner. The Commissioner will be able to issue compliance notices to require an agency to do something, or stop doing something. The Bill creates new criminal offences, including misleading an agency in a way that affects someone else's information or to destroy documents containing personal information if a request has been made for it. The proposed penalty is a fine up to $10,000. An agency is to comply with investigations and the penalty for non-compliance is increased from $2,000 to $10,000.[81]

Q 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?

Broadly speaking, the OIC considers that the role of the Chief Data Officer should be to provide guidance, advice, advocacy and regulation of public sector data sharing, similar to the role proposed for the National Data Commissioner. [82] In particular, the Chief Data Officer will need to play a key advocacy role in promoting cultural change across the WA public sector and in building trust with the community about the use and sharing of public sector data.

As noted earlier in this submission in relation to Question 1, the Commonwealth Data Sharing and Release Legislative Reforms' Discussion Paper noted that the National Data Commissioner (**NDC**) should have a dual role: championing greater data sharing while promoting safe data sharing practices. It was also noted in that discussion paper that the

[80] https://ovic.vic.gov.au/blog/notifiable-data-breaches-scheme-obligations-for-victorian-public-sector-organisations/; and https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-notifiable-data-breaches

[81] https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/; and https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-law-reform/

[82] See page 39 of Commonwealth Data Sharing and Release Legislative Reforms' Discussion Paper available at https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf

NDC should be empowered to apply strong penalties to intentional or negligent misuse of data and should cooperate with other regulators, including the Australian Information and Privacy Commissioner. The OIC submits that the WA Government should consider these powers and the other points outlined in Chapter 6 of the Commonwealth discussion paper regarding oversight of data sharing. The Government should also consider the functions and powers of the Victorian Chief Data Officer (**CDO**) set out in Part 2, s.7 of the *Victorian Data Sharing Act 2017* (**VDS Act**).

The OIC submits that oversight of data sharing should sit with the Privacy Commissioner, along similar lines to the Victorian data sharing regime.

As noted earlier in this submission in relation to Questions 1 and 3, the Office of the Victorian Information Commissioner (**OVIC**) plays an express oversight role over the Victorian Centre for Data Insights (**VCDI**), which is led by the Victorian CDO. This oversight role includes that the CDO must report annually to Victoria's privacy regulators - the OVIC and the Health Complaints Commissioner (**HCC**) - on matters including the steps taken to ensure compliance with privacy laws, the data projects that have been undertaken, details of data requests and refusals, and the issues and challenges that have arisen. The VDS Act also requires the CDO and departments (as data analytics bodies) to report any breach of privacy laws to the OVIC and the HCC and the original data provider. [83]

In his letter to the OIC dated 18 September 2019,[84] the Victorian Information Commissioner expressed the opinion that it would be appropriate for the oversight of data sharing in WA to sit with an Information Commissioner or Privacy Commissioner and said:

> [T]*his is the model that has been adopted in Victoria through the VDS Act, which provides an express requirement for the Chief Data Officer to report annually to the Information Commissioner on its projects involving personal information. As a business unit of the Victorian Department of Premier and Cabinet, the VCDI is subject to the PDP Act in the same way as any other Victorian public sector organisation and is therefore required to comply with the IPPs and respond to any privacy complaints made against it. Having had two years" experience with this model in Victoria, it is an approach that appears to be working well.*
>
> *My view is that the function of a Chief Data Officer (or equivalent) should not rest with the entity that administers privacy legislation; the two functions should be separated, and the WA equivalent of a Chief Data Officer should be subject to oversight from the Privacy Commissioner. For similar reasons as those noted* [in relation to the question of whether privacy and data sharing laws should be in separate pieces of legislation], *maintaining separation between Privacy Commissioner and Chief Data Officer would provide assurance to the public sector and community that those implementing government policy and regulating the handling of personal information are separate entities.*

---

[83] See '*Victorian Data Sharing Act 2017, Guidance for departments and agencies*' available at: https://www.vic.gov.au/system/user_files/Documents/vcdi/Victorian%20Data%20Sharing%20Act%202017%20Web%20Guidance%20UPDATE%20as%20at%2020%20Feb%202018.pdf

[84] See Appendix B to this submission

Q 10 What should the WA government be doing to support successful implementation of privacy and information sharing?

In addition to the matters already outlined in this submission, particularly regarding how privacy breaches should be managed and the role of the Privacy Commissioner, the OIC considers that the following options would support successful implementation of privacy and information sharing in Western Australia:

- Provide adequate resourcing for the establishment of the office of the Privacy Commissioner so that it can properly deliver on its primary function to provide protection for the privacy of personal information.
- Ensure that State privacy legislation covers both public sector agencies and also contracted service providers to government, particularly health service providers.[85]
- Provide clarity around whether state government trading enterprises are covered either by Commonwealth privacy principles or state privacy principles.[86]
- Include contemporary concepts such as biometric and genetic information in the definition of personal information[87] and acknowledge the issues around de-identified personal information.[88]
- Extend coverage of privacy laws to overseas recipients of information from WA public sector agencies so that remedies are available when those overseas recipients breach WA privacy principles. Alternatively make responsible the agency who provides information to the overseas recipient that breaches the privacy principles.[89]
- Acknowledge the need for technology specialists that will be required to assist the Privacy Commissioner and any other body that will be inquiring into interference with privacy so that expert evidence as to the circumstances in which a privacy breach may have occurred will be available.
- Identify where the onus and burden of proof lie in respect of the establishment of privacy complaints.
- Provide the Privacy Commissioner with adequate powers and resources to monitor the performance and support the functions of agencies who have privacy responsibilities (including education, training, providing advice and issuing guidelines for agencies).
- Provide the Privacy Commissioner with the role and adequate resources to inform and educate the public about their rights to privacy.
- Provide oversight of the operations of the Privacy Commissioner in the form of monitoring and review by a Parliamentary committee and requiring the Privacy Commissioner to report to Parliament annually.

---

[85] For example, see *Information* Privacy Act *2014* (ACT) s. 21.
[86] For example, see *Information Privacy Act 2014* (ACT) s. 23.
[87] For example, see *Information Privacy Act 2014* ACT s.14.
[88] For example, see *Information Privacy Act 2014* ACT s.18).
[89] For example, see *Information Privacy Act 2014* (ACT) s 22.

- Provide for sufficient investment in IT and other technology for the Privacy Commissioner and agencies so that privacy complaints can be adequately dealt with in a timely manner.

- In addition to a private person/persons who may make a privacy complaint, a privacy complaint may be commenced by referral from other complaint bodies such as the Ombudsman, the Director of the Health and Disability Complaints Office or any other entity having functions under either state or Commonwealth laws that correspond to the functions of the Privacy Commissioner or any other entity prescribed by regulations.

- Review the operation of both privacy and information sharing laws regularly (eg. every 3 - 5 years) so that the laws remain suitable and fit for purpose.[90]

- Provide the Privacy Commissioner with the ability to either provide remedies direct to the privacy complainant or allow the complainant to apply to a court or the State Administrative Tribunal (**SAT**) for orders that would then provide relief to the complainant.

- Any consequential involvement of a court or SAT to provide remedies in respect of privacy interferences should involve adequate resourcing of that body to deal with the new work relating to this additional jurisdiction.

- Provide for added protection and flexibility of protection by allowing for Codes of Practice which could apply additional requirements to certain public sector agencies. Such Codes would, at a minimum, deal with how agencies would internally handle privacy complaints and provide for reporting about privacy complaints to the Privacy Commissioner. Such draft Codes may need to be advertised and invite public comment, and also be reviewed by the Privacy Commissioner, before being adopted.[91]

- Require the Privacy Commissioner's annual report to Parliament to include information about the number of privacy complaints across government (both made and dealt with), the number privacy complaints (for review of agency decision) to the Privacy Commissioner and the number of privacy matters referred to any court or SAT for follow-up enforcement of remedies. In order to report on the number of privacy complaints across government the legislation should oblige agencies to compile and provide statistical information to the Privacy Commissioner regarding privacy interference complaints. Such statistical information would also assist the Privacy Commissioner to identify systemic privacy issues in agencies.

- The legislation should state what the relationship is with other laws that either permit information sharing of certain information (for example, health records under the *Health Services Act 2016* (WA) Part 17) or prohibit information sharing, particularly those laws that create offences (for example, section 81 of the Criminal Code and the offence provisions in the *Public Sector Management Act 1994* (WA)).

- If the Government decides that the role of Privacy Commissioner should be undertaken by the Information Commissioner then both roles should have concurrent terms and

---

[90] For example, see *Information Privacy Act 2009* (Qld) s. 192.
[91] For example, see *Information Privacy Act 2014* (ACT) ss. 49 - 51, 55.

conditions, or alternatively, both roles could be merged into one role with a new title such as the Information and Privacy Commissioner. The Government should then also consider creating the role of a Deputy Information and Privacy Commissioner who would have either vested authority or delegated authority from the Information and Privacy Commissioner with respect to the privacy functions of the Information and Privacy Commissioner.

- Delay the start of operation of new privacy and data sharing laws for at least 12 months so that the office of the Privacy Commissioner can undertake extensive education and awareness training for agencies expected to comply with the new privacy regime and also build awareness of the public as to their rights under the new privacy regime.

Office of the
Information Commissioner

Freedom of information for Western Australia

Privacy and data sharing law reform in Western Australia

Issues Paper

Office of the Information Commissioner
18 February 2019

Purpose of this Paper

The purpose of this paper is to highlight some key issues for the Western Australian Government (**the Government**) to consider in the area of privacy and data sharing law reform.

Summary of key points

The key points arising from this paper are as follows:

- While matters of policy are entirely a matter for Government and Parliament, the OIC considers that the Government should enact privacy legislation as separate stand-alone legislation to data sharing legislation.
- It is generally accepted that the protection of privacy under the common law is inadequate and that privacy legislation in Western Australia is long overdue.
- Community trust is critical to the success of data sharing legislation.
- Privacy laws should be viewed as an enabler instead of a barrier to information sharing.
- Data sharing models in other Australian jurisdictions may provide useful insight when designing data sharing legislation.
- Issues raised by other Australian Information Commissioners in response to the proposed Commonwealth Data Sharing and Release Legislation should be closely examined.
- Oversight of privacy laws in the majority of models in Australia sits with the Office of the Information Commissioner.

The role of the Information Commissioner

The Western Australian Information Commissioner is appointed by the Governor under section 56 of the *Freedom of Information Act 1992* (**the FOI Act**) and reports directly to Parliament. The Commissioner's main function is to deal with complaints made under the FOI Act about decisions made by agencies in respect of FOI applications and applications for amendment of personal information. The Commissioner's functions also include ensuring that agencies are aware of their obligations under the FOI Act and ensuring that members of the public are aware of their rights under the Act.

The FOI Act does not expressly confer on the Information Commissioner any policy functions, nor is the Commissioner's office resourced or staffed to discharge such functions. Information Commissioners in some other Australian jurisdictions have a broader policy function, as well as privacy oversight. This has allowed Commissioners in those jurisdictions to be more proactive about identifying and responding to the issues mentioned in this paper. For these reasons, the Information Commissioner does not consider it appropriate to take a lead role in resolving the issues identified in the paper. Instead, the Commissioner has brought these issues to the attention of the Attorney General and the Department of the Premier and Cabinet for further action.

It is also important to note that this paper reflects the views of OIC as an independent accountability agency. It does not necessarily reflect the views of the Western Australian Government.

Current status of privacy legislation in WA

Western Australia does not currently have privacy legislation. The Office of the Information Commissioner (**OIC**) understands that the Government is currently developing data sharing legislation.

Privacy legislation in this State has been the subject of discussion and consideration for a number of years. An outline of developments in respect of privacy laws in Western Australia is provided in this issues paper.

A Government media statement issued in October 2017[1], following the public release of the Data Linkage Expert Advisory Group report[2] stated that the 'report's recommendations will feed into a number of the Government's current reform initiatives, including a commitment to State privacy legislation'.

In a speech given by the Attorney General at the Law Society's Law Week Breakfast on 14 May 2018, it was noted that, as WA does not have an overarching legislative privacy regime, consideration was being given to the need for, and form and content of, privacy legislation to govern the collection, storage, release and use of personal information in WA.[3]

Privacy Bill 2007 and subsequent developments

Background

All Australian states and territories, other than Western Australia and South Australia, have privacy legislation governing the handling of personal information at state/territory and local government level.

In 1995, the Western Australian Commission on Government, Report No 1,[4] recommended that privacy legislation be enacted to address specific privacy issues surrounding the storage, use and retrieval of personal data and data matching between government agencies. [5]

In 2003, the then Attorney General, Jim McGinty MLA, released for public comment a policy research paper 'Privacy legislation for Western Australia.'[6]

---

[1] See https://www.mediastatements.wa.gov.au/Pages/McGowan/2017/10/Data-linkage-review-report-released.aspx
[2] https://www.jtsi.wa.gov.au/docs/default-source/default-document-library/a-review-of-western-australia's-data-linkage-capabilities---developing-a-whole-of-government-model---december-2016.pdf?sfvrsn=f6c26d1c_0
[3] See the article adapted from the speech on page 16, *Brief,* Volume 45 No 5 June 2018
[4] See https://www.slp.wa.gov.au/publications/publications.nsf/DocByAgency/5F56D2C4E29C477B48256983000CA043/$file/report1.pdf
[5] Ibid, page 62.
[6] See https://web.archive.org/web/20030624014700/http://www.ministers.wa.gov.au/Feature_stories/McGinty_privacy_research.pdf

The Attorney General said in the Foreword of the paper:

> *The Government of Western Australia believes that privacy is a fundamental right and that a person's entitlement to privacy must be protected.*
>
> *People are concerned that personal information about themselves held by government agencies and other bodies may be misused or inappropriately disclosed. These concerns have intensified with the rapid and increasing use of electronic technologies.*
>
> *There is no general common law right of privacy. The Freedom of Information Act 1992 (WA) provides a right of access to and correction of information. However, Western Australian laws do not comprehensively or adequately deal with privacy issues associated with the collection, storage, release and use of personal information.*
>
> *For these reasons it is important that we establish a proper legislative framework within which a person's right to the privacy of their personal information may be protected.*
>
> *Such privacy protection cannot be absolute. It must be balanced against other interests. For example, privacy protection should not be used as a shield to hamper investigations into criminal or other improper activities, or impede the free flow of information between government agencies when this is in the public interest.*

In proposing the introduction of privacy laws for Western Australia, the paper noted that privacy is a 'very important social issue for Australians' and that the Western Australian Commission on Government '*similarly reported a strongly held public view that existing arrangements for the protection of individual privacy are inadequate, in particular, in respect of the storage, use and retrieval of personal data by* [sic] *and data matching between government agencies*'.[7]

The 2003 policy paper also made observations about the importance of the privacy of health information and concerns about the lack of specific State privacy laws in relation to health information. [8]

Information Privacy Bill 2007

In March 2007 the then Labor State Government introduced the *Information Privacy Bill 2007* (**2007 IP Bill**) into Parliament. The Bill passed through the Legislative Assembly in November 2007 and was introduced into the Legislative Council in December 2007. The Bill lapsed when a general election was called in 2008.

Key features of the 2007 IP Bill included:

- Most public organisations to comply with a set of information privacy principles (**IPPs**).

[7] See [1] of the Executive Summary
[8] See page xxv

- Most public organisations, private sector health service providers, and persons or bodies in the private sector who hold health information about individuals to comply with a set of health privacy principles (**HPPs**).

- Creation of a right to access, or apply to amend, health records held by a private organisation – if unhappy with access or amendment decision, make complaint to State Administrative Tribunal (**the SAT**).

- Failure to comply with IPPs or HPPs would constitute an interference with privacy; an individual whose privacy has been interfered with could complain about that interference and ultimately commence proceedings in the SAT seeking redress for that interference with privacy.

- Establishment of the office of Privacy and Information Commissioner who would perform functions under the Information Privacy Act including functions relating to compliance with the Act. The Commissioner would also perform those functions presently performed by the Information Commissioner under the FOI Act. The IP Bill permitted the office of the Ombudsman and of the Commissioner to be concurrently held.

Recent developments and involvement of the OIC in privacy issues

The FOI Act provides some privacy protection, particularly the exemption in clause 3 of Schedule 1 to the Act which protects personal information from disclosure, subject to exceptions. Successive Information Commissioners have consistently, in the absence of specific State privacy legislation, said in published decisions that the purpose of the exemption in clause 3 is to protect privacy.

Part 3 of the FOI Act also deals with applications for amendment of personal information. These provisions provide a means of ensuring that personal information held by State and local government is accurate, complete, up to date and not misleading. As observed in the Second Reading Speech of the *Freedom of Information Bill 1992* (**FOI Bill**) (see Hansard, Legislative Assembly, 1 September 1992, 4156), the provisions in Part 3 were originally intended for inclusion in privacy legislation proposed at the time but were included in the FOI Bill when privacy laws were not enacted. Similar provisions are found in most privacy legislation in other states/territories and the Commonwealth.

However, the FOI Act does not provide privacy regulation or create rights or remedies when privacy is breached.

As the OIC administers the FOI Act, and the Information Commissioner makes binding determinations about whether personal information is exempt from disclosure and in relation to an agency's decision not to amend personal information, the OIC's view is often sought by agencies and members of the public in privacy related matters, despite it not having a specific privacy remit.

Privacy law reform in recent years has been led by the State Solicitor's Office, which has consulted with the OIC. The OIC has been closely involved in drafting and considering the provisions of previous iterations of privacy legislation. The OIC has expressed concerns about the importance of the introduction of privacy legislation, both in the lead up to and

following the Commonwealth's e-health database and personal health record system becoming operational in July 2012.

With its substantial knowledge and experience in privacy related issues, the OIC would welcome the opportunity to have significant input into draft privacy legislation including at the drafting stage and beyond.

The OIC has previously prepared estimates of resource requirements for the administration of privacy legislation as well as organisational charts for an expanded office to administer both FOI and privacy. The OIC remains willing to take on additional oversight for privacy laws and is well placed and experienced to oversee a new legislative framework. As noted below, in many jurisdictions the role of Information Commissioner includes responsibility and oversight for privacy laws. The OIC currently receives communications and jurisdictional updates from Privacy Authorities Australia, which is a group of Australian privacy authorities that meet regularly to promote best practice and consistency of privacy policies and laws.[9]

If the Government decides to proceed with privacy legislation and to use the provisions in the 2007 IP Bill as a starting point, the OIC recommends that it be consulted about any detailed proposals, but at a minimum the OIC recommends that:

- Jurisdiction in relation to alleged interferences with privacy be conferred on the Information Commissioner instead of the SAT.

- The name of the Commissioner should be the Information Commissioner (as opposed to the Privacy and Information Commissioner), in line with the practice adopted in other States.

- The provisions that would allow the positions of Information Commissioner and Ombudsman to be combined should not be retained.

- The Government consider the provisions in the Commonwealth Privacy Act and in privacy laws in other Australian States and territories.

Privacy oversight in other Australian jurisdictions

The majority of other States in Australia have found that the administrative functions and oversight of privacy legislation sit logically with the Office of the Information Commissioner. Similarly, in the federal jurisdiction the Freedom of Information Commissioner has undertaken the role of Privacy Commissioner since 2015. Examples of where this has worked successfully for some time include Queensland, with the introduction of the *Information Privacy Act 2009* and New South Wales, where the Information and Privacy Commission was established on 1 January 2011. [10] In September 2017 the Office of the Information Commissioner and Office of the Commissioner for Privacy and Data Protection were combined to create the Office of the Victorian Information Commissioner.

[9] See https://www.oaic.gov.au/engage-with-us/networks

[10] The NSW Information and Privacy Commission is overseen by the Information Commissioner, who is the CEO of the IPC

The decision to combine the two functions in one office suggests that it is both more efficient and effective to administer both privacy legislation and FOI legislation in a single, independent office.

While recognising that any new legislation and its oversight is of course a matter for government, the OIC has the necessary whole of government oversight experience and decision-making expertise to effectively manage and administer any new privacy legislation.

Australian data sharing laws

Three other Australian jurisdictions have enacted data sharing legislation – Victoria, New South Wales and South Australia[11] – and the Commonwealth Government is currently developing and designing a new Data Sharing and Release Bill.[12]

As observed by the Office of the Australian Information Commissioner (**OAIC**) - in its submission in response to an issues paper released for consultation on 4 July 2018 by the Department of the Prime Minister and Cabinet (**DPMC**) on the 'New Australian Government Data Sharing and Release Legislation'(**the Cth Data Sharing Issues Paper**) - other data sharing models may provide useful insight when designing data sharing legislation:[13]

> [T]*here are a number of other legislative data sharing models operating across other Australian (and international) jurisdictions, all in the early stages of implementation... The OAIC notes that these models are narrowly drafted, and generally restrict the purposes for which data may be shared to those which may inform government policy making, service planning and design....They also generally provide that, unless otherwise expressly provided for, the relevant legislation does not override other relevant obligations, and in particular privacy or data protection legislation....The OAIC would recommend that the Department consider the design of these schemes as part of its design and implementation of the DS&R Bill.* [footnotes omitted]

Data sharing legislation in Victoria and New South Wales operates in the context of existing privacy legislation, as is proposed at Commonwealth level.

Development of data sharing laws in WA

2016 - Data Linkage Expert Advisory Group

On 17 March 2016 the then Director General of the Department of the Premier and Cabinet (**DPC**) commissioned a review of Western Australia's data linkage capabilities, 'to maximise the State's competitive advantages in health data linkage and to develop a whole-of-Government model that builds on these strengths for the future'. The review was undertaken by the Data Linkage Expert Advisory Group (**the Data Linkage Advisory Group**). That group comprised Professor Peter Klinken (WA Chief Scientist), Chair; Professor Fiona

[11] See *Data Sharing Act 2017*(Vic), *Data Sharing (Government Sector) Act 2015* (NSW), and *Public Sector (Data Sharing) Act 2016* (SA)
[12] See https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation
[13] See page 4 of OAIC submission at https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20720.pdf

Stanley AC (Patron and Founding Director of the Telethon Kids Institute and Distinguished Research Professor of The University of Western Australia); and Mr Giles Nunis (the then Government Chief Information Officer).

Privacy issues identified in OIC submission to Data Linkage Advisory Group

In his submission to the Data Linkage Advisory Group in June 2016, [14]the former Western Australian Information Commissioner – now the Victorian Information Commissioner – made the following observations, in summary:

- Western Australia does not currently have privacy legislation. Commonwealth privacy legislation governs the handling of personal information by the Australian Public Service (**APS**) and by much of the private sector. All states and territories, other than Western Australia and South Australia, have privacy legislation governing the handling of personal information at state/territory and local government level.

- Privacy legislation has the potential to facilitate information sharing that respects the reasonable privacy expectations of individuals.

- The absence of privacy legislation could frustrate data linkage initiatives, as it potentially does now in respect of information sharing between WA public sector agencies.

- Data-driven innovation requires trust, even where the data being used is not personally identifiable.

- The *Australian Privacy Index 2016* (**Privacy Index**) published by Deloitte found that 94% of consumers believe that trust is more important than convenience. The Privacy Index also noted that the most common type of privacy complaint made against public and private sector organisations was about information being used inappropriately, followed by organisations failing to secure personal information.

- While data linkage will primarily use de-identified and aggregated data, the Australian Privacy Commissioner and others have recently warned that modern data analytics can allow data to be re-identified in more cases than was previously thought. This further highlights the importance of building trust in all information handling practices.

- The existing administrative arrangements applying to the Western Australian public sector are expressed very generally and are not supported by any comprehensive educative, oversight or complaints mechanism.

- The Australian Privacy Commissioner has consistently encouraged the concept of 'privacy by design'. Designing privacy compliance capability into information systems at the outset is likely to be more efficient than having to retrofit such capability at a later stage. Privacy legislation would provide a stable platform upon which such systems can be designed.

[14] Set out in full as Attachment 1 to this paper

- The introduction of privacy legislation is, of course, a matter for the elected government and its passage is a matter for Parliament. However, both major parties in Western Australia are on the record as being supportive. The previous Labor government introduced the *Information Privacy Bill 2007*, but that bill lapsed when Parliament was prorogued ahead of the 2008 election. During the 2008 election campaign, the Liberal Party committed to introducing privacy legislation should it win government.

- In addition to enjoying bipartisan support, the task of formulating and implementing State privacy legislation would be made easier by the extensive experience of other Australian jurisdictions. Much practical experience already exists and the consequences are known. Little, if anything, would have to be reinvented.

Data Linkage Expert Advisory Group Report

The Data Linkage Advisory Group report entitled 'Review of Western Australia's Data Linkage Capabilities' dated December 2016 (**the Data Linkage Report**)[15] was publicly released on 13 October 2017.[16] The Report recommended, among other things, that the State Government draft privacy legislation and consider the formulation of data sharing legislation (page 16). The Report also recommended that the OIC be a member of the Policy & Legislation Working Group to implement the recommendations relating to privacy and data sharing legislation.

The Data Linkage Report noted that privacy legislation is an instrument that most jurisdictions across Australia have developed to protect an individual's data and that there was a strong need for privacy legislation in this State.

In Chapter 4, Privacy, the report noted, in summary that:

- Robust privacy protection is critical to ensuring the success and survival of any data linkage function (page 55).

- Privacy legislation would create a high level framework enabling the legality for releasing data to be assessed, ensuring that standards applied for data release are consistent across Government. Further, if the legislation was to include penalties for breach of the provisions, as occurs with privacy legislation in other jurisdictions, it would provide a strong disincentive for the malicious access of private data. Currently, there are no general criminal penalties in WA for such breaches.

- WA's lack of privacy legislation appears to have caused reluctance by some jurisdictions to share data with WA, which in turn is hampering research initiatives in this State (page 56).

[15] https://www.jtsi.wa.gov.au/docs/default-source/default-document-library/a-review-of-western-australia's-data-linkage-capabilities---developing-a-whole-of-government-model---december-2016.pdf?sfvrsn=f6c26d1c_0
[16] https://www.jtsi.wa.gov.au/what-we-do/science-and-innovation/chief-scientist-of-western-australia/data-linkage-review

- Public trust is essential for maintaining a successful data linkage regime. Privacy legislation that: (i) increases the strength of the privacy regime around public data; and (ii) clearly articulates when it can and cannot be released, will reinforce public trust in the State's data sharing regime [OIC emphasis].

- *"While the lack of privacy legislation in WA is not a legal inhibitor to data sharing within WA and with other jurisdictions, there is a perception externally that the lack of privacy legislation in WA is a concern. There is an opportunity to strengthen the State's capacity for data linkage through privacy legislation"* (Finding 8, page 57).

2017 - Service Priority Review - Privacy and Information Sharing Background Paper

In May 2017, the Western Australian Government established the Service Priority Review (**SRP**) to 'examine the functions, operations and culture of the public sector, with the aim of driving lasting reform'. [17]

A series of background papers were prepared by the SRP secretariat to inform the work of the SRP Panel. This included a background paper on 'Privacy and Information Sharing' (**the Paper**).[18] The Paper examined approaches to privacy and data sharing in other Australian jurisdictions and identified issues particular to WA and suggested options for improvement.[19]

The Paper observed at page 1:

> *Western Australia is significantly out of step with other jurisdictions. A lack of comprehensive privacy or data sharing legislation and a patchwork of specific requirements within particular statutory schemes cause a reliance on the common law. The result is that legal rules for data use are the most restrictive in Australia and government agencies are in a difficult position when asked how they can lawfully and fairly share the information they hold. State Government stakeholders told the Panel that WA lags behind others in its use of data to inform policy development and outcomes measurement.*

The Paper noted[20] that the 2016 Data Linkage Report:

> [I]*dentified the concerns of other jurisdictions about sharing datasets with WA for data linkage purposes because of its lack of privacy legislation. Similar issues have been encountered by State Government agencies seeking to participate in inter-jurisdictional projects that require information sharing.*

[17] See Foreword, page 9, https://www.dpc.wa.gov.au/ProjectsandSpecialEvents/ServicePriorityReview/Documents/SPR_Report_FINAL-5-Dec.pdf

[18] https://www.dpc.wa.gov.au/ProjectsandSpecialEvents/ServicePriorityReview/Documents/BP_Privacy_and_Information_Sharing.pdf

[19] See page 1

[20] At page 2

The Paper also noted[21] that '*The absence of specific privacy legislation means State Government agencies operate within a patchwork of rules and sources of authority about what information can be shared publicly'.*

Recommendations

The Paper put forward four options for consideration by the Government, ranging from immediate term; medium term, most beneficial option; medium term; and medium term, less beneficial option, as follows: [22]

Immediate term

Consideration should be given to revising Public Sector Commissioner's Circular 2014-02 and underlying policy instruments to accurately reflect and sensibly mitigate the risks of sharing personal information between agencies.

In particular, a revised circular or policy might:

- *draw attention to the general prohibition on breaching confidentiality*
- *realistically assess the circumstances in which an action for breach of confidentiality may be made*
- *encourage action to be taken to minimise the possibility of data handling causing disadvantage that might support an individual taking legal action*
- *support pragmatic decision making where the public interest appears to outweigh the risk.*

In making this recommendation, it is acknowledged that any revision of the circular and policy instruments will not achieve a situation in which information can be readily shared between agencies. The legal framework will continue to apply irrespective of the content of a Public Sector Commissioner's circular.

Medium term, most beneficial option

Depending on the Panel's recommendation on establishing specific data analytics capability in WA, a corresponding recommendation on establishing data sharing legislation should also be considered. Data sharing legislation should, among other things:

- *appropriately protect privacy of personal information and commercially sensitive information*
- *support decisions to share sensitive personal information in human services delivery where circumstances warrant*
- *deal with inter-jurisdictional concerns about WA's privacy framework that may otherwise inhibit data linkage and other data sharing arrangements*
- *consider the model recommended by the Productivity Commission.*

Medium term

[21] At page 8
[22] See pages 11 and 12

Introduce comprehensive privacy legislation in WA alongside data sharing legislation to promote effective data sharing while protecting the privacy of individuals (for instance, the NSW data sharing model). Trust in the way that government collects, uses, discloses and handles personal information (i.e. effective privacy legislation) can be viewed as an enabler of data sharing initiatives. The more confident the public is in the protection of their personal information, the more willing they are to provide such information to government, and the more accurate and complete the data available to government [OIC emphasis].

Medium term, less beneficial option

Introduce privacy legislation in WA to partially overcome data sharing issues and ensure the confidence of other jurisdictions when sharing sensitive data with WA. Privacy legislation can (and generally does) promote at least some information sharing. Privacy legislation will also have the effect of conferring some rights on individuals in the event that their privacy is breached. This is in contrast to existing provisions which are not actionable by affected individuals [OIC emphasis].

The Final Report of the SRP published in October 2017[23] recommended that immediate steps be taken to develop legislation to facilitate information sharing while protecting sensitive personal and other information (recommendation 6.1).

2018 - Data Sharing Advisory group

In January 2018, DPC invited the OIC to join a small inter-agency Data Sharing Advisory Group, to review and comment on data sharing policy, drafting instructions and draft legislation, for consideration by Government in 2018.

At that early stage, it was not proposed to introduce separate stand-alone privacy legislation in addition to data sharing legislation.

After attending the first meeting of the Advisory Group in February 2018, the former Acting Information Commissioner decided that, as an independent statutory office, it was not appropriate to be involved in the development or endorsement of a particular government policy. As a result, the OIC did not attend further meetings of the Advisory Group. However, under a change of leadership the new Acting Information Commissioner has offered to re-join the advisory group although similar constraints to our involvement apply.[24]

WA Government response to the Cth Data Sharing Issues Paper

In its response, in July 2018, to the Cth Data Sharing Issues Paper,[25] the Western Australian Government stated:

---

[23] https://www.dpc.wa.gov.au/ProjectsandSpecialEvents/ServicePriorityReview/Documents/SPR_Report_FINAL-5-Dec.pdf

[24] See page 32 of OIC Annual report 2018 at https://www.oic.wa.gov.au/Materials/OIC_AR18.pdf#pagemode=bookmarks

[25] https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20696.pdf

> *Improved legislative arrangements to allow safe data sharing arrangements between State Government agencies and a limited number of authorised third parties are also a priority for the Western Australian Government.*
>
> *The Final Report of the 2017 Western Australian Service Priority Review highlighted the need for the State Government to develop legislation and processes to facilitate information sharing to build a public sector focussed on community needs and enable the public sector to do its job better.*
>
> *The Western Australia Government is actively working to improve public sector data sharing practices as part of a major public sector reform, as recommended in the Review's Final Report. A key component of this reform is the development of data sharing legislation that protects personal information and other sensitive information. The objective of this legislation will be to allow information to be safely shared across government, and authorised external entities, including other government jurisdictions.*
>
> *There are significant parallels between our current respective legislative approaches to data sharing.*
>
> *The Western Australian Government's proposed approach aligns with the 'five safes' framework proposed by the Commonwealth. To protect personal and other sensitive information, it also includes a Privacy Based Framework closely modelled on the key principles underpinning the Commonwealth's Privacy Act and privacy legislation in place in other State jurisdictions* [OIC emphasis].

In relation to the point emphasised above, the OIC is not aware whether the proposed Privacy Based Framework referred to includes separate stand-alone Western Australian privacy legislation, as is the case in the Commonwealth and most Australian states and territories.

Recent developments and building a social licence for greater data use and sharing

It is commonly observed that community trust is vital for the success of data sharing legislation.

In its submission, in response to the Cth Data Sharing Issues Paper, the Office of the Victorian Information Commissioner (**OVIC**) observed:[26]

> *Community trust is crucial for the success of* [data sharing legislation]. *To ensure community trust, the scheme should draw on principles developed in privacy law to balance the potentially competing interests of data subjects and data users.*

To this end, the OIC agrees with the following comments of the Victorian Information Commissioner:

---

[26] See https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20713.pdf, at page 1

> *OVIC acknowledges the need for a simple and effective mechanism for sharing government data and is supportive of using government data for evidence-based policy design.*
>
> *However, such a scheme must be established in a way that accords with community expectations. If a data sharing scheme does not align with the manner in which members of the public expect their personal information to be used, it will not be met with community acceptance. Without this, the existing social license that data users such as researchers and government rely on in carrying out their current activities will be compromised. The Productivity Commission correctly stated that building community trust is a critical part of enhancing data sharing and release* [Productivity Commission, Data Availability and Use: Productivity Commissioner Inquiry Report, Overview and Recommendations, No. 82, 31 March 2017, p. 2, available at: https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf]. *A data sharing and release scheme must be consistent with community expectations in order for it to be successful.*
>
> *Existing privacy law seeks to reconcile the interests of data subjects and data users. Privacy has developed mechanisms and principles to handle the tension between these potentially diverging interests. For example, the objects of the PDP Act* [under section 5(a); see also section 5(b)] *expressly acknowledge the need to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information. I suggest that the proposed scheme should consider and incorporate similar principles where appropriate, including notions of necessity, proportionality, and transparency.*

In its submission in response to the Cth Data Sharing Issues Paper, the OAIC noted[27] that the OAIC's Australian Community Attitudes to Privacy Survey 2017 'highlighted that some in the community may be uncomfortable with secondary uses of information, but that people are more likely to support data sharing for some purposes [more] than others'. It also observed that the figures it quoted 'suggest that there is still some work for the Australian Government to do to build an informed community confidence in government's planned secondary uses of personal information' and referred to the concerns expressed in recent community debate in relation to the secondary uses of data collected for the purposes of the My Health Record system.[28]

An article in the *Mandarin* on 1 August 2017 'Harmonising Australia's privacy regime'[29] said as follows:

> *Information has never been easier to share than today... And thanks to advances in areas like analytics and AI, it has never been more valuable, with commentators grandly proclaiming from time to time that data is 'the new oil' of the 21st century.*
>
> *Of course, the flipside of this 'new age of information' lies in maintaining privacy without creating unnecessary barriers. ....*

[27] See above, n 13, page 5
[28] Ibid, page 6
[29] https://www.themandarin.com.au/82064-harmonising-australias-privacy-regime/

Any public servant introducing new technologies in government must grapple with complexity or uncertainty surrounding privacy. This is driven by the extremely context-specific nature of applying privacy principles, and may be exacerbated by differing standards across jurisdictions, the proliferation of new technologies and international developments. However, these drivers may also assist in creating more universal privacy standards, which ensures privacy is embedded from the start of the process — rather than as an afterthought.

...

Our privacy regime is governed by a complicated lattice of privacy rules administered by various federal and state authorities....

...

While most states and territories have specific privacy bodies headed by Commissioners (or an Ombudsman in the case of Tasmania), Western Australia and South Australia subsume privacy back into other agencies. As a result, aspects of those states' privacy regimes are less rigorous than other jurisdictions.

...

A Privacy by Design approach helps ensure privacy protections

...

[A] *Privacy by Design approach ensures privacy is built into the process at the start, rather than being an afterthought.*

This matters more and more as government move to join-up information. For example... the Attorney-General's Department's Face Matching Service...is running into issues in securing agreement from some states to share their driver licence photos, as other jurisdictions may not have the same level of privacy protections [OIC emphasis].

...

Of South Australia and Western Australia, [the Queensland Privacy Commissioner] *thinks that while there are some protections for more extreme issues — for example SA has created a newer Act on surveillance — some in government view privacy as an afterthought or believes that there is enough existing statute without requiring specific privacy authorities. However, the Commissioner believes that these states need to be bound by the same standards and protections as the rest of the country, for example relating to criminal code protections or child exploitations.*

An article in the *Mandarin* on 23 January 2019 'If data is for good, then trust is king'[30] made the following observations:

Gaining and maintaining the trust of citizens and consumers over the use of their data will be critical to realising the social and economic value from data. Trust is a complex concept and it is often said that it takes years to build up trust and only seconds to destroy it...

In a 2018 global annual trust survey,[31] *... two-thirds of respondents cited protection of customer data and privacy as a key way for organisations to build trust. People need to be confident in how their data is collected, stored, shared, used or re-used. When*

[30] https://www.themandarin.com.au/103243-if-data-is-for-good-then-trust-is-king/?utm_campaign=TheJuice&utm_medium=email&utm_source=newsletter

[31] https://www.edelman.com/trust-barometer

people trust that their data will be used as agreed and accept value will be created, they are more likely to be comfortable with its use.

To gain greater licence, both private and public organisations need to be transparent in how they manage data and how effectively they communicate its value. Trust needs to be earned and maintained. How business and government deal with privacy, security and control by an individual over their data will be pivotal to building this trust and gaining social licence.

An article in the Mandarin on 11 February 2019 'How can the APS maintain trust at a time of significant disruption?'[32] noted:

As digital government begins to take shape, the public sector is entering a new era of citizen expectations. Emerging technologies offer opportunities for collaboration, information sharing and data analysis, all of which can support better policy and services.

But there are growing public concerns about privacy and security; questions about ownership and appropriate use of personal information. Is open government still relevant?

Governments worldwide are striving to maintain public trust at a time of significant disruption. Agencies are under pressure to be more transparent about their actions and decision-making processes.

Open government has never been more critical for meeting customer expectations, building confidence and delivering public value.

Citizens are demanding greater participation in policy development and service design, as well as ready access to information collected or created about them. A lack of social licence can impede public sector transformation.

...

Information governance by-design can play an important role in overcoming challenges and supporting reform, reducing the cost and complexity associated with both proactive and responsive information release.

Privacy Legislation as an Enabler – shifting the focus

The SRP's background paper on Privacy and Data Sharing, already referred to in this paper, referred to the 'restrictive nature' of privacy legislation. [33]

The paper also stated that 'the fundamental principle underlying privacy legislation is that government agencies are prohibited from using information for any purpose that is secondary to the purpose for which it was collected'.[34]

[32] https://www.themandarin.com.au/103784-open-government/
[33] See above, n 18, pages 2 and 5
[34] Ibid, page 3

However, as the former Commissioner noted in his submission to the Data Linkage Expert Advisory Group:[35]

> *It is sometimes assumed that privacy legislation is primarily concerned with preventing the collection and disclosure of information. However, modern Australian privacy legislation is designed to enable the trusted collection, use and disclosure of personal information in a way that is transparent and secure.*

The then Australian Information Commissioner and Australian Privacy Commissioner, Timothy Pilgrim said as follows, in a speech given in May 2016:[36]

> ***Simply put, a successful data-driven economy needs a strong foundation in privacy.***
>
> *Our experience and community research shows that by and large people do want their personal information to work for them, provided that they know it is working for them.*
>
> *When there is transparency in how personal information is used, it gives individuals, choice and confidence that their privacy rights are being respected.*
>
> ***Accordingly, good privacy management and great innovation go hand in hand.***
>
> *Because when people have confidence about how their information is managed, they are more likely to support the use of that information to provide better services.*
>
> *In fact, their expectations often become entirely supportive.*
>
> *Most people do expect organisations to use their information where it's necessary to provide them with the services they want or to improve on those services.*
>
> *They do expect law enforcement agencies to use information resources to stop crime and to keep people safe.*
>
> *However, people also want to know how their information is being used, who has access to it, and what that means for them in terms of their personal identity.*
>
> *Accordingly, privacy law - often misunderstood to be about secrecy, is really underpinned by transparency and accountability.*
>
> *And by ensuring organisations are transparent and responsible when handling personal information, privacy management strengthens customer trust.*
>
> *Building this trust is key to our big data challenges - whether sought in the form of customer confidence or political mandate.*

[35] See page 2 of Attachment 1 to this paper

[36] See https://www.oaic.gov.au/media-and-speeches/speeches/privacy-data-de-identification

Conditions Enabling Open Data and Promoting a Data Sharing Culture

The NSW Information Commissioner and NSW Open Data Advocate recently commissioned the University of New South Wales to undertake independent research to 'provide contemporary insights to support the promotion of Open Government and Open Data'. The research report, prepared by Dr Alana Maurushat, entitled 'Conditions Enabling Open Data and Promoting a Data Sharing Culture 2017'[37] noted, among other things, that:

- In leading jurisdictions privacy and data assurances are seen as enablers to open government as opposed to barriers. The legislative and regulatory environment recognises the requirement to balance the release of data together with privacy and to provide clarity to authorise release of data in certain circumstances [OIC emphasis]: page 6.

- In most countries, Open Data Policy is deeply entrenched in frameworks, directives, guidelines, charters and principles which are embedded in data governance frameworks. These frameworks draw upon a sound legislative basis to authorise Open Data. Leading jurisdictions have mature data governance frameworks that include clearly articulated roles and responsibilities, and provide detailed information and guidance around processes and tools: page 5.

- In most countries, the right to information regimes provide the initial and conceptual basis for Open Data. This right to information is set in a regulatory environment that guides agencies in meeting their obligations and expectations under legislation and policy, and monitors, supports and enforces policy and legislation. This has meant that in a country such as the UK the Information Commissioner's Office (ICO) enforces rights to data, is able to take complaints, approves publication schemes (schemes to identify open datasets and registries) of public authorities, assesses good practice, establishes consistent frameworks to facilitate the release of data and harmoniously balance privacy and other protections, imposes fines for non-compliance, recommends information including datasets to be opened, prosecutes those who commit criminal offences under the Freedom of Information Act, and hears appeals [OIC emphasis]: page 5.

New Australian Government Data Sharing and Release Draft Legislation

The submissions provided to DPMC[38] in response to the Cth Data Sharing Issues Paper include submissions from Information and Privacy Commissioners around Australia[39]. The OIC recommends that the Government considers the issues raised in those submissions, including the following, which are summarised.

Office of the Australian Information Commissioner

In its submissions the OAIC observes:

---

[37] Available at https://www.ipc.nsw.gov.au/sites/default/files/file_manager/Conditions_Enabling_Open_Data_Report.pdf; the OIC gave DPC a link to this research report in January 2019.

[38] Available at https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms/submissions

[39] This office did not make a submission.

> [T]he Australian Government also holds a vast wealth of data that is personal information about its citizens, which when linked together, can paint a rich and detailed picture of who we are as individuals....As such data is usually collected on a compulsory basis (as authorised or required by law), with individuals having little choice or control over whether to provide it, the Australian Government carries a unique responsibility when making decisions about how it should be used and disclosed.
>
> It is particularly important then, for any policy proposals which would use and disclose personal information for purposes beyond those originally intended at the time of collection, to have a strong public interest purpose and minimise any privacy impacts. Further, the social licence and level of community support for data sharing activities under a new scheme will need to be considered carefully throughout the design and implementation of the scheme. Ensuring that the privacy impacts of the scheme are minimised will help to build this social licence and trust [OIC emphasis].[40]

The OAIC's key recommendations, in summary, were:

1. Data sharing should occur on a de-identified basis wherever possible, to minimise the privacy impacts of the scheme for individuals.

2. The scope and purpose of data sharing legislation should be defined as clearly and narrowly as possible in order to minimise the impact on privacy.

3. The existing privacy protections for Commonwealth-held data should be maintained as far as possible, including the preservation of the OAIC's regulatory remit as the national, independent privacy regulator. This will help ensure accountability, and also avoid duplication, inconsistency and regulatory burden. The standards set out in the Commonwealth Privacy Act should remain the baseline, and any new arrangements under data sharing legislation should be developed in a way that ensures consistency with the existing regulatory requirements under the Privacy Act [OIC emphasis][41].

The OIAC also noted that '[t]here is significant complexity and risk involved with the publication of unit record level data derived from personal information'. [42] The OIAC expressed the view that 'open data environments are generally only appropriate for information that is either not derived from personal information, or information that has been through an extremely robust de-identification process...that ensures...that no individuals are reasonably identifiable'.[43]

Office of the Information Commissioner, Queensland

The Office of the Information Commissioner Queensland (**Qld OIC**) noted in its submission[44] that:

[40] See above, n 13, pages 1 and 2
[41] Ibid, pages 3 and 4
[42] Ibid, pages 6 and 7
[43] Ibid
[44] See https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20706.pdf at page 2

> *Striking the right balance between greater data availability and use and the protection of an individual's privacy and personal data is critical to realising the benefits of data, achieving greater openness and transparency and enhancing levels of trust in government.*

On the issue of de-identification, the QLD OIC noted that '[i]n October 2017, the UN Special Rapporteur on the Right to Privacy presented to the General Assembly the interim report of the work of the Taskforce on Big Data Open Data - the first of the thematic reports to be presented to the General Assembly'. The Qld OIC noted that the Special Rapporteur was considering a range of recommendations regarding publication of data about individuals; that 'the recommendations contained in the final report may have implications for the public release of de-identified data'; and that 'there is ongoing debate about the effectiveness of de-identification due to the increased risk of re-identification as more data becomes available'. [45]

Information and Privacy Commission New South Wales

In its submission[46], the Information and Privacy Commission New South Wales observed that:

> *From a privacy perspective, the community expectation is that any datasets that contain personal or health information will be handled in accordance with privacy legislation. Many citizens would have significant concerns should their personal and/or health data, often compulsorily collected by government in exchange for access to payments or services, were to be made available to other government agencies or private sector organisations for purposes separate to that for which it was collected, or to conduct research which may commercially benefit private entities, in circumstances where they have not consented to, or been notified of, that disclosure. More broadly, individuals may not support their data being used for secondary, unspecified purposes which they view as having no clear personal or public benefit.*
>
> *It is clear from recent media coverage of the commencement of the "opt-out" period for the My Health Record, and the strong concerns expressed about the use of, and access to, health information by other government agencies, that the community has concerns about certain types of government use and sharing of information. To build trust and support, governments must be transparent about the intended uses of data, particularly when there is the ability for personal or health information to be used for purposes beyond those for which it was collected.*
>
> *Taking a proactive 'privacy-by-design' approach, which aligns data sharing frameworks with privacy requirements from the outset, will assist in building trust in the community and between public sector agencies* [OIC emphasis].

[45] See page 3 of the submission. The final report of the UN Special Rapporteur was submitted to the General Assembly on 17 October 2018 and is available at https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/Issues/Privacy/SR_Privacy/A_73_45712.docx&action=default&DefaultItemOpen=1

[46] See https://www.pmc.gov.au/sites/default/files/public-submissions/data-sharing-2018/20726.pdf at pages 4 and 5

Office of the Victorian Information Commissioner

In addition to OVIC's submissions noted on pages 13 and 21 of this paper, OVIC submitted, among other things, that '[r]elying on de-identification of personal information carries with it significant challenges and risk and is unlikely to be appropriate in a data release context'. [47]

Data Sharing models in other jurisdictions

While not recommending any particular model, the Government may wish to consider the following features of the *Victorian Data Sharing Act 2017* (**VDS Act**):

- The VDS Act promotes data sharing across government by:
    - Creating a clear framework for sharing and using data for policy making, service planning and design
    - Establishing the Chief Data Officer (**CDO**) who leads the Victorian Centre for Data Insights (**VCDI**) in working to transform how government uses data.
- The VDS Act provides a range of **protections and safeguards**, including:
    - Requiring all data to only be used for informing policy making, service planning and design
    - Providing for how identifiable data should be handled
    - Annual reporting and notifying of possible breaches to the Office of the Victorian Information Commissioner (OVIC) and the Health Complaints Commissioner (HCC)
    - Providing that existing obligations under privacy laws continue
    - New offences for unauthorised access, use or disclosure of information.[48]
- The VCDI employs a number of **privacy-enhancing techniques** including:
    - express privacy and data security safeguards under the VDS Act, including mandatory breach notification and annual reporting requirements to OVIC;
    - an additional layer of protection for data analytics conducted in a controlled environment, ensuring that reasonable steps have been taken to ensure that data no longer relates to an identifiable individual or an individual who can reasonably be identified before data analytics work commences;
    - the provision of a clear legislative framework for the sharing of public sector data only, as distinct from the release of public sector data; and
    - the employment of the Five-Safes Framework in the context of a secure environment to conduct data analytics.[49]

---

[47] See above, n 26, page 1. For further information on the limits of de-identification of personal information, see OVIC's publication 'Protecting unit-record level personal information - The limitations of de-identification and the implications for the Privacy and Data Protection Act 2014' available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf

[48] See '*Victorian Data Sharing Act 2017, Guidance for departments and agencies*' available at: https://www.vic.gov.au/system/user_files/Documents/vcdi/Victorian%20Data%20Sharing%20Act%202017%20Web%20Guidance%20UPDATE%20as%20at%2020%20Feb%202018.pdf

[49] See above, n 26, page 3

- The VDS Act **interacts with privacy laws** in the following way:
    - Privacy laws allow identifiable data to be shared where this is authorised by another Victorian law.
    - The Act works within privacy laws by providing a new 'authorisation by law' for sharing and using identifiable data (in addition to existing privacy exceptions). Otherwise, obligations under privacy laws (including the information and health privacy principles, and the Victorian Protective Data Security Framework and Standards) continue to apply. This means that the sharing of data that is already allowed under privacy laws is not affected.

- The OVIC plays an **express oversight role** over the VCDI:
    - The interaction between the VDS Act and the PDP Act is clearly outlined under section 24 of the VDS Act.
    - The CDO must report annually to Victoria's **privacy regulators: the OVIC and HCC**. This report must include matters, such as the steps taken to ensure compliance with privacy laws, the data projects that have been undertaken, details of data requests and refusals, and the issues and challenges that have arisen.
    - The VDS Act also requires the CDO and departments (as data analytics bodies) to report any breach of privacy laws to the privacy regulator (OVIC and HCC) and the original data provider.

- In order to strike a balance between data sharing and privacy considerations, the VDS Act creates two **new offences**:
    - a **general offence** for unauthorised access, use or disclosure of data or information (with a penalty of 2 years imprisonment or 240 penalty units or both)
    - a **more serious offence** where the person knows or is reckless that the data or information may be used to endanger life or safety, assist in committing an offence or impede justice (with a penalty of 5 years imprisonment or 600 penalty units or both).

OVIC has combined oversight of privacy, data protection and freedom of information in Victoria, and administers the *Privacy and Data Protection Act 2014 (Vic)* (**PDP Act**) and *the Freedom of Information Act 1982* (Vic). The Victorian Information Commissioner's legislative responsibilities include commenting on matters affecting the personal privacy of individuals, and ensuring that the objects of the PDP Act are upheld.

My Health Record and privacy issues in WA

As already noted in this paper, there has been recent community debate and concerns expressed about the use of, and access to, health information in the My Health Record System.

Under the original Personally Controlled Electronic Health Record (**PCEHR**) system introduced in 2012, Australians 'opted in' to have an online summary of their health information, whereas all Australians will now have a My Health record created under the My Health Record system, unless they 'opted out' by 31 January 2019.

The OAIC's publication 'Handling personal information in the My Health Record system' [50] states as follows:

> *When a person is authorised to collect, use or disclose health information under the My Health Records Act, this action is also authorised under the Privacy Act. This means that if a particular collection, use or disclosure is authorised by the My Health Records Act then it will not breach the* [Commonwealth] *Privacy Act.*
> ...
> *Information held in a patient's My Health Record can be downloaded to a healthcare provider organisation's local IT system.*
>
> *If information is downloaded onto a local IT system, only the information that is reasonably necessary to provide healthcare to the patient should be downloaded.*
>
> *Once information is downloaded to a local IT system, the My Health Records Act no longer applies to the health information's collection, use or disclosure. Instead, it will be subject to the Privacy Act and/or the local state or territory health information and privacy laws and professional obligations just like other health information that healthcare provider organisations handle* [OIC emphasis].

The OIC understands that the emphasised point above means that, when Western Australian State health care providers download information in a My Health Record to their local IT system, privacy legislation will not apply because the Commonwealth Privacy Act does not apply to State health care providers and Western Australia does not have privacy legislation.

The OAIC's webpage (above) says towards the bottom:

> *For further information on which privacy legislation applies when handling health information outside of the My Health Record system, see the OAIC's State and territory health privacy webpage*

The State and Territory webpage[51] says the following about WA:

> ***Western Australia***
>
> *The state public sector in Western Australia does not currently have a legislative privacy regime. Various confidentiality provisions cover government agencies and some of the privacy principles are provided for in the Freedom of Information Act 1992 (WA) overseen by the Office of the Information Commissioner (WA). The Health and Disability Services Complaints Office (HaDSCO) is an independent statutory authority that also handles complaints relating to health and disability services in Western Australia.*

The OIC has drawn this issue to the attention of the Western Australian Department of Health. The Department responded that:

---

[50] See https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-23-handling-personal-information-in-the-my-health-record-system

[51] https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions#state-and-territory-health-privacy

> *While WA does not have privacy legislation, there is legislation which covers how public health services deal with health information, namely the Health Services Act 2016 and the Mental Health Act 2014. The common law duty of patient confidentiality would also apply. ...*[T]*he downloading of information from My Health Record would be treated the same way as the collection of any other personal health information within the WA public health system (e.g. receipt of a pathology report).*

However, as noted on page 1 of this paper, it is generally accepted that the protection of privacy under the common law is inadequate and that legislation is needed both to safeguard the privacy of personal information, to provide clear guidance on the circumstances in which government can collect, hold, use and disclose personal information, and to create rights and remedies for the public when privacy is breached.

While the lack of privacy protection of health information held by WA government agencies, and the lack of rights and remedies for the public if the privacy of their health information is breached is not a new issue, the OIC considers that this issue arising from the My Health Record system highlights the associated risks.

Other privacy issues

This office has recently joined a Western Australian working group, led by the Department of Transport, looking at draft legislation (*Transport Legislation Amendment (Identity Matching Services) Bill 2019*) to enable Western Australia to participate in and support the National Identification Security Strategy, as it relates to National Driver Licence Recognition and Document Verification Service.

The OIC also considers that the lack of privacy protections in Western Australia, in the absence of privacy legislation in Western Australia, may be a significant issue in this State's proposed participation in the national biometric facial recognition system. As observed on page 15 of this paper, other states may have concerns about sharing driver licence photos with Western Australia and the public may have strong concerns about their drivers licence photos being shared in the absence of Western Australian privacy legislation regulating their disclosure and use.

Attachment 1

Office of the
Information Commissioner

Freedom of information for Western Australia

Our Ref: 07/097/01

30 June 2016

Professor Peter Klinken
Chair, Data Linkage Expert Advisory Group
Office of Science
Department of the Premier and Cabinet
2 Havelock Street
WEST PERTH WA 6005

By post and email to: [redacted]

Dear Professor Klinken Peter

SUBMISSION – REVIEW OF WESTERN AUSTRALIA'S DATA LINKAGE CAPABILITY

I refer to our previous discussions in relation to the Review of Data Linkage Activities and Capabilities in Western Australia (**the Review**). As discussed, I consider that data linkage can realise tremendous social and economic benefits for the community and I am pleased to provide this submission to the Review.

Outline

This submission addresses an aspect of the second key focus area outlined in the Terms of Reference for the Review, namely 'to examine the barriers and impediments to data linkage, and address how they can be improved'. Specifically, the submission identifies the absence of privacy legislation in the State as a potential impediment to realising the full potential of data linkage.

Context

Western Australia does not currently have privacy legislation. Commonwealth privacy legislation governs the handling of personal information by the Australian Public Service (**APS**) and by much of the private sector. All states and territories, other than Western Australia and South Australia, have privacy legislation governing the handling of personal information at state/territory and local government level.

Western Australia has some administrative arrangements that seek to encourage agencies to comply with good privacy practice in the absence of privacy legislation. These include Public Sector Commissioner's Circular 2014-02 and the associated 'Policy Framework and Standards – Information Sharing Between Government Agencies' published in January 2003. However, these arrangements are expressed broadly and, in any event, do not have the direct force of law. Their practical effect is further limited by the absence of a formal oversight or complaints role.

Albert Facey House, 469 Wellington Street, PERTH WA 6000
Telephone: (08) 6551 7888 Facsimile: (08) 6551 7889
Freecall (WA country): 1800 621 244
Email: info@foi.wa.gov.au
Web: www.foi.wa.gov.au

There are also various isolated obligations that govern the handling of personal information by Western Australian State and local government agencies in particular contexts including in some State legislation and codes of ethics and conduct.

As Information Commissioner, I am appointed by the Governor under the *Freedom of Information Act 1992* (WA) (**the FOI Act**). My main function is to deal with complaints made against decisions of Ministers and State and local government agencies under the FOI Act. The FOI Act includes provisions that provide some limited protections against the disclosure of personal information in the narrow context of a FOI application. The FOI Act does not apply to the disclosure of personal information outside the scope of the FOI Act, nor does it generally regulate the collection, storage or use of personal information by agencies.

In making this submission, I draw on my experience as Information Commissioner as well as my previous experience in the APS and in the private sector. My experience in the private sector includes advising on the impacts of privacy legislation coming into force in 2000 to cover the state and local government sectors in Victoria.

Privacy Legislation as an Enabler of Data Linkage

It is sometimes assumed that privacy legislation is primarily concerned with preventing the collection and disclosure of information. However, modern Australian privacy legislation is designed to enable the trusted collection, use and disclosure of personal information in a way that is transparent and secure.

I am aware that the current absence of privacy legislation in Western Australia at times acts as an inhibitor to information sharing between government agencies. I have witnessed agencies being reluctant to share information with other government agencies in the belief that to do so would breach privacy laws, even though no such law currently applies to them. While this reluctance may be borne out of a commendable desire to protect the privacy of individuals, it is nevertheless based on a misunderstanding. More worryingly for data linkage, the belief may be formulated in such absolute terms as to prevent any data sharing by that agency, regardless of the sensitivity or even the identifiability of the information. My office frequently receives queries from agencies demonstrating this misunderstanding.

Privacy legislation has the potential to facilitate information sharing that respects the reasonable privacy expectations of individuals. Agencies can be confident that sharing is permitted, provided it is done in accordance with clear principles that have the force of law. Further, the agency providing the information can be confident that the recipient is bound by the same privacy principles, further building trust.

The absence of privacy legislation may also frustrate data linkage initiatives that rely on personal information from other jurisdictions. Data custodians in those jurisdictions are likely to be subject to legislative obligations that only allow them to share personal information with organisations in another jurisdiction where the receiving organisation is subject to binding privacy obligations that are similar to those in the data custodian's jurisdiction. In most cases, an agency in Western Australia will not satisfy such a requirement.

The Importance of Trust

Data-driven innovation requires trust, even where the data being used is not personally identifiable. The report *Public Sector Data Management* published by the Department of the Prime Minister and Cabinet in July 2015 notes that '[f]or the APS to make effective use of data, it is crucial that we have the trust of the public. Strong assurances about data privacy and security based on rigorous adherence to protocols, and demonstrated value are key.'

The *Australian Privacy Index 2016* published by Deloitte found that 94% of consumers believe that trust is more important than convenience. The Privacy Index also noted that the most common type of privacy complaint made against public and private sector organisations was about information being used inappropriately, followed by organisations failing to secure personal information. As data linkage generally seeks to obtain insights by using data which was previously collected for some other purpose, these findings are particularly relevant. Good privacy practice and the resultant levels of trust depend not just on whether and how new information is collected, but how existing information is used and disclosed.

The reliability of big data insights relies on accurate data being collected in the first place. The Privacy Index warns that failing to meet individuals' privacy expectations can lead to organisations receiving inaccurate or fabricated personal information. While this is unlikely to have any effect on the linkage of existing data sets in WA, a general deterioration of trust in government information handling practices across the board is likely to lead to lower data reliability in data sets over time. This would negatively affect the quality of future data linkage initiatives and the insights that can be drawn from them.

While data linkage will primarily use de-identified and aggregated data, the Australian Privacy Commissioner and others have recently warned that modern data analytics can allow data to be re-identified in more cases than was previously thought. This further highlights the importance of building trust in all information handling practices.

Building Trust in the Absence of Privacy Legislation

There are ways to develop trust in government information handling practices other than through legislation. However, I consider that these are likely to be less effective and potentially more expensive and cumbersome.

The existing administrative arrangements applying to the Western Australian public sector are expressed very generally and are not supported by any comprehensive educative, oversight or complaints mechanism. In my role as Information Commissioner I have not sensed much awareness of these arrangements among the public sector, let alone among the community whose trust we are seeking to build.

Another mechanism for building trust is through requiring bilateral arrangements between data custodians, at least for the sharing or linking of personally identifiable data. These would likely take the form of Memoranda of Understanding (**MOUs**). Even leaving aside the issue of enforceability, a MOU only places obligations on those agencies that are a party to it. Given the nature of data custodianship across the sector, the number of MOUs that would need to be negotiated and administered is likely to be significant. This would come at a substantial cost. It is also likely that the obligations would vary significantly between

individual MOUs. It is easy to foresee a situation where two MOUs may be directly inconsistent. This is plainly not desirable. Finally, this patchwork approach would again lack a comprehensive educative, oversight and complaints mechanism, further eroding trust.

The Australian Privacy Commissioner has consistently encouraged the concept of 'privacy by design'. Designing privacy compliance capability into information systems at the outset is likely to be more efficient than having to retrofit such capability at a later stage. Privacy legislation would provide a stable platform upon which such systems can be designed. This contrasts with the less predictable foundation of MOUs developed on a case by case basis.

Political Support for Privacy Legislation

The introduction of privacy legislation is, of course, a matter for the elected government and its passage is a matter for Parliament. However, I note that both major parties in Western Australia are on the record as being supportive. The previous Labor government introduced the *Information Privacy Bill 2007*, but that bill lapsed when Parliament was prorogued ahead of the 2008 election. During the 2008 election campaign, the Liberal Party committed to introducing privacy legislation should it win government.

In addition to enjoying bipartisan support, the task of formulating and implementing State privacy legislation would be made easier by the extensive experience of other Australian jurisdictions. Much practical experience already exists and the consequences are known. Little, if anything, would have to be reinvented.

Further Discussions

I would be pleased to provide further information or to discuss this submission with the Advisory Group. I have no objection to this submission being made public.

Yours sincerely

Sven Bluemmel
INFORMATION COMMISSIONER

OVIC
Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/1139

18 September 2019

Ms Catherine Fletcher
Information Commissioner
Albert Facey House
469 Wellington Street
PERTH WA 6000

Dear Ms Fletcher Catherine

Western Australia privacy and data sharing law reform

Thank you for your email dated 21 August 2019, in which you sought my office's views on a number of matters relating to the administration of privacy and data sharing laws in Victoria.

I am pleased to provide you with responses to your questions, in the hope that it will assist your office prepare a submission to the Western Australian Department of Premier and Cabinet (**WA DPC**) on its discussion paper, *Privacy and Responsible Information Sharing for the Western Australian public sector* (**the discussion paper**).

Overview of the Office of the Victorian Information Commissioner

My office, the Office of the Victorian Information Commissioner (**OVIC**) was established in September 2017, by way of the *Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017*. The establishment of OVIC combined the functions of the former Freedom of Information Commissioner and Commissioner for Privacy and Data Protection, providing OVIC with regulatory oversight of freedom of information (**FOI**), information privacy, and protective data security for the state of Victoria. The Information Commissioner is supported by two Deputy Commissioners – a Public Access Deputy Commissioner and a Privacy and Data Protection Deputy Commissioner.

OVIC administers two pieces of legislation – the *Freedom of Information Act 1982* and the *Privacy and Data Protection Act 2014* (**PDP Act**). The PDP Act provides the Information Commissioner and Privacy and Data Protection Deputy Commissioner with functions and powers in relation to information privacy, protective data security and law enforcement data security.[1]

[1] The functions of the Information Commissioner and Privacy and Data Protection Deputy Commissioner are set out in Part 1A of the PDP Act.

The regulation of information privacy in Victoria is shared between OVIC and the Health Complaints Commissioner (**HCC**). The Information Privacy Principles (**IPPs**)[2] under the PDP Act apply to personal information, but they do not apply to information of a kind to which the *Health Records Act 2001* (**HR Act**) applies.[3] Individuals' health information is instead covered by the Health Privacy Principles, set out in the HR Act. The views I express in this letter are therefore limited to my office's experience in administering the PDP Act. If it would be helpful for your office to gain a complete picture of privacy regulation in Victoria, I recommend getting in touch with the HCC to hear about their experiences. I would be happy to put you in touch with my colleagues at that office.

1. Privacy and data sharing laws should be in separate pieces of legislation

It is my view that privacy and data sharing laws should be in separate pieces of legislation.

Data sharing laws were introduced in Victoria in 2017 with the passage of the *Victorian Data Sharing Act 2017* (**VDS Act**). The purposes of the VDS Act include to:

- promote the sharing and use of public sector data to support government policy making, service planning and design;
- remove barriers that impede the sharing of identifiable data with the Chief Data Officer or data analytics bodies, and facilitate sharing of data across the Victorian public sector; and
- provide appropriate protections for data sharing under the VDS Act.[4]

The VDS Act does not limit the operation of the PDP Act, and both pieces of legislation work together to facilitate appropriate data sharing within the Victorian public sector.[5]

There are a number of reasons for my view that the two laws should be enacted separately, which I have formed based on the Victorian experience of privacy and data sharing laws.

- In Victoria, the Information Commissioner is an independent regulator who has oversight of information handling in the Victorian public sector. The Information Commissioner's functions are performed independently of government, whereas the Chief Data Officer and the Victorian Centre for Data Insights (**VCDI**) sit within the Department of Premier and Cabinet, providing advice and conducting joint projects with government organisations. Having the respective functions of the privacy regulator and Chief Data Officer set out in separate legislation signals to the public sector and the community that the work of the privacy regulator is performed independently of government.
- The VDS Act gives the Information Commissioner – and the HCC – an oversight role of the activities of the Chief Data Officer. For example, the Chief Data Officer is required to report to the Information Commissioner annually on the projects conducted under the VDS Act that relate to personal information.[6] The Chief Data Officer, and data analytics bodies, are also required to notify the Information Commissioner of any breaches of the PDP Act in relation to data handled under the VDS Act.[7] These mechanisms provide the public sector and the community with assurance that data sharing and data analytics activities involving personal information are subject to scrutiny and regulatory oversight. Should WA DPC propose a similar model for WA, whereby the privacy regulator has oversight of the activities of the Chief Data Officer (or equivalent), incorporating both schemes under

[2] The 10 IPPs are contained in Schedule 1 of the PDP Act and set out the obligations of organisations in relation to their handling of personal information.
[3] The definition of 'personal information' is contained in section 3 of the PDP Act, and expressly excludes information covered by the *Health Records Act 2001*.
[4] The purposes of the VDS Act are set out in section 1 of that Act.
[5] Section 24(2) of the VDS Act states that that Act does not affect obligations under the PDP Act.
[6] Section 29 of the VDS Act.
[7] Section 24(3) of the VDS Act.

the one piece of legislation may have the perception that the privacy regulator is not independent of government. As such, I recommend WA DPC consider the model in operation in Victoria.

- Privacy laws around Australia and internationally provide privacy protections for individuals beyond when information about them is shared. The PDP Act, for example, also contains important protections for the collection, security, quality and destruction of personal information, that are critical for the use and ongoing management of information to ensure individuals' privacy is maintained. By creating a single law to cover privacy protection and data sharing, the two concepts may become conflated, and the protection of privacy may be viewed as having significance in respect of data sharing, but not more broadly.

- The Victorian experience has shown that organisations are often reluctant to share personal information for fear of breaching the IPPs in doing so. Although we believe privacy law is an enabler of safe data sharing, many government agencies still view privacy law as a barrier to information sharing, even where the act or practice an organisation is considering is already authorised by the IPPs. Creating stand-alone data sharing legislation would provide an express authority for public sector organisations to share data (which may include personal information) for specific purposes, signalling Parliament's intention that data be shared and used across government. In Victoria the VDS Act has created a clear pathway for data sharing to take place, by separating the authority for data sharing from privacy law and reshaping cultural attitudes.

2. The role of a Privacy Commissioner should include determinative functions or be limited to conciliation/mediation of privacy complaints

I am of the opinion that a Privacy Commissioner should have a power to make determinations in respect of privacy complaints.

Under the PDP Act, the Information Commissioner and Privacy and Data Protection Deputy Commissioner have a function to conciliate privacy complaints made to OVIC;[8] the Information Commissioner and Privacy and Data Protection Deputy Commissioner are not able to make determinations. If conciliation fails, or is deemed inappropriate, a complainant is able to request their complaint be referred to the Victorian Civil and Administrative Tribunal (**VCAT**),[9] where VCAT can make a determination as to whether or not there was an interference with privacy.[10]

My experience in receiving and conciliating privacy complaints has contributed to my view that a Privacy Commissioner should have determinative powers, the reasons for which are outlined below.

- The ability for a Privacy Commissioner to make determinations in a privacy complaint would provide an expeditious and informal complaint pathway, benefiting both the complainant and the respondent organisation. Complaints that have little merit can be resolved quickly where the Privacy Commissioner is able to make a decision that there has been no interference with privacy, potentially saving the complainant time and angst in going through a formal conciliation process, and in some cases, taking their complaint to VCAT. Similarly, where the Privacy Commissioner is of the view that the respondent organisation has contravened one or more of the IPPs, their determination could influence the organisation's future practices. This would be especially beneficial where the respondent organisation is a contracted service provider, that may not otherwise have obligations to comply with privacy legislation, save for those services provided under State contract.[11] As the current conciliation process under the PDP Act does not result in a determination from the Information Commissioner or Privacy and Data Protection Deputy Commissioner, neither party receives an independent view as to

[8] Section 8C(2)(d) of the PDP Act.
[9] Sections 66(2) and 71(2) of the PDP Act.
[10] Section 77 of the PDP Act.
[11] Section 17 of the PDP Act relates to the effects of outsourcing and the applicability of the IPPs in those cases.

whether or not there was an interference with privacy, potentially causing uncertainty and doing little to influence organisational practices.

- Determinations made by a Privacy Commissioner, and published on their website, can guide and influence organisational practices beyond the respondent organisation. In July 2019 OVIC commenced publishing its notices of decision in relation to FOI reviews, with the intention of educating agencies and applicants, and providing certainty as to what future decisions by the Information Commissioner and Public Access Deputy Commissioner might be on similar matters. OVIC has experienced a positive reaction to this initiative from agencies, who are using the published notices of decision as guides when making their own decisions. Having the ability to make determinations in relation to privacy complaints, and publish them, would provide predictability and assurance to both respondent organisations and privacy complainants as to the outcome they can anticipate in a given matter. Previous decisions can also serve to educate and promote best practice to other regulated organisations.

- A determination process would make it less burdensome for a complainant to demonstrate a breach of their privacy. When a privacy complaint is referred to VCAT, the complainant is at a disadvantage as the onus is on them to provide evidence that their privacy had been breached. Where a complaint is able to be investigated by a Privacy Commissioner, a more inquisitorial approach can be taken in hearing the views of both parties, before an assessment is made by the Privacy Commissioner. This would result in greater benefits for the complainant, whose privacy rights the law is intended to uphold.

3. Privacy oversight should sit with the Office of the Information Commissioner

In my view, oversight of privacy law is well placed within an Information Commissioner's office, combining information privacy and FOI functions.

The establishment of OVIC in 2017 saw the privacy regulator functions merge with those of the former FOI Commissioner, bringing the two areas under the remit of a single Information Commissioner. This approach had already been adopted in other Australian states before Victoria followed suit, leveraging off the success of this approach in other jurisdictions, particularly New South Wales and Queensland. The experiences of the New South Wales Information and Privacy Commission, Office of the Information Commissioner Queensland and OVIC have demonstrated that combined oversight of FOI and privacy has the potential to provide a coherent, consistent regulatory approach to governance and enforcement of information rights.

Despite the seeming tension between the notions of public access to government information and information privacy, in practice, it is rare for privacy law and FOI law to conflict. Where there is potential for inconsistencies between the two laws, it is my view that having a sole regulator for both areas is likely to result in a better outcome when seeking to resolve tensions, in contrast to two regulators who approach their respective jurisdictions from a single perspective.

As a former WA Information Commissioner, and having continued to work with you and your office in my role as Victorian Information Commissioner, I am of the view that the Office of the Information Commissioner for WA (**OIC**) would be well placed to take on the role of privacy regulator. As an office that already receives and responds to complaints and reviews relating to information rights, the receipt of privacy complaints would be a natural extension for the OIC. Given the existing structures and processes in place at the OIC, an expansion into oversight of privacy law would offer an effective and efficient model for implementing the regulation of privacy rights in WA. I offer this view on the assumption that the OIC would receive appropriate funding and resourcing for the expansion of its remit to oversight of information privacy.

4. Oversight of data sharing should sit with a Privacy Commissioner

In my opinion, it would be appropriate for the oversight of data sharing to sit with an Information Commissioner or Privacy Commissioner.

As noted earlier in this letter, this is the model that has been adopted in Victoria through the VDS Act, which provides an express requirement for the Chief Data Officer to report annually to the Information Commissioner on its projects involving personal information. As a business unit of the Victorian Department of Premier and Cabinet, the VCDI is subject to the PDP Act in the same way as any other Victorian public sector organisation and is therefore required to comply with the IPPs and respond to any privacy complaints made against it. Having had two years' experience with this model in Victoria, it is an approach that appears to be working well.

My view is that the function of a Chief Data Officer (or equivalent) should not rest with the entity that administers privacy legislation; the two functions should be separated, and the WA equivalent of a Chief Data Officer should be subject to oversight from the Privacy Commissioner. For similar reasons as those noted above in question 1, maintaining separation between Privacy Commissioner and Chief Data Officer would provide assurance to the public sector and community that those implementing government policy and regulating the handling of personal information are separate entities.

5. Your jurisdiction's privacy and/or data sharing laws apply to local government

The information privacy provisions under Part 3 of the PDP Act apply to local councils in Victoria.[12]

Councils often have a very direct relationship with their constituents, perhaps more so than any other level of government. The personal information held and used by local government can directly affect people's lives. Ensuring that this information is appropriately protected is an important component of privacy law and a critical function of a privacy regulator, and I would encourage the extension of a WA privacy law to local government.

Thank you again for seeking my views on the proposal for the introduction of a privacy law in WA. Your office is welcome to quote any aspect of this letter in your submission to WA DPC, or to provide a copy of this letter along with your submission, if you feel it would assist WA DPC in their consideration of the issues. My office also intends to make its own submission to WA DPC, reiterating the comments made above and in response to the additional questions raised by the discussion paper.

If you have any questions about the above comments you are welcome to contact me directly, or get in touch with my colleague Adriana Nugent, Assistant Commissioner – Policy at [redacted]. Please let me know if there is any further assistance my office can provide.

Yours sincerely

Sven Bluemmel
Information Commissioner

[12] Section 13 of the PDP Act.

OAIC

Australian Government
Office of the Australian Information Commissioner

Home / Submissions

Data Sharing and Release legislative reforms discussion paper — submission to Prime Minister and Cabinet

Date: 17 October 2019

Our reference: D2019/010579

Ms Deborah Anton
Interim National Data Commissioner
Department of Prime Minister and Cabinet
One National Circuit
Barton ACT 2600

Data Sharing and Release – Legislative Reforms Discussion Paper

Dear Ms Anton

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Office of the National Data Commissioner's (ONDC) 'Data Sharing and Release Legislative Reforms' Discussion Paper (the Discussion Paper).

The Discussion Paper continues an important conversation around the future of data sharing in Australia, commenced in 2016 by the Productivity Commission's report into *Data Availability and Use,*[1] and furthered by the 'New Australian Government Data Sharing and Release Legislation' Issues Paper in 2018[2] and the

release of the *Best Practice Guide to Applying Data Sharing Principles* (the Data Sharing Principles Guide)in early 2019.[3]

The Discussion Paper is a further step in the development of proposed Data Sharing and Release (DS&R) legislation, which has the potential to significantly change the way the Australian Government manages the data it holds on behalf of the Australian community. Since 2018, the ONDC has refined the core policy positions, which has resulted in a more detailed data sharing framework.

The OAIC appreciates the broad and consultative approach the ONDC has taken in developing this proposal. This has included acknowledgement of, and response to, a number of the privacy concerns of stakeholders. The privacy safeguards in the DS&R framework, and clarification in the Discussion Paper about how the proposed DS&R legislation will interact with the existing privacy framework, are important inclusions.

Data held by the Australian Government is a valuable national resource that can yield significant benefits for the Australian people when handled appropriately, and in the public interest. The Government holds a large volume of data that is not derived from personal information, and the OAIC generally supports greater use and sharing of such data.[4]

However, the Australian Government also holds a vast quantity of data about its citizens that is 'personal information',[5] much of it collected on a compulsory basis to enable individuals to receive a service or benefit. Some of this data is sensitive – or can become sensitive when linked or matched with other data sets.

The Australian Government therefore has unique responsibilities when making decisions about how that data should be used or disclosed. It is important to ensure that there is a strong public interest case for a policy proposal that authorises the use and disclosure of personal information for purposes beyond those originally intended at the time of collection. Laws that authorise acts or practices that may otherwise breach privacy laws must be necessary, reasonable and proportionate to achieving a legitimate policy objective.

While the OAIC understands that agencies would not be compelled to use the proposed new DS&R arrangements, the framework has the potential to allow agencies to override existing use and disclosure provisions of the *Privacy Act 1988*

(Cth) (the Privacy Act) that apply to Commonwealth-held data, invoking the 'required or authorised by law' exception to Australian Privacy Principle (APP) 6 for Australian Government agencies. In addition to the baseline standards which apply by way of the Privacy Act and APPs, additional protections apply under agency-specific legislation, such as in the form of secrecy provisions.

The OAIC has previously submitted that in order to ensure any adjustments to these arrangements are reasonable, necessary and proportionate, it will be important to consider the evidence of why existing arrangements are no longer appropriate and how to ensure any new arrangements contain more appropriate privacy safeguards.[6] The OAIC notes that some examples have been provided on the potential benefits of data-sharing including: IP NOVA, Bureau of Meteorology real-time forecasts, and work conducted by the Victorian Agency for Health Information into cardiac outcomes.

In relation to privacy safeguards, the OAIC understands that the DS&R framework will comprise primary legislation (the DS&R legislation, including the Data Sharing Principles), subordinate legislation (including the Sensitive Data Code and Accreditation Rules), contractual and administrative arrangements (including Data Sharing Agreements), and other guidance and advice as issued from time-to-time by the ONDC. It will be important to ensure that these important privacy safeguards are consistent, clear and enforceable.

In this submission, the OAIC focuses on a number of key privacy safeguards that we recommend the ONDC consider further as it develops the proposed DS&R legislation and supporting framework.[7]

A clearly and narrowly defined purpose test

A key safeguard to minimise privacy impacts of the proposal will be to ensure that the scope and purpose of the authorising legislation is clearly and narrowly defined. The OAIC recognises the ONDC's commitment to refine the purposes of data sharing to narrow the scope of the legislation taking community expectations about acceptable uses of government-held information into account.[8]

The Discussion Paper indicates that 'the sharing must be reasonably necessary to inform government policy, programs or service delivery, or be in support of

research and development'. Data Custodians will be required to apply this test as a gateway into the data sharing system. As such, the OAIC recommends that these three 'purposes' are clearly and narrowly defined in any DS&R legislation. A constrained purpose test will assist in ensuring that any subsequent impacts on individual privacy are reasonable, necessary and proportionate to achieving a legitimate policy objective with a strong public interest purpose. Additional consideration could be given to the purpose test through the Explanatory Memorandum, to clearly set out the rationale of the test, any operational limitations and provide examples as appropriate.

The OAIC also notes that the ONDC is still considering the use of public sector data for commercial purposes, which the ONDC acknowledges is a concern for stakeholders. The use of government held personal information for commercial purposes raises additional privacy impacts that would warrant a cautious and thorough consideration through a separate PIA and further public consultation, to ensure that community trust in the system is maintained.

The *Privacy Act 1988* (Cth) standards

The Privacy Act contains important rights, obligations and enforcement mechanisms to protect the personal information provided to the Commonwealth agencies and private sector organisations that are subject to its jurisdiction. The OAIC considers that data safeguards and protections introduced by the DS&R legislation should at least be commensurate with those under the Privacy Act, which provides the basis for nationally consistent regulation of privacy and the handling of personal information.[9]

We note the ONDC's proposed approach is to require that all entities handling personal information under the DS&R system are subject to the Privacy Act, or other laws that provide equivalent protections. In the Discussion Paper the ONDC noted that equivalent privacy protections would include: protections for personal information, access to redress mechanisms, monitoring and oversight by an appropriate regulator and data breach notification requirements.[10]

The OAIC welcomes further discussion with the ONDC about how these important objectives will be achieved through the DS&R legislation in order to ensure that the acts and practices of entities undertaken in connection with the data sharing

system are subject to appropriate and consistent privacy protections under the DS&R framework.

The OAIC also suggests that new data handling requirements and obligations are aligned with the Privacy Act to the greatest extent possible. For example, if the DS&R framework creates a new data breach notification scheme for data that is not personal information, the OAIC recommends that the new scheme align as closely as possible to the Notifiable Data Breach scheme under the Privacy Act. Similarly, the OAIC supports additional clarity and alignment in relation to enforcement, cooperation and investigations where the ONDC, Commonwealth, State and Territory privacy frameworks have the potential to intersect.

In relation to the Discussion Paper's proposed approach to accreditation, the OAIC supports embedding further privacy safeguards in the system through the accreditation mechanism. The OAIC supports the role that accreditation can play in ensuring that entities build privacy-by-design into their information handling practices at the outset of a project. The OAIC has experience of accreditation schemes that embed privacy protections through our work implementing the Consumer Data Right. Under that scheme, data recipients must be accredited by the ACCC and meet security requirements which have been developed in consultation with the OAIC. Australia has also committed to implementing APEC's Cross Border Privacy Rules system, which is an enforceable certification scheme to facilitate the flow of personal information across borders. The EU's General Data Protection Regulation also makes provision for certification.

The OAIC suggests that the ONDC considers other such privacy related accreditation schemes to ensure consistency and avoid fragmentation. To assist in meeting this objective, the OAIC recommends that the legislation include a requirement for the Minister to consult with the Australian Information Commissioner when making legislative rules about the privacy standards to be included in accreditation criteria.[11]

The OAIC suggests that these measures will assist to ensure consistency between the Privacy Act and DS&R framework, and will also provide clarity and simplicity for both the regulated community and regulators.

Further safeguards

The OAIC notes further important privacy safeguards – consent, data minimisation and de-identification – form part of the 'Data Principle' set out in the Data Sharing Principles Guide. The OAIC reiterates the view that data sharing should occur on a de-identified basis where possible, to minimise the privacy impacts of the scheme for individuals. Where it is not possible to use de-identified information, consideration should be given to whether it is reasonable and appropriate to seek consent.[12]

We note that the Discussion Paper says that consent will not be required in all instances of data sharing. We would welcome further clarity in the DS&R legislation about when consent will be required.

One focus of the Discussion Paper centres on the potential benefits that the introduction of the DS&R framework could bring to government service delivery. While acknowledging those potential benefits, the OAIC suggests that a consent-based model may be appropriate in relation to the proposed service delivery purpose. This would be in line with the objective of providing individuals with greater control over the handling of their personal information. We also encourage the ONDC to produce guidance on when consent would be appropriate in relation to the other purposes under the scheme, and how it should be sought.

The OAIC welcomes the opportunity to continue to work with the ONDC in relation to the matters raised in this submission.

Yours sincerely,

Angelene Falk

Australian Information Commissioner
Privacy Commissioner

23 October 2019

Footnotes

[1] Productivity Commission 2017, *Data Availability and Use,* Report No. 82, Canberra.

[2] Department of Prime Minister and Cabinet 2018, *New Australian Government Data Sharing and Release Legislation: Issues Paper for Consultation,* DPMC, Canberra.

[3] Office of the National Data Commissioner (Department of Prime Minister and Cabinet) 2019, *Best Practice Guide to Applying Data Sharing Principles*, DPMC, Canberra

[4] This is supported by s 3(3) of the *Freedom of Information Act 1982* (Cth), which provides that an object of the Act is 'to increase recognition that information held by the Government is to be managed for public purposes, and is a national resource.'

[5] 'Personal information' is defined by s 6 of the *Privacy Act 1988* (Cth).

[6] Office of the Australian Information Commissioner 2018, *New Australian Government Data Sharing and Release Legislation – Submission to the Department of Prime Minister and Cabinet*, OAIC, Sydney.

[7] Under the Privacy Act, one function of the Australian Information Commissioner and Privacy Commissioner (the Commissioner) is to examine proposed enactments that would require or authorise acts or practices of an entity that might otherwise be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals (s28A(2)(a) of the Privacy Act). The Commissioner also has the function of ensuring that any adverse effects of a proposed enactment on the privacy of individuals are minimised (s 28A(2)(c) of the Privacy Act).

[8] See, for example, the OAIC's Australian Community Attitudes to Privacy Survey 2017, which indicated that 86% of Australians considered a secondary use of their personal information (use for a purpose other than the original purpose it was provided for) to be a misuse of their personal information, but 46% of Australians were comfortable with government agencies using their personal details for research or policy-making purposes.

[9] Section 2A (c) of the *Privacy Act 1988* (Cth).

[10] Department of the Prime Minister and Cabinet 2019, *Data Sharing and Release: Legislative Reforms Discussion Paper*, p 31.

[11] Examples of such a requirement can be found in legislation or proposed legislation such as s 53 of the *Office of the National Intelligence Act 2018* (Cth), clause 7(5) of the Identity Matching Services Bill 2019, and clause 355-72 of the Treasury Laws Amendment (2019 Tax Integrity and Other Measures No. 1) Bill 2019, a proposed amendment to the *Taxation Administration Act 1953* (Cth).

[12] Office of the Australian Information Commissioner 2018, *New Australian Government Data Sharing and Release Legislation – Submission to the Department of Prime Minister and Cabinet*, OAIC, Sydney.

OVIC
Office of the Victorian
Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/4386

15 October 2019

Data Legislation Team
Department of the Prime Minister and Cabinet
PO Box 6500
CANBERRA ACT 2600

Dear Data Legislation Team

Submission in response to Data Sharing and Release Legislative Reforms Discussion Paper

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission to the Department of the Prime Minister and Cabinet (**PM&C**) in response to the *Data Sharing and Release Legislative Reforms Discussion Paper* (**discussion paper**).

OVIC is the primary regulator for information privacy, information security, and freedom of information in Victoria. My office administers both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). One of my functions under the PDP Act is to make public statements on matters that affect individuals' personal privacy. The Australian Government's data sharing and release (**DS&R**) reforms are of great interest to OVIC, given the proposed legislation provides a new authority for entities participating in the DS&R system to share public sector data, including personal information.

This submission focuses on some of the themes covered in the discussion paper relating to the proposed data sharing model.

Data sharing and open data release

OVIC strongly supports the new policy position outlined in the discussion paper of the proposed DS&R legislation providing a framework to only share public sector data, instead of facilitating sharing *and* open data release, as initially proposed in the *New Australian Government Data Sharing and Release Legislation Issues Paper* (**issues paper**).[1] In OVIC's submission to the issues paper, we identified a range of challenges with open release, particularly involving the release of information derived from personal information.[2] We are pleased to see this change outlined in the discussion paper.

Further, OVIC welcomes the distinction made between data sharing and data release, concepts which were previously conflated in the issues paper. However, further clarification regarding the term 'open data' may be useful. Data release is currently defined in the discussion paper as 'open data that is made available to the world at large', however without any of the additional context or explanation provided in the discussion paper, the term 'open data' may be unclear at face value. Specifying that the data is made

[1] July 2018.
[2] *Submission in response to the New Australian Government Data Sharing and Release Legislation Issues Paper*, 8 August 2018, available at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.

publicly available *without any restrictions on further use or disclosure* may help clarify what constitutes open data and data release.

Sharing for public benefit

Under the proposed DS&R legislation, data sharing may occur for public benefit, with the purpose test satisfied if sharing is reasonably necessary to inform or enable government policy, program and service delivery, or research and development. While a purpose test is valuable to ensure that data shared is used for the benefit of the community, it is OVIC's view that in deciding whether the purpose test is satisfied, consideration should also be given to other potentially competing public interests, such as the public interest in protecting individuals' privacy. Guidance and training provided to entities in relation to the application of the Data Sharing Principles should encourage this balancing between the public interest in reaping the benefits arising from data sharing and other public interests. Further, the DS&R legislation could include an express provision to this effect; for example, one of the objects under the PDP Act is 'to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector'.[3] OVIC suggests a similar object be included in the DS&R legislation.

The discussion paper also explores the potential for data sharing for commercial purposes. OVIC acknowledges that data sharing for research and development for commercial uses can bring benefits to the community. However, sharing for commercial purposes should be in the public interest and, importantly, meet community expectations, as noted in the discussion paper.[4] OVIC suggests PM&C consider additional safeguards where data sharing for commercial purposes is enabled under the DS&R legislation. This may include, for example, developing additional considerations or a separate decision making framework for Data Custodians to use when determining whether or not to share data for commercial purposes, in addition to or as part of applying the Data Sharing Principles. PM&C could also consider establishing a body to review decisions to share for commercial purposes specifically.

A further issue to consider is the potential for data shared for an approved purpose to be subsequently indirectly used or linked to other unauthorised purposes, such as compliance or assurance activities. Controlling the downstream uses of data will be challenging. For example, an instance may arise where data is shared for research, and that research then informs a compliance or assurance activity. Additional oversight may therefore be required around public benefit for the uses of shared data where they may be linked to unauthorised purposes.

Privacy-enhancing measures

OVIC welcomes PM&C's approach of building privacy enhancing measures into the DS&R legislation, including setting higher protections for sensitive data in a binding Sensitive Data Code. In particular, OVIC supports specific accreditation criteria for those handling personal information. More broadly, the discussion paper notes that the DS&R model will require all entities participating in the system to be subject to equivalent legal privacy obligations, including individuals and small businesses that may be exempt from the Privacy Act. Further, State and Territory users are required to be covered by the Privacy Act or a State or Territory law that provides equivalent privacy protections to the Privacy Act, including data breach notification requirements.[5]

While OVIC supports these positive privacy measures in principle, OVIC notes that the PDP Act does not contain mandatory data breach notification requirements similar to the Notifiable Data Breaches Scheme under the Privacy Act, and queries how this requirement will operate in practice, noting Recommendation 4 of the privacy impact assessment (**PIA**) report prepared by Galexia in relation to the DS&R Bill and related regulatory framework recommends the Bill 'should include a mechanism for imposing a Data Breach

[3] s 5(a) of the PDP Act.
[4] On page 27.
[5] On page 31.

Notification requirement where the entities involved operate in a State or Territory where such a requirement does not yet exist'.[6] OVIC would welcome further consultation on the design of the privacy coverage model.

Annual reporting on the operation and integrity of the DS&R system by the National Data Commissioner (**NDC**) is another welcome measure. While it does not appear that the Office of the Australian Information Commissioner (**OAIC**) will play an express oversight role within the DS&R system, OVIC suggests PM&C consider whether it would be appropriate or useful for the NDC to provide an annual report to the OAIC on data sharing decisions involving personal information, as a requirement under the DS&R legislation. This is similar to Victoria's data sharing model where the *Victorian Data Sharing Act 2017* requires the Chief Data Officer to report to OVIC annually on projects involving personal information. This could serve as an additional safeguard to ensure data sharing under the DS&R system that involves personal information is conducted transparently, and help maintain a constructive relationship between the NDC and the OAIC.

Role of the National Data Commissioner and National Data Advisory Council

OVIC recognises the importance of a positive culture towards data sharing for the success of the DS&R system, and agrees that the Office of the National Data Commissioner (**ONDC**) will play a key advocacy role in promoting cultural change across the Australian public sector. However, OVIC highlights that adequate resourcing will be needed to support the ONDC to effectively fulfil this role.

In relation to the role of the National Data Advisory Council (**Council**), the discussion paper does not specify whether the NDC will be required to follow the advice of the Council, or whether the Council plays a purely consultative role. As previously raised in its submission to the issues paper, OVIC suggests clarifying this relationship within the DS&R legislation.[7]

Data Sharing Principles

OVIC notes that PM&C issued a *Best Practice Guide to Applying the Data Sharing Principles* in March 2019. Detailed guidance on the proposed Data Sharing Principles is crucial to assist entities to safely and responsibly share data under the DS&R system, however OVIC suggests that a key message promoted in any such guidance should be that the Data Sharing Principles do not displace entities' obligations to adhere to privacy principles under any applicable privacy legislation; rather, it should be promoted that the Data Sharing Principles complement, not replace, privacy principles relating to information sharing under the Privacy Act or State or Territory privacy legislation.

Consent

The discussion paper notes that the proposed DS&R legislation will not require consent for sharing personal information, with responsibility instead placed on Data Custodians and Accredited Users to share personal information safely and respectfully, where reasonably required for a legitimate purpose.[8]

While OVIC recognises that consent is an important mechanism for individuals to protect their privacy by allowing them to exercise control over their personal information (in certain circumstances), OVIC is of the view, in agreement with PM&C's view, that consent may not be practical or feasible for all instances of data sharing under the DS&R model. As identified in the discussion paper, making consent a prerequisite for all instances of data sharing could have an adverse impact on the integrity of a dataset to be shared, in turn undermining the purpose and intention of this system.

---

[6] Recommendation 4, Galexia Privacy Impact Assessment on the Proposed *Data Sharing and Release (DS&R) Bill* and Related Regulatory Framework, 28 June 2019.

[7] Available at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.

[8] Page 32 of the discussion paper.

Rather, OVIC supports a model where consent provides one avenue to permit data sharing, but is not the sole legal authority to allow entities to do so. This is consistent with consent under the PDP Act, whereby it is one of several grounds (under certain Information Privacy Principles) that permit organisations to use, disclose, and handle personal information.

Further, OVIC notes the importance of ensuring any consent obtained is meaningful. Seeking consent may appear disingenuous to the public where an entity seeks consent from individuals to share data but shares it regardless of whether or not consent is provided, under another authority provided by the DS&R legislation or another law.

This is not to suggest that OVIC believes protections for individuals are not necessary simply because consent is not an appropriate mechanism. Entities participating in the DS&R system will therefore benefit from guidance around when consent should be built into the Data Sharing Principles, and how to ensure such consent is meaningful. OVIC believes the ONDC can play a valuable role in this regard, with guidance and advice that promotes best practice around the use and appropriateness of consent. OVIC's discussion on consent in its *Guidelines to the Information Privacy Principles* may be useful for the ONDC to consider when exploring issues around consent.[9]

Thank you for the opportunity to provide a submission to this discussion paper. OVIC notes that further consultations will occur in relation to certain elements of the proposed DS&R model and the exposure draft of the legislation. OVIC will follow the progress of these reforms with interest, and looks forward to engaging once again with these consultation processes.

I have no objection to this submission being published by PM&C without further reference to me. I also propose to publish a copy of this submission on the OVIC website, but would be happy to adjust the timing of this to allow PM&C to collate and publish submissions proactively.

If you have any questions about this submission please contact me or my colleague Tricia Asibal, Policy Officer, at [redacted]

Sven Bluemmel
Information Commissioner

[9] See the 'Key concepts' chapter, available at https://ovic.vic.gov.au/book/key-concepts/.