http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.htm

6 November 2020

Office of the National Data Commissioner

**By submission portal**

## RE: Submission to the National Data Commissioner in response to the Exposure Draft of the Data Availability and Transparency Bill

This submission from the Australian Privacy Foundation (the "Foundation") responds to the exposure draft of the Data Availability and Transparency (DAT) Bill.

### Opening comments

The Foundation recognises that access to data can improve efficiencies, and when used for the right purposes and with appropriate controls, can lead to public benefit and positive societal outcomes. However, the pursuit of greater data sharing should not come at the cost of personal privacy, and the freedoms that Australians expect and enjoy today. We are concerned that the data sharing scheme proposed under the DAT Bill underestimates its impact on the privacy landscape in Australia, and does not adequately consider the possible harm caused by mishandling of personal information.

We are unconvinced that creating a new mechanism such as this for sharing of personal information is actually an effective way of simplifying and streamlining the process. It is our view that personal information should not be included in the proposed scheme. The Foundation questions why the approach recommended by the Productivity Commission to reform ss.95 and 95A of the *Privacy Act 1988* was not undertaken instead, to broaden the

allowable research purposes for personal information. In doing this, any non-personal information datasets could then be handled under the new DAT Bill. Given that review of the *Privacy Act* is imminent, the timing of developing this scheme, which stands to have substantial impact on the privacy of Australians, is unideal. We strongly recommend that if personal information is to be included in the scheme, that the implementation of the scheme should wait until the review of the *Privacy Act* is complete.

It is clear that a significant amount of consultation and review has informed the current iteration of the DAT Bill, and while we are pleased to see the reduction in scope of the scheme to focus only on sharing of public sector data between entities, rather than the initial proposal to include public release, we remain very concerned that the proposed scheme drastically alters, and undermines, the landscape of information privacy in Australia.

Results from research commissioned by the Office of the Australian Information Commissioner on community attitudes to privacy in 2020 shows that 9 in 10 Australians want more control and choice over their personal information, not less. The MyHealth Record debate of 2018, and the low uptake of the COVIDSafe App are just two of many examples that demonstrate this attitude in action. Given the mandatory nature of much Commonwealth, state and territory data collection it is typically impractical for individuals to opt out, it is highly unlikely that the proposed data sharing scheme will provide Australians with the transparency, control and choice needed to meet community expectations.

The proposed approach of overriding all existing secrecy provisions unless explicitly excluded by the accompanying Data Availability and Transparency Regulations is a simplistic and potentially dangerous response to a complex problem. The existing laws reflect the evolution and debate of over 30 years of privacy jurisprudence, including hundreds of separate public policies resulting from consultation and debate concerning the specific social and legal context. Alarmingly, the Bill also stands to override future secrecy provisions. This top down approach fails to make appropriate contextual consideration of the potential impacts of such a broad stroke.

.

## A human rights charter is needed

The Foundation believes that fundamental human rights protections are a priority in Australia. Australia does not have national human rights protections in either legislation or in our constitution. Most advanced countries now have those protections.

The proposed DAT Bill should not proceed until Australians are guaranteed basic human rights protections which would include privacy protections.

## Privacy Impact Assessment

The recommendations in the Privacy Impact Assessment must be accepted and applied in full as a minimum response to meet basic privacy standards.

## Data sharing scheme undermines established privacy rights

The data sharing scheme proposed by the DAT Bill is essentially a carve out from the general principle of Australian Privacy Principle 6 (under the *Privacy Act 1988*) that personal information must not be used for secondary purposes. Sharing personal information under this framework would essentially be an authorised exception under the *Privacy Act* such that use or disclosure for a secondary purpose would be permitted under APP 6.2(b). This is a fundamental and significant relaxation to the way information privacy is understood and implemented in Australia.

While The Foundation is pleased to see “privacy and security of data” included as a criterion in order to become an accredited entity and as such, to enter and participate in the scheme, we are concerned that there is no mention of privacy, nor data security, in the data sharing principles themselves, which govern the way in which data is to be shared once entities are accredited. Privacy of personal information ought to be considered at every stage in the process of sharing, not limited to the entry point of the scheme. Further, management of privacy risk should be addressed in legislation, not guidance.

## Scope

The DAT Bill authorises data custodians to share public sector data, including personal information, with accredited entities from all levels of government, as well as industry, research and other private sectors. Sharing of government-collected personal information with the private sector presents immense challenges to the current privacy landscape, especially community expectations. Notably, the 2020 OAIC Community Attitudes to Privacy Survey highlighted that 70% of Australians are uncomfortable with government agencies sharing their personal information with private businesses.

The Foundation appreciates the value of sharing public sector data containing personal information with specific academic researchers or research bodies, and we support strictly controlled data sharing in this instance. We strongly recommend that the scope of the DAT Bill be narrow such that public sector data that contains personal information is not to be shared or sold to private sector entities.

## Governance

At a fundamental level it is not appropriate for the National Data Commissioner (NDC) to have powers to investigate or suspend activities given that its role includes “advocating for the sharing and release of public sector data.” This presents a conflict in the strategic direction of the NDC.

## Consent

The Foundation appreciates that consent has been recognised as particularly important throughout the consultation process and as such has been elevated to be specifically included in the data sharing principles. However, we question the reliance on a consent-based model for a scheme such as this.

The requirement to seek consent to share personal information is likely well-intentioned, yet it is not clear how a consent-based model could possibly be implemented in practice, in particular for existing data containing personal information that was collected prior to the implementation of this scheme. It is likely to be considered to be “impracticable” for a data custodian to seek individual consent for any substantial dataset that has already been collected for a particular purpose, rendering the requirement for consent essentially meaningless.

Beyond this, consent-based models do not necessarily minimise privacy related harm for individuals. It is well understood that individuals are not able to provide meaningful consent where there is a significant imbalance of power, or when dealing with complex systems that they may not fully understand. The nature of the proposed data sharing scheme is complicated, and it is unreasonable to expect individuals to be able to provide fully informed consent. We would rather see the data sharing principles explicitly emphasise upholding privacy, regardless of whether consent to share has been obtained. We have already seen the outcome of what happens when entities bombard individuals with requests for consent it turns into a tick-box compliance exercise without genuine consideration of the individual.

There is now considerable evidence that “consent fatigue” may mean that people did not understand and did not provide meaningful consent.

## Data sharing principles based on Five Safes is not a complete risk management approach

The Foundation has concerns that the risk management approach of the data sharing scheme has placed an over reliance on the Five Safes framework. The Five Safes is a useful conceptual approach to consider data access risks, but it does not address all privacy-related issues. Further, the Five Safes methodology may be useful to determine *how* to share data, but it does not adequately assess *whether* the information should be shared at all. We recognise that there is some level of public interest test under the project principle, however, “a description of how the public interest is served by the sharing” to be set out in the data sharing agreement is not a robust enough ‘test’.

While the proposal of an accreditation framework to facilitate some level of controlled access is a positive step, the proposed framework still puts the onus of assessing risk on each data custodian. The Discussion Paper states that “data custodians will have access to information about accredited entities and their data capability before deciding whether and how to share data.” We have concerns about the level of responsibility to appropriately manage risk associated with sharing personal information is being passed onto organisations that may not necessarily have the resources or capability to make these kinds of decisions. The inclusion of ADSPs to act as an “agent” of the data custodian does not resolve this issue. Agencies will need to have not only a clear and accurate understanding of the framework but also very detailed understanding of each proposed application of the personal information in order to make a sound determination. The chances of poor decision making are high.

The Foundation would rather see an approach from the NDC that focuses on the creation of a secure collaborative virtual workspace in which entities could securely access data without taking copies of it. In this sense, the NDC could build a best-practice data security environment rather than expecting each data custodian and accredited entity to manage data security and privacy risks themselves. Providing secure access for specific data for a specific period would minimise the risks associated with transfer, storage and disposal of personal information between entities.

## Increased work for the OAIC requires increased funding

We appreciate that clause 27 of the DAT Bill requires "privacy coverage" of all accredited entities to ensure that personal information is handled in accordance with privacy obligations set to the standard of the Privacy Act. Subclause (1) to this provides that entities that are not usually covered by the Privacy Act or comparable legislation may 'opt-in' for privacy coverage under the Privacy Act. This raises the potential for the OAIC to be required to regulate the handling of personal information by a broad scope of entities it has not in the past. While we welcome the potential increased coverage of the Privacy Act, the OAIC must be appropriately funded in order to be able to handle the increase in workload due to the implementation of this scheme.

## De-identified data

While there are minimal references to 'de-identified data' in the Bill, the Foundation is not reassured that this scheme has considered the implications and risks associated with de-identification. It is a matter of "when" not "if" that data will be re-identified. There have been several high-profile cases where data has been re-identified including MyKi[1] and the MBS/PBS data[2].

The Consultation Paper notes that de-identification can be used as a "privacy-enhancing measure" in instances where consent has not been sought. References like this do not adequately recognise the complexity of de-identification as a method, and the very real risk of re-identification of personal information once "de-identified."

## Deletion of data

The General Data Protection Regulation recognizes that people should have a right to delete data that is no longer legally required. This is a fundamental right in the way people control their personal information. Deleted data will not have the risk of a data breach. This right needs to be incorporated into the DAT Bill.

---

[1] See https://about.unimelb.edu.au/newsroom/news/2019/august/myki-privacy-de-railed-travellers-movements-and-identities-at-risk-by-public-release-of-anonymised-data

[2] See https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records

## Public registers, reporting and review periods

The Foundation is pleased to see that data sharing agreements, accredited users and ADSPs under this scheme are to be made publicly available. This is important in order to increase the transparency of the scheme and allow individuals, journalists and civil society groups to be able to understand the scope of data being shared between entities, and for what purposes.

The initial three-year review of the scheme should include substantial reference to the extent to which the privacy protections are operating effectively. The subsequent reviews should occur much more frequently than every ten years. Technology, societal needs, and community expectations change rapidly, and ten years is too long a period to go without reviewing the effectiveness (and potential harm) of the scheme. All reviews of the scheme should be made public.

## Payment for accreditation

It is noted in the Accreditation Framework Discussion Paper that it is possible that "fees could be introduced to meet increasing demand for accreditation as the data sharing scheme matures." This is problematic in two ways. First, it is likely to act as a barrier for some organisations to participate in the scheme. Second, aside from the issue of equal access, paying for accreditation essentially means paying for access to public sector data. This, combined with the ability for for-profit private sector companies to enter the scheme, raises significant ethical concerns about the prospect of essentially buying Australians' personal information.

If there are any concerns around "increasing demand for accreditation," this should be met with appropriate funding, rather than defaulting to a fee system. We note the ongoing underfunding of the OAIC, and strongly recommend that the NDC and other regulatory and integrity bodies are appropriately funded to perform their duties under this scheme.

## Public interest and no harm

The Foundations strongly recommends that the term public interest is defined and a “no harm test” is added to the DAT Bill. The public interest test should be defined similarly to public interest in the joint NHMRC/OAIC Guidelines[3].

If you have any questions please do not hesitate to contact Kat Lane.

Yours sincerely

Kat Lane,

Vice-Chair

[redacted]

[redacted]

[3] See NHMRC Guidelines under s.95 of the Privacy Act. Available at https://www.nhmrc.gov.au/file/2176/download?token=b90VI2ZH

## About the Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems.

The APF makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters. Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance. When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.