17 February 2021

Senate Finance and Public Administration Legislation Committee (**committee**)
PO Box 6100
Parliament House
Canberra ACT 2600

Via email: fpa.sen@aph.gov.au

To whom it may concern

Inquiry into the Data Availability and Transparency Bill 2020 and the Data Availability and Transparency (Consequential Amendments) Bill 2020

We refer to your email dated 5 February 2021, concerning the above matter. We thank you for your invitation to provide a written submission to the committee.

As the committee may be aware, we represent a group of privacy practitioners and interested citizens who made a submission on the exposure draft of the *Data Availability and Transparency Bill 2020* to the Office of the National Data Commissioner on 5 November 2020 (**NDC Submission**). The NDC Submission was an update to a previous submission that we made in 2018.

As the concerns that we raised in our NDC submission have not been addressed in the *Data Availability and Transparency Bill 2020* which was introduced to Parliament on 9 December 2020, we wish to provide you with a copy of our previous submission, with authorisation to use it for your inquiry.

As the submission is already public, we consent to the further publication of our submission for the committee's purposes. All contributors named in Annexure A of the submission are aware of this letter and have agreed to be named.

If you have any questions about this submission, please contact its primary authors at the contact details set out below.

Yours sincerely

Melanie Marks
Principal

w: elevenM.com.au

elevenM

Anna Johnston
Principal, **Salinger Privacy**
We consult, train, publish, blog and tweet on all things privacy.

Submission to the Office of the National Data Commissioner
Data Availability and Transparency Bill exposure draft
By electronic submission at https://www.datacommissioner.gov.au/exposure-draft/submission

6 November 2020

Representative response on privacy issues in the *Data Availability and Transparency Bill 2020*

We refer to the exposure draft of the Data Availability and Transparency Bill 2020 (**DAT Bill)** and the associated Explanatory Memorandum and Accreditation Framework Discussion Paper (**Discussion Paper**).

This submission brings together the views of the stakeholders listed in Annexure A of this document. We are a group of commercial, public sector and academic professionals with a common interest in ensuring that the DAT Bill and its operating framework will adequately protect, not diminish, the privacy of Australians.

1. Opening statement

We acknowledge that a significant amount of consultation and review has informed the current iteration of the DAT Bill and accompanying documents, and note that there have been substantial improvements to the proposed framework as compared to the 2018 Data Sharing and Release Issues Paper, in relation to which we made our initial group submission. Notably, we welcome the reduction in scope of the scheme for focus only on sharing of public sector data between entities, rather than the initial proposal to include public release. Public release, or 'open data', creates significantly different risks and requires a different set of safeguards compared to controlled sharing between approved entities. We are pleased to see this change in overall scope.

We also state that we are not opposed to the sharing of 'data'. Data should be made more easily available between agencies, if it will support effective public services which benefit our community and the economy. As it was stated in the 2018 Australian Government Data Sharing and Release Legislation Issues Paper, "*Greater use and sharing of public data facilitates increased economic activity and improves productivity. Without improving data accessibility within government, the opportunity for enhanced productivity, increased competition, improved service delivery and research outcomes will be missed.*" (page 3). Effective data sharing may assist with achieving these outcomes. However, the pursuit of more data sharing and usage should not come at the cost of personal privacy and should not undercut the privacy rights that Australians hold today or should hold in future. Our submission is therefore focused on the risks to privacy that we see in the DAT Bill.

2. Summary of concerns

In order of significance, we have identified the following key issues with the DAT Bill:

a) It provides a top-down override of Australian Privacy Principle (APP) 6. This is a blunt approach which dilutes the legal protections and remedies currently available to Australians.

b) It replaces a clear boundary with a set of vague and subjective controls (e.g. apply the five safes, consider risk, de-identify where possible, data security steps.) These can be effective operational measures but should supplement and enhance (rather than replace) privacy protections in law.

c) It will exacerbate the existing data governance challenges that many government agencies are currently facing. Today's inefficiencies and errors will be worsened by increasing the volume and speed of data sharing. There will be a direct downstream impact on consumers and particularly vulnerable groups who will no longer be able to seek redress under APP 6.

d) Governance and assurance over controls is overseen by the National Data Commissioner (**NDC**), a regulator whose mandate is to encourage data sharing. This is an inherent conflict of interest. Accountability for privacy governance and assurance should reside with the privacy regulator, under the Office of the Australian Information Commissioner (**OAIC**) and the OAIC must be properly funded to perform this job effectively.

e) It is a departure from global standards and is out of line with community expectations. We note the release of Terms of Reference and an issues paper (on 30 October) relating to review of the *Privacy Act 1988* (**Privacy Act**) and advocate that to the extent of crossover, the DAT Bill should not be considered until the recommendations and amendments flowing from that review are known[1].

3. Our preferred approaches

We would prefer to see the following approaches taken to reform data sharing between agencies:

a) The scope of the DAT Bill should exclude personal information and in relation to the sharing of other 'data', the DAT Bill should set minimum standards for anonymisation.

b) We advocate for review of the Privacy Act to address s.95/95A in the Privacy Act as recommended in the Productivity Commission's 2016 Report, which will negate the need to enable the sharing of personal information under the DAT Bill.

Failing these outcomes, we advocate for the following changes and clarifications to the DAT Bill:

a) Defining the 'public interest' test by drawing from existing and appropriate frameworks (such as from the joint NHMRC/OAIC Guidelines) or otherwise via an appropriate democratic process and incorporating a 'no-harm' element where the sharing includes personal

[1] Consultation on review of the Privacy Act was announced on 30 October and is open until 29 November 2020. We submit that the DAT Bill consultation period should be extended so that the impacts of the review of the Privacy Act can be contemplated properly.

information;

b) Mandating the completion of a Privacy Impact Assessment (PIA) which meets prescribed requirements and publication of the PIA with the relevant Data Sharing Agreement;

c) Enshrining in the participation framework that data sharing is to occur within a single controlled environment, namely a shared, secure research environment, to disallow copies or replications of data to occur. Under this model, access and use of data would be limited to the approved purpose for a limited time. There would be strict monitoring of the environment;

d) If consent is to be relied upon, the NDC must establish a viable model which would enable individuals to exercise a meaningful consent rather than to further entrench consent as a tick box exercise. The My Health Record system debate of 2018, and the low uptake of the contact tracing app, COVIDSafe, clearly demonstrate that Australians expect genuine choice and control when it comes to sharing their data. This is further supported by the findings of the OAIC's Community Attitudes to Privacy Survey 2020, which found that 87% of Australians want more control and choice over their personal information;

e) Excluding the private sector from participation indefinitely and at least until the first review after the framework is operating effectively; and

f) Removing all governance and assurance accountabilities relating to privacy from the NDC and assigning them to the OAIC or another suitable regulator without a conflict of interest.

Detailed feedback

Scope

1. The DAT Bill authorises data custodians to share public sector data with accredited entities from all levels of government as well as industry, research and other private sectors. Sharing of public sector data with private sector entities presents immense challenges in the current privacy landscape, including community expectations of privacy. Individuals are unlikely to reasonably expect that personal information they share with a government agency (in particular where such information is required to be provided to the government agency by law) will be shared with the private sector, especially with for-profit companies. Notably, the 2020 OAIC Community Attitudes to Privacy Survey highlighted that Australians feel more comfortable with government agencies sharing information with each other than with the private sector. In fact, 70% of Australians are uncomfortable with government agencies sharing their personal information with private businesses. (Even when asked about government agencies sharing their personal information *within* government, the level of discomfort sits at 40%.)

2. Whilst we understand and appreciate the value of sharing public sector data containing personal information with specific academic researchers or research bodies, and support controlled sharing of public sector data that does not contain personal information more broadly, we strongly recommend that the scope of the DAT Bill be narrowed such that public sector data containing personal information is not to be shared with private sector entities..

At the very least, any private sector use of public sector data containing personal information must be consistent with the permitted purposes, be able to demonstrate the public interest as well as a 'no-harm' test, must offer a demonstrable benefit to the Australian public, and not be used for commercial gain.

Privacy rights are significantly diminished

3. While there are many references to privacy in the documents accompanying the DAT Bill, there is an overarching underappreciation of the fact that the entire framework itself is a carve out from the general principle under Australian Privacy Principle (**APP**) 6 (under the Privacy Act) that personal information must not be used for secondary purposes. This represents a fundamental and significant change to information privacy protections in Australia. Sharing information under this framework is essentially an authorised exception under the Privacy Act such that use or disclosure for a secondary purpose would be permitted under APP 6.2(b) "… *authorised by or under an Australian law*." This is a significant relaxation of APP 6 as it applies to government agencies (and the private sector, as noted above).

4. At an operational level, it is unclear how key mechanisms for managing privacy risk would operate as part of the data sharing principles. The Consultation Paper notes that in the absence of individual consent, other safeguards outlined by the data sharing principles can be "dialled up" to protect privacy, such as "undertaking a privacy impact assessment as required under the Australian Government Agencies Privacy Code"(hereafter **Code**) (page 21). We recommend that the DAT Bill should specify that a privacy impact assessment (PIA) must be undertaken in every instance of sharing public sector data containing personal information under this scheme, and that reference to the PIA be made in the data sharing agreement. A PIA should be a minimum privacy control for any sharing of data containing personal information. This is consistent with the Code which requires PIAs to be conducted on all 'high risk' projects, and the OAIC's guidance which states that "factors that point to a high privacy risk"[2] include: "activity-based risk factors"; "using or disclosing personal information for secondary purposes"; "disclosing personal information outside your agency" and "data matching (linking unconnected personal information) or data linkage".

5. We are pleased to see "privacy and security of data" included as a criterion in the accreditation framework in order for an entity to enter into and participate in the data sharing scheme (DAT Bill, cl.74(2)). However, there is no reference to privacy, nor data security, in the data sharing principles under clause 16 of the DAT Bill, which govern the way in which data is to be shared once entities are accredited. In order to ensure that privacy is considered at every stage in the process of sharing, and not limited to the entry point of the scheme, we suggest that privacy and security of data be emphasised in the data sharing principles.

6. It is proposed that guidance on the data sharing principles will be developed by the NDC in consultation with relevant agencies including the OAIC to appropriately address privacy risks. As noted above, the management of privacy risk should be addressed in legislation, not guidance. Guidance should support the legislation and it should be developed by the OAIC.

[2] See https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment

7. 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 Commonwealth *Privacy Act*. Greater clarity is needed around what privacy laws are considered to meet the standard of the Commonwealth *Privacy Act*, and how this will work in practice.
8. We foresee significant difficulties with the workability of this aspect of the scheme, because accreditation is intended as a once-off process based on a judgment about an organisation, whereas privacy coverage in law shifts over time and between activities, with different activities of even the same organisation covered (or not) by different regimes.

9. For example, when private sector organisations are operating as a contracted service provider under a State contract, the practices involved in fulfilling that contract are exempt from the Privacy Act; see s.7B(5). But this does *not* necessarily mean that they are bound by a State law equivalent to the Privacy Act. They may be unregulated for those practices.

10. The effect of s.7B(5) is that a private sector organisation may only *sometimes* be bound by the APPs in the Privacy Act, sometimes by State or Territory privacy principles (either directly or via contract), and sometimes by no privacy law at all (e.g. if a supplier uses their market power to refuse to be bound by State law under contract; or if contracting with state or local government or public universities in SA and WA, which have no law to bind them to).

11. Nor can such private sector contracted service providers 'opt back in' to the APPs even if they wanted to; the 'opt in to the APPs' method is only available for small businesses (s.6E), and the 'be prescribed in' method is only for State/Territory instrumentalities (s.6F). Even if they agree to be bound by contract to meet the standards set by through the relevant set of State or Territory privacy principles, that contract is only enforceable by their client, providing no recourse or remedy for individuals who seek to complain about non-compliance with the standards set via that contract, and no investigative powers for any privacy regulator.

12. By way of example, a large consulting firm which assists public sector clients with data analytics capabilities will say, in pursuit of accreditation under this scheme, "we are bound by the APPs in the Privacy Act because our turnover is more than $3M pa". However to the extent that their clients are State or Territory public sector agencies, which includes public Universities, they will *not* be bound by the APPs. Whether or not they are bound by a State or Territory privacy law instead will differ from State to State (noting SA and WA have nothing to bind them to), as well as from client to client, and even from contract to contract.

13. An issue which highlights this gap is the right of individuals to seek correction of personal information under APP 13.2. Under APP 13.2, individuals have a right to have data corrected 'down the line' as well as in the source system. In other words, where personal information is shared between entities, the source system entity must ensure that any corrections flow to third parties with whom the personal information has been shared. If third party entities (say, the large consulting firm which assists public sector clients with data analytics capabilities) falls into the gap described above, they will not necessarily be bound by the APPs and will hold no obligation to update personal information when a correction request is made. The primary impacts are data errors and disempowerment (and potentially harm) for individuals.

14. We strongly suggest that the accreditation criteria for data recipients, that they must be bound by enforceable and effective privacy law at least equivalent to the APPs, must apply to all *recipients* (not just a lead agency such as a University when in partnership with other organisations), and to all the *practices* involved in a data-sharing or related activity. We cannot see how this can be achieved if the accreditation framework under the DAT Bill scheme does not require examination of each proposed activity on a case-by-case basis.

15. Further, if successful, this provision will require the OAIC to regulate more entities than it has historically, including different types of entities. Whilst we welcome the potential for the Privacy Act to cover some smaller private sector organisations (if they opt in under s.6E) and possibly public sector agencies and universities in SA and WA not currently regulated by privacy laws (if they agree to be prescribed under s.6F), the OAIC must be appropriately funded to absorb the increase in workload due to the implementation of this scheme.

16. Reform of ss 95 and 95A of the Privacy Act would allow for appropriate sharing of data which includes personal information between agencies, whilst offering individuals protection under the Privacy Act. We remain unconvinced that creating a new channel for data sharing simplifies and streamlines, rather than complicating matters more; why not follow the recommendations of the Productivity Commission[3] and reform ss.95 and 95A of the Privacy Act to broaden out the categories of data that can be shared for research purposes, and broaden out the allowable research purposes? Any non-personal information datasets (data about the environment etc.) can then be dealt with under the new DAT Bill.

17. Further, the approach of overriding all existing secrecy provisions unless explicitly excluded is a simplistic and dangerous response to a complex problem. Instead, we advocate for appropriate, contextual consideration of whether impacts are justified in each case. A review should be conducted of each of the statutes with secrecy provisions, and if deemed appropriate, a standard exemption inserted, pointing to the DAT Act and/or the research exemptions in the Privacy Act. See also Australian Law Reform Commission (ALRC) recommendations for review and guidance of secrecy offences.

18. We note that by also overriding all future legislation by default, the DAT Bill increases the burden on future policy-makers and legislators to remember to consider drafting exceptions to this data-sharing scheme for every new Act or set of regulations, as well as every new significant dataset. There is a high likelihood that newly created datasets, deserving of protection (such as has been recognised for the MyHealthRecord and COVIDSafe app datasets), will not be prescribed.

Consent

19. Consent is not a silver bullet when it comes to setting data sharing preferences, and this is now recognised by policymakers and many privacy regulators globally. Indeed, we note that the TOR for the current review of the Privacy Act includes consideration of the effectiveness of consent for managing personal information. Whilst we appreciate the fact that the NDC has listened to feedback on this point during consultation and that consent now appears in

[3] Recommendation 6.16 in Productivity Commission, *Inquiry Report: Data Availability and Use*, No. 82, 31 March 2017

the data sharing principles, it will not be an effective tool in practice and it will be open to circumvention or abuse as a result.

20. Specifically:
    a) It is not clear how a consent model could be implemented and maintained, particularly for the sharing of datasets containing personal information already held by a data custodian. It is likely to be considered "impracticable" for a data custodian to seek individual consent for any substantial dataset that has already been collected.
    b) Seeking consent for future data sharing plans will continue to be challenging because it is very difficult to articulate ongoing data analytics activities in any detail and will require technical know-how to be explained in plain English. Whilst this may sound simple, we observe that many entities today struggle with this task and the pace of evolution in data driven technologies is exacerbating this issue.
    c) Consent-based models have been shown to not be an effective way of minimising harm for individuals where there is an imbalance of power (such as receiving social welfare benefits), or when dealing with systems they may not fully understand.
    d) Consumers are bombarded by privacy messaging every time they engage with an app or a service, find privacy terms hard to understand and typically accept the terms of the consent without reading them.

21. If consent is to be relied upon, the NDC must establish a viable model which would enable individuals to exercise a meaningful consent rather than to further entrench consent as a tick box exercise. For example, consideration should be given to an ONDC/DAT level campaign whereby individuals understand the context of the scheme and are informed of the participants and purposes and can set their preferences periodically, rather than being hit with a request for consent for every single data flow.

De-identified data

22. References to 'de-identified data' are notably absent in the DAT Bill, and it is only mentioned once in the Explanatory Memorandum. In any case, there is a misplaced faith in the safety of 'de-identified' data, and we are not reassured that this scheme has grappled with the implications of such misplaced faith.

23. The Consultation Paper refers to de-identification as a "privacy-enhancing measure" that can be implemented where consent is not sought (page 21). References such as this do not adequately highlight the complexity of de-identification as a method, nor realise the very real risk of re-identification of personal information once "de-identified." The 2016 breach of the Privacy Act by the Department of Health regarding the release of supposedly de-identified MBS/PBS data offers a case in point. The 2018 breach of the *Privacy and Data Protection Act 2014* (Vic) by Public Transport Victoria also with regard to supposedly de-identified Myki data further highlights the extent to which the risk of re-identification continues to be underestimated. It is also quite possible to identify a person via metadata (see for example, this study by University College, London).

24. The standard should be set to the higher test of 'anonymous' data, rather than 'de-identified' data. The *General Data Protection Regulation* adopts the higher standard of 'anonymous' data, reflecting a lower risk appetite towards re-identification risk than the Australian Privacy Act currently allows. We note that the Office of the Victorian Information

Commissioner **(OVIC)** has advocated that the risks of re-identification are so high that personal information should never be publicly released in unit level record form – see 'Protecting unit-record level personal information - The limitations of de-identification and the implications for the Privacy and Data Protection Act 2014' **(OVIC Report).**

Five Safes is not a complete risk management approach

25. While the data sharing scheme has improved substantially since the 2018 Data Sharing and Release Issues Paper, there remain concerns around a risk management framework based upon the Five Safes. The Five Safes is a conceptual approach to thinking about one type of privacy risk, namely statistical disclosure (i.e. re-identification) risk. Even in the field of de-identification, the Five Safes has been criticised as not fit for purpose.[4] It is even less fit as a replacement for current legal and ethical criteria for sharing, because it was not designed to create an authority to share personal information in the first place. Five Safes does not provide for unequivocal outcomes, nor does it address all privacy-related issues or risks. Risk should be assessed and managed in a more dynamic way and should consider potential threats and attack vectors as well as 'safety' measures.

26. For a risk management approach to be consistent and effective, there must be a common understanding of risk tolerance (i.e. what constitutes 'safe'?). While the proposal of an accreditation framework to facilitate controlled access is a positive step, the proposed framework still puts the onus of assessing risk on the data custodian. We believe that the framework requires a statement of risk tolerance/appetite which has the mandate of the Australian community, flexes to the sensitivity of the dataset and includes a 'no-harm' test. The initial and evolving risk appetite statement must be set by appropriate bodies in consultation with the Australian community.

27. The Accreditation Framework 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." This implies that the data custodian is responsible for applying the principles and requirements of the DAT Bill to share and release data appropriately. While we appreciate that this process introduces a second opportunity to identify and respond to risk according to the specific context of the proposed data sharing agreement, it also raises concerns about the level of responsibility placed upon data custodians in this scheme. The inclusion of accredited data service providers to act as an "agent" of the data custodian does not resolve this issue. How will agencies (or other custodians) be equipped to make these risk-based decisions? Agencies will need to hold not only a clear and accurate understanding of the framework but also a very detailed understanding of each proposed application of the data in order to make a sound determination. The resources required to exercise effective, risk-based decision making may be prohibitive for agencies and other participants, leading agencies not to use the framework, or to make poor decisions.

28. In the alternative, the NDC could add genuine sector-wide value by building and offering a secure collaborative virtual workspace in which entities could securely access data without taking copies of it. The NDC could build a best-practice data security environment instead of expecting each data custodian and accredited entity to manage data security risks themselves. In this way, data custodians could provide access to accredited users to specific

[4] Dr. Chris Culnane, Associate Professor Benjamin I. P. Rubinstein, Professor David Watts, "Not fit for Purpose: A critical analysis of the 'Five Safes'", November 2020, available at https://arxiv.org/abs/2011.02142v1

data for a specific purpose and period, which minimises the risk associated with transfer, storage and disposal of personal information between entities. In our experience, many organisations may wish to build and/or use these types of environments, but the cost to do so is prohibitive or places limits on the software they are able to use, which results in transfer of raw data and as such, raises the privacy and data security risks. We also note that there is increasing concern about national security risks associated with Australia's capacity to secure our critical data assets (see, for example, this report from the Australian Strategic Policy Institute). This approach could mitigate many of the risk management concerns which are currently placed on the data custodian. It would also reduce duplication and data quality issues.

29. By way of example, we point to the Victorian Centre for Data Insights (VCDI), which operates under the *Victorian Data Sharing Act 2017* (VDS Act). The Victorian approach is more restrained and targeted, and more closely aligns with community expectations. Under the VDS Act, data may only be shared between Victorian government agencies (not the private sector), and only for data analytics for the purpose of informing policy making, service planning and design (not for targeting or delivery of government services). Partnerships with research organisations and industry are enabled through the VCDI, with data remaining within the VCDI's secure and purpose-built analytics environments. Data shared under the VDS Act is also subject to additional safeguards to protect individual privacy. Most notably, while personal information may be shared and integrated with other data sets under the regime, all shared data must be de-identified before use. Organisations conducting analytics with shared data must take reasonable steps to ensure that no individual is reasonably identifiable within the analytics environment or in any products of that work. Additionally:
    - secrecy provisions are only overridden where data is requested by the Chief Data Officer; and
    - the regime is subject to enhanced oversight by the Victorian Information Commissioner, including annual reporting and enhanced data breach notification requirements.

30. The Five Safes methodology helps to determine *how* to share data safely. It does not assess *whether* the data should be shared or released at all. We support the inclusion of public interest 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.' We recommend that the detailed formulation of the public interest test is copied from the joint NHMRC / OAIC guidelines which are issued under s.95/95A of the Privacy Act. Beyond this, inclusion of a 'no harm' test where the sharing includes personal information would be an improvement, to ensure that individual harm is considered as well as broad public interest. Also, in every instance, proposed sharing or disclosure should be subject to examination (ideally via a PIA, as noted above) of whether the project would breach privacy promises made to individuals in the past, or would be within their expectations. It should also consider what the downstream impacts might be on individuals once any insights arising from the data-sharing project are operationalised. Those privacy impacts could arise for people not even represented in the original dataset under consideration. A comprehensive PIA and robust application of a detailed public interest test offer a practical way of identifying and mitigating privacy risks, as well as establishing that the initiative has a 'social licence'.

Governance

31. At a fundamental level, it is not appropriate for the NDC to have powers to investigate or suspend activities given that its role includes 'advocating for the sharing and release of public sector data', (Part 4.1, DAT Bill). We see the dual roles of promoting and maximising sharing whilst protecting privacy to be at odds, and a conflict of interest.

32. Putting aside the issue of conflict, the NDC has a huge initiative to deliver with limited resources. Given that privacy protection does not appear in the principles of the Bill nor the responsibilities of the NDC, it is hard to see how the ONDC's limited funding will enable it to prioritise and provide any meaningful oversight of privacy aspects of the framework. This accountability should reside with the OAIC, bolstered by additional funding.

Enforcement framework will not prevent harm to citizens

33. Whilst the DAT Bill establishes a penalty framework for non-compliance, such as for intentional misuse of data, we consider that it is more likely that harm for individuals will result from poor decision making by data custodians – for instance, an assessment of risk which fails to identify the risk of harm to vulnerable sectors of the community, a de-identification process which is inadequate, leading to harm through re-identification, or data security controls that are inadequate or not implemented adequately. None of these examples are risks of non-compliance under the DAT Bill, and yet they give rise to real risks of harm for individual Australians.

34. We understand that data sharing decisions by data custodians will not be reviewable on their merits under this scheme. While the Explanatory Memorandum states that "existing avenues for redress in other schemes continue to be available", in reality the effect of the DAT Bill will be to close off the opportunity for redress under the Privacy Act for unauthorised disclosures, because all disclosures made under the DAT Bill will be automatically considered 'authorised'. This is a significant lessening of privacy rights for individuals who could be harmed by a disclosure under this scheme, which otherwise could have been challenged via the OAIC as a breach of APP 6. Closing off an existing complaints mechanism and opportunity to seek compensation for any harm suffered is a significant change which lessens privacy rights for Australians. We urge lawmakers and politicians to consider the gravity of this consequence and to re-think this aspect of the Bill.

35. In any event, a tort for 'serious invasion of privacy' should be enacted, with negligent release or use of government data being specifically listed in the legislation.[5] Individuals harmed need access to the courts, and the ability to pursue class actions. We note that the ACCC supported the ALRC's recommendation for a privacy tort in its Digital Platforms Inquiry Final Report (Rec 19).

[5] The ALRC's recommended tort for serious privacy invasion should be considered but would not provide adequately because it is limited to intentional privacy invasions and provides a defence for conduct 'authorised by law'. Also see Remedies for the serious invasion of privacy in New South Wales, a bi-partisan NSW parliamentary inquiry and report into remedies for the serious invasion of privacy in New South Wales.

Purposes as defined are too broad

36. Within the proposed framework, the threshold for release or sharing of data is too low because the purposes are too broad, particularly given that the framework contemplates the sharing of personal information. For example, there are very few activities of agencies that would not be caught by the terms "inform government policy or programs" or "delivery of government services".

37. We welcome the introduction of a public interest test, which is an improvement to the previous iteration of this scheme. However, there remain questions about thresholds of what is and is not in the public interest, and who gets to decide. As highlighted above, the public interest test should be utilised from the joint NHMRC/OAIC Guidelines, or else it stands to lessen the current standard applied in relation to disclosures for research purposes. The purposes test should also provide that in every instance the public interest must be met and a 'no-harm' test must be passed.

Public registers, reporting and review

38. We support the proposal that the DAT Bill would provide for data sharing agreements, accredited users and ADSPs to be publicly available. This will assist in creating a transparent scheme and allow individuals and other entities to understand the scope of data being shared between organisations, and for what purposes.

39. We also welcome the fact that the NDC is required to report annually on the scheme and its integrity. However, reporting must also address the operating effectiveness of the safeguards and controls that are in place, and any data breaches. Reporting on the benefits of sharing information should be supplemented with other important aspects, including privacy. We note that it would be more appropriate for the OAIC to provide a layer of assurance by reporting on the effectiveness of privacy measures.

40. Data sharing agreements involving personal information (whether or not attempts have been made to de-identify the personal information) should be required to address compliance with the APPs including in relation to data security, data quality, retention and destruction, access and correction. They should include a right to inspection or audit of the recipient of the data by the OAIC and/or the supplier of the data.

41. 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 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 safeguards) of the scheme. All reviews of the scheme should be made public.

Payment for accreditation

42. 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." We believe that this is likely to act as a barrier for some organisations to apply for accreditation, and therefore prevent them to participate in the scheme. Aside from

issues of unfairness and equitable access, paying for accreditation looks alarmingly like paying for access to public sector data, which, when combined with the possibility of for-profit private sector companies being able to enter the scheme, raises significant ethical concerns.

The costs associated with running the participation framework (as well as oversight, regulation, complaints and reporting) should be met through the NDC's budget. We have seen other regulatory bodies receive insufficient funding in the past (such as the OAIC), and we strongly recommend that if this scheme remains a priority for government, that the NDC is appropriately funded to be able to perform its duties under it. This should not be passed on to other organisations as a fee.

We would be willing to discuss these matters in further detail if it would assist.

(On behalf of the signatories listed in Annexure A).

Annexure A – Signatories

(Inquiries about this submission should be sent to

Dr Thalia Anthony
Professor of Law
University of Technology Sydney

Michele Bahari
Privacy specialist - In personal capacity

Susan Bennett
Principal, Sibenco Legal & Advisory
Co-founder & Director, Information Governance ANZ

Samantha Floreani
Privacy & Technology Specialist, Salinger Privacy

Donna-Leigh Jackson
Director, Calabash Solutions

Anna Johnston
Principal, Salinger Privacy

Andrew Lim
In personal capacity

James Logan
Security Specialist – In personal capacity

Melanie Marks
Principal, elevenM Consulting

Professor Moira Paterson
Director Graduate Studies, Faculty of Law
Monash University

Lynne Saunder
International Advisory Council to Information Governance ANZ

Tim de Sousa
ANZ Advisory Board member, International Association of Privacy Professionals

Jordan Wilson-Otto
Senior Consultant, elevenM Consulting

Dr Normann Witzleb
Associate Professor, Monash University Law School
Convenor, Privacy and Access to Information Group, Castan Centre for Human Rights Law
Member, Centre for Commercial Law and Regulatory Studies