SUBMISSION ON DATA AVAILABILITY AND TRANSPARENCY BILL 2020 EXPOSURE DRAFT

Minderoo Tech & Policy Lab, UWA Law School

Contents

1 Executive Summary

This submission responds to the Department of Prime Minister and Cabinet's ('DPC') *Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper ('Consultation Paper')* *(Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper, 2020)* The central position advanced by this submission is that the *Consultation Paper* and draft Bill disclose evident gaps that ought to be addressed.

The draft Bill sets out criteria for entities seeking to 'share' data (a term that includes collecting, accessing, and using data) to waive requirements to obtain the consent of people whose data will be shared. At present, those criteria are insufficiently robust and risk creating perverse incentives for widespread data collection. In light of this, this submission recommends:

Recommendation 1: That requirements for waiver of consent set out in s16(b) of the draft Bill be strengthened. Waiver of consent should require, at a minimum, demonstrating:

- **that the benefits from the data sharing are supported by evidence, and justify any risks of harm associated with not seeking consent;**
- **that there is no known or likely reason for thinking that participants would not have consented if they had been asked; and**
- **the possibility of commercial exploitation of derivatives of the data will not deprive the participants of any financial benefits to which they would otherwise be entitled.**

The *Consultation Paper* emphasises that access to data sharing arrangements will be mediated by a need to demonstrate that those arrangements are in the 'public interest'. Yet, the 'public interest' is not defined. Given the centrality of the notion of 'public interest', this submission contends that there should be a process for determining the content of that interest in any particular case is required. In order to maximise public acceptance of the practice of data sharing, that process should be relevantly democratic, with input and advice from subject matter experts.

Recommendation 2: The draft Bill be amended to require a purposive assessment of any proposed data sharing project by a Reference Committee, prior to its formalisation in a data sharing agreement. A Reference Committee should include subject matter experts relevant to the particular project, governance experts, community members (with a focus on ensuring representation of any group identified as particularly affected by a proposal), as well as a representative from the Commonwealth body from which the relevant data was sought.

Despite suggestions to the contrary in the *Consultation Paper* that a purposive *assessment* will be required before data sharing is permitted, the draft Bill

does not, in fact, require data sharing projects to be assessed against the 'public interest'. Rather, it requires only that applications for data sharing *self-repor*t on how the public interest might be served. This submission contends that the draft Bill should be amended to clearly and unambiguously require such an assessment of proposed data sharing projects to be undertaken.

Recommendation 3: The draft Bill be amended to require that any particular data sharing arrangement be assessed with specific reference to whether that proposal meets the 'public interest' test, and the content of that test be meaningfully set out.

The governance structures proposed in the *Consultation Paper* and enshrined in the draft Bill are inadequate, for two reasons. On the one hand the particular governance frameworks proposed, such as the 'Five-Safes' framework, are unproven, and have 'undergone little legal or technical critical analysis'. They are quite simply not appropriate for adoption as a governance framework for the Commonwealth's data sharing framework. Secondly, the notion that high-level governance structures are the appropriate mechanism for managing the risks associated with data sharing is misconceived. Indeed, robodebt represents a recent and egregious example of a policy failure fuelled by inappropriate use of data sharing. Robodebt demonstrates clearly that high-level governance structures will not be sufficient to manage the risk of very serious policy failures. Rather, specific, purposive assessment of individual projects is required.

Consequently, this submission recommends:

Recommendation 4: The draft Bill be amended to ensure that the functions of the Commissioner and the National Data Advisory Council include specific reference to their roles in 'ensuring that public data is used in ways that deliver public benefit', as well as in 'avoiding uses which cause public detriment'.

To remove reliance on the so-called 'five-safes' framework, we recommend:

Recommendation 5: That section 16 of the draft Bill be amended to remove references to the unproven and inappropriate 'five-safes' model. That this section be redrafted to include a traditional and robust risk-management - rather than a 'safety' - focus.

To ensure that the high-level governance frameworks be supplemented with processes requiring *all* applications for data sharing to meet a minimum standard of ethics approvals and technical skills and competence relevant to the specific project being assessed, we recommend:

Recommendation 6: That alongside the high-level governance frameworks, the Minister formulate and enact specific rules under s119(1) setting out minimum standards for ethics approvals for all proposed data sharing projects. These rules should operate alongside the assessment of the public interest in the project undertaken by the proposed Reference Committee.

All told, the *Consultation Paper* is focused on balancing the potential benefits of data sharing against the possible risks of the misuse, or leaking of that data. This is cast as balancing risks to privacy against the realisation of the 'value' of the data held by the Commonwealth government (while also diminishing that value through its free dissemination). In essence, this submission argues that this is the wrong issue to focus on. Instead of an abstract enterprise in balancing risks and opportunities, the Department should instead seek to ensure that any use of the data is in fact valuable. The 'value' of data is not merely that it exists. From the public sector's perspective, it is valuable only when it is used to achieve a particular purpose; namely the advancement of the public interest. Indeed, losing public control of that data may well significantly devalue a unique asset. Ensuring that purpose is achieved will require making intelligent assessments about particular proposals for the use of data sharing on their merits. A broad framework for the governance of data sharing is a necessary, *but not sufficient* condition for the realisation of that goal. It must be supplemented with concrete, practical mechanisms which ensure that the best possible decisions are made as to which data sharing projects to engage in, in which manner, and for which purposes.

Data sharing, on its own, is value neutral. It is neither a good, nor a bad thing. It has the potential to greatly advance the reach and scope of projects in research, development and the assessment and implementation of government policy. If follows that data sharing, as a method, will be beneficial or detrimental to the extent that it facilitates and extends good or bad proposals. It follows that a neutral framework for assessment of data sharing proposals cannot ensure that the benefits of data held by the Commonwealth are realised. Those benefits can only be realised by the successful selection of data sharing projects which achieve the goal of advancing the public interest. The recommendations made by this submission are an attempt to assist the Commonwealth to make specific improvements to the proposed data sharing framework and draft Bill so that we might better meet that goal.

2 Who We Are - The Minderoo Tech & Policy Lab

The Minderoo Tech & Policy Lab is a research institute headquartered at The University of Western Australia. The Lab is directed by legal scholar Associate Professor Julia Powles and technologist Associate Professor Jacqueline Alderson, who lead an interdisciplinary team of researchers that specialise in the development and regulation of emerging technologies.

The Lab commenced operations in September 2020 as a core node in an international tech impact network focused on tackling lawlessness in the technology ecosystem, with partners including the University of Cambridge, the University of California Los Angeles, New York University, the University of Oxford, the

Australian National University, the University of Sydney, and more.

The Lab pursues twin objectives: promoting and protecting rights for individuals and communities faced with the harmful consequences of digital technologies and data-informed systems; and providing a robust pro-innovation environment and use-cases for the stimulation of civic tech development in the public interest.

The Lab acknowledges the support of Australian charity Minderoo Foundation in the creation of the Lab. We maintain the highest standards of academic integrity and are committed to the autonomy and independence of our researchers to pursue work free of external influence.

3 Definition of Data

Data is defined in subsection 10(5) of the Draft Bill, which provides:

> **Data** is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means.

This definition mirrors other statutory provisions which set a definition of data, for example schedule 1 of the *Home Building Act 1989 (NSW),* and sections 3 of the *Public Sector (Data Sharing) Act 2016 (SA)* and *Victorian Data Sharing Act 2017 (Vic)* which provide:

> **"data"** means any facts, statistics, instructions, concepts or other information in a form that is capable of being communicated , analysed or processed (whether by an individual or by a computer or other automated means).

In practice, this definition will be limited by operation of other sections, specifically subsection 10(2), which notes,

> **Public sector data** is data lawfully collected, created or held by or on behalf of a Commonwealth body, and includes ADSP-enhanced data.

Additionally, subsection 11(3) excludes a series of listed entities, which are mainly bodies which have a law enforcement, or national security function.

This definition is very broad. Given a plain reading, it would capture quite literally all information held by any Commonwealth body. This is because all information is, by definition, in a form capable of being communicated. Were it not in such a form, it would not be information.

Section 13 provides that any data custodian of public sector data is authorised to share the data with an accredited user if the criteria in subparagraphs (a) through (e) are met. Those criteria are:

> (a) the sharing is for a data sharing purpose and not a precluded purpose (see section 15), and only the data reasonably necessary to contribute to the purpose is shared; and
>
> (b) the sharing is consistent with the data sharing principles (see section 16); and
>
> (c) the sharing is not excluded (see section 17); and
>
> (d) the sharing is in accordance with a data sharing agreement (see section 18); and
>
> (e) if the data custodian is not the only data custodian of the data—the sharing is authorised in writing by each other data custodian, or by a data custodian authorised in writing by each other data custodian to act on their behalf for the purposes of this section.

The broad definition of data taken in the draft Bill is appropriate, and avoids difficulties and confusions inherent in more restrictive definitions. However, the consequence of such a definition is that, functionally, all information held by the Commonwealth will be captured by it. Consequently, any analysis of the appropriateness of data sharing arrangements must take seriously the enormous breadth of personal data which the present scheme gives access to. The need for a data custodianship approach to management of the data is paramount.

3.1 Data custodianship

Despite its breadth, the definition of data does not capture the notion of data custodianship, which is fundamentally premised on a recognition of, and respect for, the humans behind data. Where individuals and communities entrust public officers, departments and agencies with data, those public entities are obliged to use it only for the public interest. We submit the Bill, despite its reliance on the term, fails to encapsulate the essence of what it means to be a data custodian. In addition to our detailed critique of the Bill's treatment of the notion of the public interest (see sections 4 and 7.1 of the submission), we make some observations as to the avenues for redress under the proposed scheme, and the requirement for more robust treatment of waivers of consent.

3.2 Access to remedies

We question the extent to which the Bill's remedial scheme acknowledges the impacts of data sharing on the individuals and communities to whom the shared data relates. Part 6.2 - 'Review of decisions' provides for internal and external merits review of decisions made by the Commissioner and the Commissioner's delegates. The *Explanatory Memorandum* to the Bill (at [512]) provides some context:

> Decisions made under the Commissioner's regulatory function are generally appropriate for merits review as they may directly impact the rights and interests of individuals. This would include decisions

> made under the accreditation framework (refer part 5.2) and decisions under Chapter 5 to conduct assessments and investigations, make determinations, and issue directions (refer clauses 86, 88, 89, and 98 respectively).

This demonstrates a preoccupation with the rights and interests of the parties who will most immediately and directly benefit from the proposed scheme: those who are, or are attempting to be accredited under the Bill, in order to obtain data. This is also reflected in the limited availability of the complaints mechanism in s 75 of the Bill; only (current or recently ceased) data scheme entities may complain to the Commissioner about potential breaches of the legislation.

In respect of data sharing decisions by data custodians, the *Explanatory Memorandum* states (at [52]),

> [these] will not be reviewable on their merits under this scheme. Such decisions are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data.

This position fundamentally fails to acknowledge that the interests of individuals, or groups of individuals, can, and are likely to be, adversely affected by decisions to share data that is about them. It also belies the *Consultation Paper's* emphasis on the centrality of community expectations to determining whether data sharing is in the public interest and its assurances that data scheme entities will be held accountable for the public interest of their projects. While we acknowledge that data sharing decisions will be subject to judicial review outside of the scheme, this does not resolve the Bill's failure to capture the core of data custodianship in its provision for remedies under the proposed scheme.

The *Explanatory Memorandum* also states (at [54]) that 'a person affected by a decision *based on* shared data may seek review of that decision, where legislation governing that decision sets review rights' (our emphasis). Again, the significance of a data custodian's decision to share data in the first place is bypassed. We also note that judicial or administrative review of decisions based on shared data will necessarily be confined to decisions which are made by public entities. It is concerning that while private sector decision-making based on public sector data fundamentally inheres in the scheme, none of materials acknowledge such decision-making is excluded from the oversight of public law protections.

3.3 Consent

Finally, the notion of data custodianship implies a need to respect and safeguard the autonomy of the people whose data is collected. This need is heightened in situations where the data custodian is in control of a repository of data which was not collected with consent, or was collected only for a particular purpose. Many Commonwealth agencies hold personal data in circumstances where it is

functionally impossible for individuals to opt out of data collection. For example, data on a person's travel is collected by Commonwealth agencies such as the Australian Border Force in a manner which is both routine and mandatory for all overseas travellers. Citizens might well accept that the mandatory collection and storage of that data is necessary and proportionate to the purpose of regulating border crossings. However, it does not follow that the data subjects would consent to the further use of that information for other purposes.

This concern is further compounded by the sheer scale of data collected by Commonwealth agencies. That scale is likely to make contacting individual data-subjects to seek their consent difficult, and hence arguably 'impractical'. This gives rise to a potential absurdity: that data collection practices so widespread as to make seeking consent from data-subjects impractical could be used as a justification for not requiring entities to seek consent from data-subjects.

Further, the discussion of consent within the *Consultation Paper* is extremely limited. While it notes the importance of consent, there is no discussion of the place of consent within the research framework. The *Consultation Paper* does not distinguish between situations in which data was initially collected without consent, nor where consent was limited to a particular purpose. There is no discussion - such as is found in the *National Statement on Ethical Conduct in Human Research* ('*National Statement*') - on the level of consent required, nor the capacity to withdraw or renegotiate consent.(NHMRC, 2007)

All told, the only substantive requirement relating to consent in the draft Bill is found in the project principles in 16(b): 'any sharing of the personal information of individuals is done with the consent of the individuals, unless it is unreasonable or impracticable to seek their consent;'. This differs markedly from the more robust treatment of waivers of consent found in the *National Statement.* That document requires a Human Research Ethics Committee to be satisfied of nine separate criteria before it may permit the waiver of consent requirements.(NHMRC, 2007)

The present treatment of requirements to obtain consent are insufficiently robust and risk perverse incentives. Consequently, this submission recommends:

Recommendation 1: That requirements for waiver of consent set out in s16(b) of the draft Bill be strengthened. Waiver of consent should require, at a minimum, demonstrating that the benefits from the data sharing are supported by evidence, and justify any risks of harm associated with not seeking consent; that there is no known or likely reason for thinking that participants would not have consented if they had been asked; and the possibility of commercial exploitation of derivatives of the data will not deprive the participants of any financial benefits to which they would otherwise be entitled.

4 The Notion of the 'Public Interest'

4.1 Ascribing content to the concept of public interest

The *Consultation Paper* suggests that the public interest is the central normative consideration when assessing the appropriateness of a data sharing project. It emphasises that the concept of the public interest drives the entire Bill and is also a pivotal safeguard against misuse of data shared with the private sector. In discussing data sharing with commercial applications, the *Consultation Paper* explicitly states that the authorisation to share does not exist if the public interest of a data sharing project is not satisfied. Despite its significance to the proposed scheme, the Bill does not define the term; nor does the Bill prescribe any relevant factors to be considered, or principles to be used, in evaluating the public interest in sharing particular data.

This lack of content will likely result in the use of different - and inconsistent - definitions of 'public interest' to justify assessments of how and when data should be shared by data custodians. Evaluation of the public interest forms one component of a broader assessment of an agreement's consistency with all of the five data sharing principles in section 16 (which reflect the "five-safes" risk management model, that is critiqued further in section 7.1 of this submission). Subsection 16(6) leaves an agreement's consistency with those principles to be determined by its proponents: it requires a data scheme entity to be 'satisfied that each principle is applied to the sharing in such a way that, when viewed as a whole, the risks associated with the sharing are appropriately mitigated'. The diversity of potential data scheme entities under the scheme - academics, scientists, and innovators in the public and private sectors - will invariably bring their own interests, industry experience and subjective views on the public interest served by any proposed data sharing program. If the term is empty of content, different interest groups will inevitably obscure differences in values and interests behind the more general language of 'public interest' in the proposed scheme.

4.2 Effective accountability for public interest evaluations

As the *Consultation Paper* acknowledges, transparency and consultation in the process of evaluating the public interest are vital for building trust and accountability. Both of the *Consultation Paper* and the *Explanatory Memorandum* to the Bill promote the public register of data sharing agreements, established by section 116, for this purpose. We support the public register as a means of achieving what is undoubtedly necessary accountability and oversight. However, we consider its function as a democratic mechanism for measuring the public interest should be enhanced in two primary ways.

First, in respect of achieving transparency, we note that a data sharing agreement is only required to contain 'a description of how a data sharing project serves the public interest' (subsection 116(2)(a) of the Bill, read with the defi-

nition of 'mandatory term' in section 9 and section 18, item 7). A 'description of how a data sharing project serves the public interest' need not contain any explanation of how data scheme entities have weighed the competing risks and benefits of data sharing - to the economy, public health, the environment, and overall social wellbeing - as well as the potentially different implications of data sharing for different population groups (in particular, vulnerable communities) to conclude a project serves the public interest. For an evaluation of the public interest served by any project to be truly transparent, members of the public must have access to some level of reasoning behind any conclusion.

Second, the Bill does not provide for any consultative process by which members of the public can comment on, or contribute to developing the content of public interest considerations - either generally, or in respect of a particular project. Publication of data sharing agreements will not, in itself, effectively hold data scheme entities accountable to communities for the public interest of projects if the proposed scheme does not provide communities with an effective voice about those projects. We also note the *Consultation Paper* cautions that 'special care' ought to be taken in assessing the public interest of data sharing that impacts on vulnerable groups. Surely, any such assessment would require the direct input of representatives of any group(s) identified as particularly at risk in a particular project, if the public interest is to operate as an effective safeguard in the scheme.

4.3 A democratic mechanism for assessing the public interest

The *Consultation Paper* describes the public interest as an 'evolving' concept, subject to shifting community expectations. If it is not possible to give a definitive account of 'public interest', the scheme needs to prescribe a defined mechanism for determining what its content is at any particular time, for the purposes of assessing a particular proposal, so as to reflect community expectations. That mechanism should be broadly democratic.

This submission recommends:

Recommendation 2: The draft Bill be amended to require a purposive assessment of any proposed data sharing project by a Reference Committee, prior to its formalisation in a data sharing agreement. A Reference Committee should include subject matter experts relevant to the particular project, governance experts, community members (with a focus on ensuring representation of any group identified as particularly affected by a proposal), as well as a representative from the Commonwealth body from which the relevant data was sought.

Recommendation 3: The draft Bill be amended to require that any particular data sharing arrangement be assessed with specific reference to whether that proposal meets the 'public interest' test, and the content of that test be meaningfully set out.

Functionally, Reference Committees would provide a community-focused and industry specific assessment of proposed data sharing on a project-by-project basis. This would be a democratic means of engaging with the many, sometimes competing, values and interests that the *Consultation Paper* acknowledges are inherent in evaluations of whether data sharing is, in a particular case, in the public interest.

5 Accreditation Criteria and Data Competency Standards

One of the key mechanisms for building trust and confidence in data sharing is that public sector data will only be shared with accredited users and organisations with the appropriate technical skills and capability to do so. However, the *Accreditation Framework Discussion Paper* provides scant meaningful guidance on what is required to demonstrate this capability and meet the accreditation criteria.

The Accreditation criteria speak to organisations demonstrating effective governance and administrative frameworks, appropriate arrangements for data privacy and security, and skills and capability to handle data safely.

Section 3.3, one of the leanest sections of the *Discussion Paper*, elaborates the substantive content of the technical skills and capabilities with a standard that could be met by anyone with basic computing experience. From an organisational perspective, it could be enough that data roles were merely recruited for, or that the organisation had previous project experience with data.

While more detail is certainly required to elaborate the accreditation criteria and process, our concerns are two-fold. First, given the acknowledged capability gap between the public sector and those that seek access to public sector data, a rigorous, transparent, and contestable process for assessing capability by appropriately trained experts will be essential. Second, the supposed benefit of a streamlined, one-time-only accreditation process, which does not provide any tailored assessment of capability proportionate to a given project, provides false confidence to Data Custodians.

6 When is Data Sharing Undesirable?

The *Consultation Paper*, and exposure Bill demonstrate a clear intention on behalf of the drafters to advocate for broader data sharing. Specifically, the *Consultation Paper* notes that,

> Better use of public sector data can help us improve government services for Australians and ensure our programs and policies are informed by evidence. Greater access to public sector data with

a consistent approach to managing risk can improve research solutions to current and emerging social, environmental and economic issues.

The draft Bill establishes a National Data Commissioner by proposed s40. The Commissioner's functions are set out at proposed s41. Notably, those functions are formulated such that the Commissioner will be obliged by statute to advocate for the the benefits of sharing and releasing public sector data:

41 Functions

(1) The Commissioner has the following functions:

(a) the advice related functions set out in section 42;

(b) the guidance related functions set out in section 43;

(c) the regulatory functions set out in section 44;

(d) an advocacy function of *promoting understanding and acceptance of*:

(i) *the benefits of*, and best practice in, *sharing and releasing public sector data*; and

(ii) safe data handling practices;

(e) any other functions conferred on the Commissioner by this Act or the rules or by any other law of the Commonwealth;

(f) to do anything incidental or conducive to the performance of 18 any of the above functions.(our emphasis)

Similarly, the proposed Bill establishes a National Data Advisory Council, by proposed s60. That section also sets out the function of the Council,

60 Establishment and function of Council

The National Data Advisory Council is established by this section, and has the function of advising the Commissioner on the following matters relating to sharing and use of public sector data:

(a) ethics;

(b) balancing data availability with privacy protection;

(c) trust and transparency;

(d) technical best practice;

(e) industry and international developments;

(f) any other matters.

The proposed functions of the Council are less prescriptive than the role set by the draft Bill for the Commissioner. Nevertheless, the draft Bill does lock in

consideration of a central balance to be struck between 'data availability' and 'privacy protection'. As this submission has suggested, this dichotomy is the wrong point of focus. If the purpose of the bill is, as the *Consultation Paper* suggests, to 'to ensure data is used for the right reasons and in ways that deliver public benefit', then the focus of the Commissioner and the Council should be on that purpose. The absence of such a focus in the Commissioner and Council's proposed statutory mandate is a striking omission that ought to be remedied. Hence this submission's recommendation that:

Recommendation 4: The draft Bill be amended to ensure that the functions of the Commissioner and the National Data Advisory Council include specific reference to their roles in ensuring that data is used in ways that deliver public benefit.

Further, as presently formulated, neither the Commissioner, nor the Council have a specific stated function aimed at preventing data being used in ways that cause detriment to the public. This, too, ought to be remedied by amending the draft Bill to ensure that it contains specific reference to the function of the Commissioner and Council in safeguarding against data use which causes public detriment.

6.1 Robodebt as an example of data sharing enabling for poor policy outcomes

This submission has made the point that data sharing *per se* is a technique which is broadly neutral. That is, we would not expect the use of the technique of data sharing as such to improve or detract from the public interest. Rather, the potential of data sharing lies in its capacity to greatly expand the scope, reach and impact of research, policy assessment and implementation. The consequence of this is that data sharing has the potential to magnify the underlying benefit or detriment which attends the purpose to which it is being put. For this reasons, a neutral assessment of data sharing - or even the default assumption that data sharing on its own will attend benefits - is likely to fail to realise the true potential of data sharing as a technique. Worse still, failure to recognise the potential for data sharing to magnify the scope, reach and impact of detrimental projects is likely to lead policy makers to fail to implement sufficient controls to guard against those detriments. It is this submission's argument that the *Consultation Paper* and the draft Bill in fact fail to implement sufficient controls in this regard.

It is worth illustrating the capacity for data sharing to exacerbate poor policy outcomes by reference to a concrete example. Robodebt provides a telling case study of how the use of data sharing can be harmful in practice, by greatly multiplying the scope, reach and impact of a poorly designed and implemented project. It is worth noting at the outset that discussion of robotdebt is undertaken here to set out a recent and specific example of detrimental outcomes caused by data sharing despite the existence of robust governance frameworks. We recognise that assurance and compliance related to service delivery - such

as determining a person's eligibility for a welfare payment - is not a permitted purpose for data sharing, as noted in [107] of the *Explanatory Memorandum*. However, the two broader points illustrated by robodebt remain relevant: (1) the capacity for data sharing to greatly exacerbate poor policy outcomes, and (2) the inadequacy of high-level governance frameworks as a mechanism to guard against those outcomes in practice. Further, it is notable that despite the statements in the *Explanatory Memorandum*, the draft Bill provides at s15(4):

> (4) However, a purpose of delivery of government services, or informing government policy or programs, or research and development, in relation to matters that relate generally to compliance with or enforcement of laws is not an enforcement related purpose.

Drawing a bright line between an enforcement purpose *per se*, and 'matters that relate generally to compliance with or enforcement of laws', is likely to be difficult, particularly where the broader purpose identified is 'delivery of government programs'. Because of this, it is not possible to be entirely confident that data sharing arrangements under this proposed draft Bill will excluded all cases which might give rise to the same considerations as in robodebt.

6.2 Robodebt as a policy failure

The second interim report of the ongoing Community Affairs Reference Committee's inquiry into Centrelink's compliance program summarises the issue at hand,

> Known colloquially as 'Robodebt' due to its use of data matching, income averaging and online systems, the Income Compliance Program conducted over one million reviews of past income, issuing up to three quarters of a million debt notices to current and former social security recipients over five years until the Commonwealth Government announced that it did not have a legal basis to raise nearly half a million of those debts.(Community Affairs Reference Committee, 2020)

It bears emphasis that these are genuinely staggering figures. The Commonwealth Government raised approximately 470,000 debts without a lawful basis. In total repayment of those unlawfully raised debts is estimated to be between $721,000,000 and $1,000,000,000.(Community Affairs Reference Committee, 2020) 373,000 individuals were subject to these unlawful debt demands.(*Robodebt Class Action*) It is difficult to overstate the scale of the problem.

Crucially, the scale of the problem was a function of automating a process based on the use of inappropriate data-matching techniques. As the Commonwealth Ombudsman's 2017 report notes,

> The scale of the OCI (Online Compliance Intervention) project is significantly larger than DHS' previous debt raising and recovery pro-

> cess. DHS estimates it will undertake approximately 783 000 interventions in 2016-2017 compared to approximately 20 000 compliance interventions per year under the previous manual process.(Glenn, 2017)

What is striking about the robodebt experience is the extent to which high level governance, auditing and review frameworks systematically failed to identify or address the problem. A review by the Auditor-General which captured the robodebt program concluded 'Human Services had an effective high-level compliance strategy for administered payments made under the Centrelink program, from 2015–16 to 2017–18'.(Hehir, 2017) The 2017 report undertaken by the Commonwealth Ombudsman sounds some warnings in relation to program design,

> We asked DHS whether it had done modelling on how many debts were likely to be over-calculated as opposed to under-calculated. DHS advised no such modelling was done. In our view the absence of modelling means DHS cannot say how many debts may be under-calculated or over-calculated and by what margin.(Glenn, 2017)

It also notes '[t]he risk of over-recovering debts from social security recipients and the potential impact this may have on this relatively vulnerable group of people', recommending 'DHS re-evaluate where the risk for debts calculated on incomplete information should properly lie and investigate whether there are ways to mitigate this risk.' However, the Ombudsman did not investigate whether the OCI in fact was generating errors. Rather, they noted only 'we would be concerned if this figure [the proportion of discrepancies which do not proceed to debt recovery action] was significantly higher under the OCI than under the previous manual process. However, this *does not appear to be the case'*(our emphasis).

Given the sheer scale of the problem at hand - that is, the Commonwealth Government raising 470,000 unlawful debts - it seems incredible that specific and direct analysis separate analyses of the robodebt program by both the Auditor-General and the Commonwealth Ombudsman could fail to detect the issue. Yet, fail they did, with devastating personal consequences for many of the vulnerable individuals in the group of 373,000 against whom these unlawful debts were raised. These failures ought to chasten policymakers.

Robodebt illustrates two stark problems. First, that even the simplest examples of data sharing can act as a force-multiplier for bad policy outcomes. In that case, coupling the technique of data sharing with a project of automation expanded the capacity for errors - and hence the impact of those errors on the public - by an order of magnitude.

This is a serious risk which needs to be managed. Any data sharing arrangement which does not build in a structural mechanism for proactively identifying, managing and addressing this risk will inevitably result in far more egregious examples of policy disasters. Put another way – data sharing as such is neither

necessarily good or bad. As a technique it has the potential to turbo-charge the activities of research, development and informing policy proposals. But it will turbo-charge bad research, development and policy proposals just as readily as good. Every potential benefit of data sharing is, therefore, also a potential detriment.

The second problem robodebt illustrates is the incapacity of traditional governance mechanisms to prevent wide-scale policy disasters. As noted, both the Auditor-General and the Commonwealth Ombudsman examined the robodebt program. Both failed to identify a genuinely enormous number of concrete errors made by the Department. Indeed, the Auditor-General's report is a striking example of the fact that even 'high-level compliance strategies' which are assessed by external audit to be *effective* will not necessarily capture errors of this magnitude.

What follows from this is that governance frameworks are demonstrably insufficient for the task of guarding against public detriment exacerbated by data sharing. Rather, to avoid an inevitable string of robodebt style policy disasters being turbo-charged by use of data sharing, there will need to be some mechanism for making intelligent decisions about whether and how to use data sharing to achieve particular purposes. Absent such a mechanism, this proposed legislation will be using the hope of achieving some good policy outcomes as a reason to sanction the use of the public's data for much worse policy outcomes than would be possible without that use.

7 Alternative – Data Access Requiring Purposive Assessment by Reference Committee

As presently formulated, the Bill contains a number of significant deficiencies with respect to safeguards as to when data access will be permitted. Despite suggestions to the contrary in the *Consultation Paper*, the Bill does not restrict data sharing to cases where a public interest can be demonstrated. Further, the Bill proposes to enshrine the 'five-safes' governance framework, despite the fact that this framework is unproven and conceptually incoherent. Finally, the Bill relies almost solely on broad, high-level governance structures to guard against poor outcomes. As the discussion of robodebt above as demonstrated, these are simply not sufficient.

This submission argues that the *Consultation Paper* correctly identifies the need for purposive assessment of proposed data sharing projects on a case-by-case basis. However, this safeguard is not contained in the draft Bill as formulated. For the reasons set out below, it should be.

7.1 Failure to authorise data sharing only when 'public interest' can be demonstrated

The *Consultation Paper* sets out framework for when data sharing will be permitted. It suggests that data sharing will only be permitted in situations where there has been a specific assessment of the merits of the proposal for which data is being shared. The *Consultation Paper* specifies that:

> The Bill will authorise data sharing and release for particular purposes only, which could include:
>
> - informing government policy making
> - supporting the efficient delivery of government services or government operations
> - assisting in the implementation and assessment of government policy, and
> - research and development with clear and direct public benefits.

These provisions are laudable. However, they are not contained in the draft Bill itself. Rather, the Bill specifies at section 15 only that:

> (1) The following are **data sharing purposes**:
>
> (a) delivery of government services;
>
> (b) informing government policy and programs;
>
> (c) research and development.

Notably, the provisions of the Bill are broader than those set out in the *Consultation Paper*. In particular, the Bill does not contain the normative restrictions which are contained in the *Consultation Paper's* description of when the Bill will authorise data sharing. That is, the purpose specified in the Bill is 'delivery of government services' not 'supporting the *efficient* delivery of government services', and 'research and development', rather than 'research and development *with clear and direct public benefits*'(our emphasis).

Instead, the Bill provides only that to be an authorised sharing under section 13(1)(b), 'the sharing is consistent with the data sharing principles (see section 16)'. Subsection 16(c) provides relevantly that 'a description of how the public interest is served by the sharing is to be set out in the data sharing agreement;'. It is notable that section 18, which sets out the requirements for a data sharing agreement does not contain any particular reference to the requirement for an identified public interest.

It follows that, despite the description in the *Consultation Paper*, the Bill as presently formulated does not 'authorise data sharing and release for particular purposes' which it sets out. Rather, the Bill provides that data can be shared for the much broader reasons set out in section 15 - and no purposive assessment is made as to whether those purposes do, or are likely to meet the normative

requirements which the *Consultation Paper* implies will be mandatory. The only requirement in the Bill is that a data sharing agreement be drawn up as required by s18, and that agreement contain 'a description of how the public interest is served' by the sharing.

The difference in formulation is subtle. However, in practice that different will be very significant. Readers of the *Consultation Paper* are likely to conclude that data sharing will only be authorised for research and development where 'clear and direct public benefit' can be demonstrated. But that is not the case. Rather, the Bill provides a mechanism for sharing data without making any assessment of whether a 'clear and direct public benefit' can be established. Instead, all that is required is that the data sharing agreement contain a description of how the public interest is served by the sharing. The Bill does not specify a particular content or form for such a description.

As noted above, the Bill does not contain a definition of the 'public interest'. Taking these two observations together, we are left in a situation where data can be shared by meeting the requirement to provide only a broad reference - of unspecified content and form - to undefined criteria of 'public interest'. This seems plainly undesirable. It is certainly at odds with the description of the mechanism of the Bill contained in the *Consultation Paper*.

There is a plain disjunction between the expectations raised by the *Consultation Paper* on the one hand, and the content of the bill on the other. This submission suggests that the appropriate mechanism for remedying that disjunction is to introduce an explicit requirement for a purposive assessment of any proposed data sharing arrangement on a project-by-project basis. Hence this submission's recommendation that:

Recommendation 4: The draft Bill be amended to require that any particular data sharing arrangement be required to be assessed with specific reference to whether that proposal meets the 'public interest' test.

As will be seen, this recommendation will also address the lack of adequate governance safeguards in the Bill as presently formulated.

7.2 Inadequate governance safeguards in the proposed Bill

The *Consultation Paper* also notes that '[t]he DS&R Bill will apply appropriate and consistent safeguards to data sharing and release for these purposes'. In particularly, it identifies the 'internationally recognised Five-Safes disclosure risk management framework'. Two problems arise here. First, the 'Five-Safes' framework is unproven, and not appropriate for adoption as the main governance mechanism for the data sharing framework. Second, it is not at all clear that high-level governance frameworks are an appropriate or sufficient tool for managing the risks of data sharing. On the contrary, the experience of robodebt demonstrates that high-level governance frameworks are totally inade-

quate mechanisms for managing those risks. Third, despite the *Consultation Paper*'s suggestion that robust and purposive assessment of the merits of data sharing projects will be required by ethics reviews, the draft Bill does not in fact subject all data sharing proposals to this standard.

7.2.1 Deficiencies in the 'Five-Safes' framework

As the submission by Brennan et. al. to the WA government's *Privacy and Responsible Information Sharing for Western Australia* discussion paper notes,

> The 'five-safes' originated in work done in 2003 at the UK Office of National Statistics for its Virtual Microdata Laboratory, a confidential research enclave...
>
> Whether or not the five-safes is an appropriate effective methodology is open to question. Although a range of materials have promoted its use, we have been unable to identify any independent evaluative material that assesses its efficacy. Although it has been adopted by some jurisdictional governments, and the Commonwealth is considering deploying it in its proposed data sharing and release initiative, enthusiasm for it is largely confined to Australia and, to a lesser extent, New Zealand. It is not regarded as an internationally-accepted benchmark. It has not been adopted or endorsed by the European Union, the USA, or by Canada. We have been unable to locate any material produced by any privacy regulator in the world that endorses it.(Brennan & et. al, 2019)

This undersells the matter. The Five-Safes framework has never been subject to peer-review. There are no independent reviews of its effectiveness in practice. To adopt the unreviewed, untested 'Five-Safes' framework as the principal governance mechanism - as the proposed Bill in fact does - would be to make the Australian public at large data governance guinea pigs. This seems plainly objectionable.

Even putting aside the methodological deficiencies of the Five-Safes framework, the framework is also conceptually and practically deficient. As Brennan et. al. point out,

> The five-safes framework is not, and has never been, designed to constitute the legal authority to disclose personal information. It is intended as a methodology to address risk where the preceding legal authority to disclose personal information has first been conferred. As such, it is designed to assess risks to determine whether personal information can 'safely' be disclosed.
>
> Although the five-safes purports to be a risk management framework, it is not. It assumes that the disclosure of personal information is 'safe' where each of the five 'safe' criteria apply. It mistakenly assumes that these five factors can be crystallised at the inception of a project that seeks to disclose personal information where an

> individual has not consented to the disclosure or where some exception to privacy is available. As such, it assumes that information risk across information sharing projects is static and fixed. This assumption is wrong because disclosure risks are dynamic. They vary on an information lifecycle basis.
>
> For example, the five-safes provides no assistance in determining what 'safe people' are. If the people are 'safe' at the inception of an information disclosure project, how will an agency determine that they are 'safe' across the lifecycle the project? How will an agency go about assessing whether 'data' (i.e., personal or sensitive information) is safe to share? At the inception of an information disclosure project it might seem that disclosure risks are minimal, but the disclosed information may be linked by the recipient with other data at some time in the future in a way that is highly intrusive and uncontrolled.(Brennan & et. al, 2019)

The recent work of Culnane et. al. confirms those critiques. Indeed, they go much further, noting,

> **[T]he Fives-Safes is fundamentally flawed**: from being disconnected from existing legal protections and appropriation of notions of safety without providing any means to prefer strong technical measures, to viewing disclosure risk as static through time and not requiring repeat assessment. The five-safes provides little confidence that resulting data sharing is performed using 'safety' best practice or for purposes in service of public interest.(*Not fit for Purpose: A critical analysis of the 'Five-Safes'*)(Our emphasis).

We share these views. The Five-Safes framework 'is a largely untested and unevaluated decision-making framework that is of limited value...'(Brennan & et. al, 2019) We strongly recommend that it not be adopted.

7.2.2 Inadequacy of high-level governance frameworks

More broadly, it should be recalled that these governance frameworks - including the Five-Safes - were adopted by the Department of Social Services (DSS) in their data sharing arrangements.(Ritchie & Greene; Dr Steven McEachern,) The inadequacy of these frameworks - and of high-level governance generally as a mechanism for managing data sharing risks - is demonstrated by the DSS' involvement in robodebt. The Community Affairs References Committee notes the DSS was instrumental in the implementation of the robodebt program,

> On 11 June 2020, the Prime Minister apologised for any hurt, harm or hardship which people had experienced due to the government's raising and recovery of debts under the Income Compliance Program. This apology has also been echoed by the *Department of Social Services* and Services Australia, the government agencies responsible for the program.(Community Affairs Reference Committee, 2020) (Our

emphasis)

Given the crucial role played by DSS in the robodebt program, analysis of the data sharing principles adopted by DSS is likely to assist in understanding how such a systemic failure could occur. In that respect, the Department of Social Services Data Access Project Final Report is instructive. Specifically that report - by an author of the 'Five-Safes' framework - argues for the adoption of the evidence-based, default-open, risk-managed, user-centred (EDRU) model of data access planning, over the so-called 'traditional' model and alongside the 'Five-Safes' framework. That report notes,

> The traditional model is fundamentally defensive in nature; the focus is on the costs and risk to the data owner, and it assumes that the primary aim of any data access strategy is to prevent malicious misuse. This model therefore makes extensive use of worst-case scenarios and protection against hypothetical possibilities. The traditional model is default-closed; that is, it assumes that no access will be granted unless it can be proven to be safe. The evidence-based, default-open, risk-managed, user-centred (EDRU) model reverses almost all of these precepts.(Ritchie & Greene)

The preference for the EDRU model is spelled out explicitly;

> This reports concludes that the EDRU ethos provides a more sustainable world-view and, on the limited evidence available, is more likely to provide a secure and useful data access solution; it also seems better suited to exploit the gains from increased data access by engaging with researchers more. The report acknowledges that this is very much a minority view, but a growing one which seems likely to become much more significant.(Ritchie & Greene)

In light of the significant policy failures which attended robodebt, it is worth revisiting the extent to which adoption of the 'minority view' in favour of the EDRU model might have mirrored, or indeed exacerbate those failures. The relevant question is this: had the DSS adopted a data access strategy other than the EDRU, is it more or less likely that robodebt would have occurred as it did?

Necessarily this question is hypothetical. Consequently, it is impossible to answer definitively. Yet, this is itself a telling point. The EDRU model of data access specifically rejects the place of hypothetical worst-case scenarios as an appropriate technique for analysing risks which attend data access. As Ritchie notes, the EDRU model 'is evidence-based: hypothetical possibilities have little or no place in decision-making.' One might reasonably whether how such a model of assessment precluded serious contemplation of hypothetical, but nevertheless forseeable risks in the case of robodebt. Would such hypotheticals as 'what if inappropriate assumptions underlie the analysis of the data which is to be matched' have been dismissed as having 'no place in decision-making'?

Indeed, Ritchie goes further, arguing that the DSS' Data Access Policy Principles(*Data Access Policy Principles — Department of Social Services, Australian Government*) ought to be amended, '. . . to emphasise uncertainty and judgment, and there is also a need to acknowledge that risks are acceptable, and mistakes are expected; the important thing is contingency planning.' It is not clear when or how the public were invited to express a view on whether it believes that 'risks are acceptable,and mistakes are expected' ought to be a guiding principle for a government departments' data access policy.

Fundamentally, the Data Access Project Final Report speaks to a willingness to countenance a shift from the much maligned 'traditional', 'default-closed' system of data access, to the newer model of 'default-open' system. This is precisely the shift which the *Consultation Paper* anticipates when it notes,

> Existing data sharing arrangements across the public service are complex and hinder the use of data.
>
> Barriers to greater sharing of data within government include:
>
> - a dense web of legislative requirements which lack consistency
> - a culture of risk aversion, leading to overly cautious legislative interpretation and approval process complexity, and
> - lack of a whole-of-government approach.

In other worrying respects the *Consultation Paper* mirrors the advocacy for new, more open data sharing arrangements contending that,

> New data sharing and release arrangements will benefit Australians by streamlining the way public data is shared and released within government and with trusted users. New arrangements will provide efficient, scalable and risk-based trusted data access to datasets that have substantial and community-wide benefits for research, innovation and policy.

Yet, the capacity for data sharing to exacerbate detriments to the public is not acknowledged. Rather, concern for 'risks' is restricted to privacy considerations, and the need to weed out potential malicious actors. As the experience of robodebt demonstrates, however, these are not the only risks associated with the more widespread adoption of the techniques of data sharing. That experience also evidences the inability of high-level governance procedures to guard against the realisation of those risks.

7.2.3 Absence of robust requirements for ethics approval in all cases

The *Consultation Paper* notes that a key requirement for ensuring that any data sharing arrangement secures appropriate outcomes in practice is 'adherence to ethics processes *to determine the merits of a project*'(our emphasis). This is quite correct. However, this requirement is not adequately reflected in the draft Bill. Rather, as presently formulated, the Bill does not *require* an assessment

of the merits of a project in all cases. Two main features of the Bill give rise to this deficiency.

The first is that the requirement to adhere to ethics processes, set out in s16 does *not* make the specific reference to purposive assessment of a project contained in the *Consultation Paper*. Rather it requires only that, at ss16(a), 'any applicable processes relating to ethics are observed;'. That is, there is no requirement for assessment of a project by reference to ethical standards which seeks to determine the project's merits. In situations where a project is not subject to an external ethics review, there are **no** requirements in the Bill as proposed for such a review to be undertaken, as s16(a) applies only to 'any *applicable* processes'. This formulation risks the genuinely perverse outcome that applications for data sharing arrangements by bodies already subject to external ethics review requirements are likely to be subject to more scrutiny under the proposed Bill than those which are not. This is a particular challenge given that commercial entities are permitted to be accredited under the proposed Bill. It would mean, in practice, that the proposed Bill imposed more obligations on a university research centre which is subject to its own robust internal ethics processes than a for-profit corporation subject to no such restrictions.

This deficiency in the Bill ought to be remedied by the inclusion of a specific requirement that all applications for data sharing demonstrate that they have undergone an appropriate ethics review process.

In light of these challenges this submission recommends:

Recommendation 5: That section 16 of the draft Bill be amended to remove references to the unproven and inappropriate 'five-safes' model. That this section be redrafted to include a traditional and robust risk-management - rather than a 'safety' - focus.

Recommendation 6: That alongside the high-level governance frameworks, the Minister formulate and enact specific rules under s119(1) setting out minimum standards for ethics approvals for all proposed data sharing projects. These rules should operate alongside the assessment of the public interest in the project undertaken by the proposed Reference Committee.

These recommendations will assist in strengthening the governance framework set out by the draft Bill. More importantly, they will provide more robust procedures for the assessment of data sharing arrangements which are will offer practical safeguards against poor policy outcomes beyond those governance mechanisms. Given the demonstrated failure of even robust governance mechanisms to guard against poor outcomes, these safeguards are appropriate and necessary.

8 Recommendations

Recommendation 1: That requirements for waiver of consent set out in s16(b) of the draft Bill be strengthened. Waiver of consent should require, at a minimum, demonstrating:

- **that the benefits from the data sharing are supported by evidence, and justify any risks of harm associated with not seeking consent;**
- **that there is no known or likely reason for thinking that participants would not have consented if they had been asked; and**
- **the possibility of commercial exploitation of derivatives of the data will not deprive the participants of any financial benefits to which they would otherwise be entitled.**

Recommendation 2: The draft Bill be amended to require a purposive assessment of any proposed data sharing project by a Reference Committee, prior to its formalisation in a data sharing agreement. A Reference Committee should include subject matter experts relevant to the particular project, governance experts, community members (with a focus on ensuring representation of any group identified as particularly affected by a proposal), as well as a representative from the Commonwealth body from which the relevant data was sought.

Recommendation 3: The draft Bill be amended to require that any particular data sharing arrangement be assessed with specific reference to whether that proposal meets the 'public interest' test, and the content of that test be meaningfully set out.

Recommendation 4: The draft Bill be amended to ensure that the functions of the Commissioner and the National Data Advisory Council include specific reference to their roles in 'ensuring that public data is used in ways that deliver public benefit', as well as in 'avoiding uses which cause public detriment'.

Recommendation 5: That section 16 of the draft Bill be amended to remove references to the unproven and inappropriate 'five-safes' model. That this section be redrafted to include a traditional and robust risk-management - rather than a 'safety' - focus.

Recommendation 6: That alongside the high-level governance frameworks, the Minister formulate and enact specific rules under s119(1) setting out minimum standards for ethics approvals for all proposed data sharing projects. These rules should operate alongside the assessment of the public interest in the project undertaken by the proposed Reference Committee.

References

(2020). Office of the National Data Commissioner. https://www.datacommissioner.gov.au/sites/default/files/2020-09/DAT%20Bill%202020%20exposure%20draft%20Consultation%20Paper%20Final_0.pdf

National Statement on Ethical Conduct in Human Research (2018th ed.). (2007). https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018

Centrelink's compliance program: second interim report. (2020). Community Affairs References Committee. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024338/toc_pdf/Centrelink'scomplianceprogram.pdf

https://www.robodebtclassaction.com.au/

Centrelink's automated debt raising and recovery system (Number 02|2017). Commonwealth Ombudsman. https://www.ombudsman.gov.au/__data/assets/pdf_file/0022/43528/Report-Centrelinks-automated-debt-raising-and-recovery-system-April-2017.pdf

Human Services' Compliance Strategies (Text 15 2018-2019; Number 15 2018-2019). (2017). (Number). https://www.anao.gov.au/work/performance-audit/human-services-compliance-strategies

Independent Submission - Privacy and Responsible Information Sharing for Western Australia. (2019). https://www.wa.gov.au/sites/default/files/2019-12/Independent_submission_P_Brennan_19141512.pdf

https://arxiv.org/pdf/2011.02142.pdf

Department of social services data access project final report. https://uwe-repository.worktribe.com/output/908255. https://uwe-repository.worktribe.com/output/908255

Enabling access to sensitive data at the Australian Data Archive. https://conference.eresearch.edu.au/2018/08/enabling-access-to-sensitive-data-at-the-australian-data-archive/

https://www.dss.gov.au/about-the-department/policies-legislation/data-access-policy-principles. https://www.dss.gov.au/about-the-department/policies-legislation/data-access-policy-principles