Submission to the Australian Government on the **Data Availability and Transparency Exposure Draft**

Submission by:
Prof. Kimberlee Weatherall[1], Sydney Law School, University of Sydney, and Chief Investigator with the ARC Centre for Automated Decision-Making and Society; and
Melanie Trezise, PhD Candidate, Sydney Law School
6 November 2020

Overview

1. This submission responds to the Exposure Draft of the Data Availability and Transparency Bill 2020 (the Exposure Draft). The question is whether the potential benefits to be gained as a result of the Exposure Draft outweigh the risks to which it gives rise. In our view, they do not, and changes are needed: to the Exposure Draft, to the surrounding legal framework, and to the culture of the public service.

2. The Exposure Draft aims to unlock the undoubted potential of data for research and policy development, and to modernise the data sharing environment in Australia and enable data sharing in the public interest. It also aims to build confidence in the use of public sector data. We do not think it is likely to achieve either goal.

3. It is not clear that the Exposure Draft will achieve the claimed benefits of rationalising or significantly encouraging data sharing. The Exposure Draft proposes a new, alternative, **optional** pathway to share data, supported by an accreditation process and other conditions on the sharing of data. Existing "ad hoc"[2] data sharing arrangements are permitted to continue, so data sharing is not rationalised, but complexity is added. The lack of mandatory integration between government service-provision agencies means that agencies may choose whether or not to engage with other agencies to support streamlined customer service provision to customers of government services in Australia. A range of other public policy approaches would be needed to effectively address the known reluctance of public sector agencies to share information.

4. At the same time, the Exposure Draft risks damaging public confidence in sharing by failing to provide the necessary safeguards to justify public confidence. The Exposure Draft, by allowing for sharing for research and development (s 15(1)) and with commercial entities opens up a very broad set of potential circumstances for data sharing. Based on evidence cited in the Discussion Paper, as well as evidence from previous research,[3] we are not convinced that the Australian government presently has the social licence to share public data for commercial research and development, even if (as self assessed by public servants) it is in the public interest. In our view, too, safeguards additional to those presently in the Exposure Draft would be

---

[1] The author can be contacted at k mber ee.weathera @sydney.edu.au. Curr cu um v tae and other nformat on s ava ab e at https://www.sydney.edu.au/ aw/about/our-peop e/academ c-staff/k mber ee-weathera .htm

[2] Off ce of the Nat ona Data Comm ss oner, *Data Availability and Transparency Bill 2020 Exposure Draft* (Consu tat on Paper, September 2020; here nafter Consu tat on Paper), 7.

[3] Gogg n, G., Vromen, A., Weathera , K., Mart n, F., Webb, A., Sunman, L., Ba o, F. (2017). *Digital Rights in Australia*, ava ab e at SSRN: https://ssrn.com/abstract=3090774.

necessary where the usual safeguards on research within the university and not-for-profit sector (such as Human Research Ethics Review) can no longer be assumed due to the breadth of potentially accredited entities.

5. In addition, the Exposure Draft creates ethical and privacy risks, including the erosion of the concept of consent as a basic privacy protection, inadequate details relating to the practical implementation of the scheme, and insufficient safeguard design. Current privacy protections for Australians are known to be inadequate,[4] and we do not have a clear sense, as yet, of when and how those inadequacies will be addressed.

6. The outcome is a proposal in which the risks to private citizens significantly outweigh any benefits.

Research and development including commercial research and development, and the need for greater safeguards for commercially oriented research

7. Access to publicly held data can enable new and important research. Under the Exposure Draft, data sharing for research purposes is not limited to universities and research institutions, but includes commercial research and development. We do not think that public concern about (and hence the limited social licence for) the use of public data for commercial purposes,[5] or the heightened safeguards that would be required to enable public trust in commercial use of public data, are adequately addressed in the Exposure Draft.

8. The 2017 Productivity Commission Report on Data Availability and Use stated that "ARAs should preferably be **public sector entities or agencies** (Commonwealth, State or Territory), other **publicly-funded** institutions or not-for-profit entities that have a focus on release of data for public interest uses… Private entities are not excluded from being ARAs, but it is less likely that a private entity could demonstrate to the ONDC that they have the desired characteristics."[6] The potential breadth of "research and development" as a data sharing purpose, and the lack of limitation on private or commercial use of data leaves the legislation open to be interpreted far beyond the original recommendation of the Productivity Commission. The anticipated accreditation of foreign-owned entities is of additional concern from the perspective of social licence and the desire to build public trust in data-sharing.

9. The chief safeguards that reflect public concerns about commercial sharing are the requirement that the sharing be consistent with the data sharing principles based on the Five Safes Framework (ss 13; 16) (which includes identifying, under the 'project principle', a description of 'how the public interest is served by the sharing') (s 18); the continued applicability of information of privacy law where a data recipient receives personal information; as well as other legal protections, such as consumer protection law.

---

[4] Th s was the conc us on, for examp e, of the Austra an Compet t on and Consumer Comm ss on n ts *Digital Platforms Inquiry: Final Report* (2019), as we as the Government s response to that Report stat ng the ntent on to rev ew the *Privacy Act 1988* (Cth).

[5] Consu tat on Paper, 27.

[6] Emphas s added: Product v ty Comm ss on, "Data Ava ab ty and Use", *Productivity Commission Inquiry Report* No. 82, 31 March 2017 <https://www.pc.gov.au/ nqu r es/comp eted/data-access/report/data-access.pdf>, 250.

10. In our view these safeguards are **not** adequate.

Public interest

11. The requirement that the data sharing be 'in the public interest' is effectively self-assessed by the data scheme participants (data custodian and accredited entity). The only 'accountability' for this judgment is that the data-sharing agreement is to be included in the register: i.e. accountability *through transparency*. However, there is no accountability *through appeal or review of the decision.* As far as we are able to determine on our reading of the Exposure Draft, a determination by a data custodian that sharing is in the public interest is not able to be challenged: whether by members of the public affected, or any other interested party. There are no consequences - other than perhaps negative publicity - for a bad decision. The Exposure Draft provides only that decisions *made by the Commissioner* (or delegates) are reviewable (ss 103; 104). A decision that certain data be shared is not made by the Commissioner or a delegate of the Commissioner. In other words, the only realistic way to hold scheme participants accountable for their data sharing decisions and their public interest decisions is through public exposure. We submit that this is unlikely to promote public trust.

12. The 'public interest' is not defined. We note that this is a deliberate decision, on the basis that it is a dynamic concept and must be allowed to develop over time. This is understandable. However, the Consultation Paper is extremely broad in its description, talking about potential benefits (and risks) to "the economy, public health, the environment, and overall social wellbeing"; the paper later refers to "increased jobs".[7] The scheme which would be established by the Exposure Draft thus has a more explicitly commercial orientation than is immediately conveyed by the stated purposes, or than was originally proposed by the Productivity Commission.

13. It would appear to be entirely possible for a data custodian to determine that sharing with a commercial firm for commercial purposes is in the public interest, because of the economic activity to which this would give rise. We would argue that this determination, although available under the Exposure Draft, is not consistent with the current social licence for data sharing. We note, too, that while the Consultation Paper refers to community expectations as important in assessing the public interest, there is no reference to community expectations in the Exposure Draft itself.

Five Safes/Data Sharing Principles

14. The Five Safes principles, adopted and remodelled in the form of the Data Sharing Principles set out in s 16, are insufficient as a set of safeguards. So far as we are aware, there has not been an independent evaluation of their effectiveness in assuring appropriate assessment of data risks. No independent evaluation has been provided in the course of this consultation. They have been criticised by experts:[8]

    a. The 'Five Safes' framework does not provide for *ongoing* assessment of risks: a particularly critical component in the case of data as it is used in machine

[7] Consu tat on Paper, 21.

[8] See, eg, Cu nane, Rub nste n, and Watts, "Not F t for Purpose: a cr t ca ana ys s of the F ve Safes " (2020), ava ab e at http://arx v.org/abs/2011.02142.

learning or artificial intelligence contexts, where analysis may give rise to unexpected results;

b. The framework focuses on finding bases for assessing *safety* rather than on identifying and analysing *risks.*[9] This is not merely semantic - a mindset focussed on *risk* considers potential attackers or harms - which we submit would be critical for many data projects;

c. We note also that in the context of the data sharing principles, the concept of 'safety' has been replaced with 'appropriate' (that is, 'appropriate' persons, projects, settings, data). We suggest that 'appropriate' is a weaker concept than 'safety', and even less connected to an assessment of risk;

d. The Five Safes framework (and its counterpart in the Exposure Draft) considers **outputs** but not **outcomes** beyond the immediate scope of the project. 'Outputs' may be publications or products. *Outcomes* are impacts in the world; the possible implications that may emerge from a data analysis. Again, we would argue that in the context of an environment in which the use of artificial intelligence and machine learning is increasing, and where data may be used to automate decision-making, **outcomes** are important, including for example the human impact of decisions made using data. We note that in New South Wales, while the Five Safes framework is used, data-sharing also operates within a broader **outcomes framework** that focuses attention of departments on the overall public goals of the government.[10]

Ethical assessment of projects

15. The data sharing principles do not require the ethical assessment of projects. Human research conducted through the university system must undertake Human Research Ethics processes and receive Human Research Ethics Committee (HREC) approval. No such requirements apply to commercial bodies undertaking research (except in certain limited circumstances, like medical research). The current data sharing principles in s 16 refer only to *applicable* processes relating to ethics. They do not mandate any ethics in cases where such an obligation does not already exist. The Consultation Paper only states that data scheme entities ***should consider*** seeking independent advice on the ethical implications of the project and how to mitigate identified risks"[11] (emphasis added). This is particularly striking in the context of (commercial *and* non-commercial) research projects potentially proceeding without full consent of the participants.[12]

16. It is submitted that, if data sharing for the purposes of research is to extend beyond that set of accredited entities where researchers are always obliged to obtain ethical approval for human research, some equivalent safeguard is needed. For example, an

---

[9] Ib d, 6.

[10] See, for examp e, https://www.f nance.nsw.gov.au/human_serv ces.

[11] Consu tat on Paper, 20.

[12] Regard ng part c pat on consent by nd v dua s and the requ rement to make use of an HREC where th s s unab e to be obta ned, see Nat ona Hea th and Med ca Research Counc , *National Statement on Ethical Conduct in Human Research*, updated 2018, <https://www.nhmrc.gov.au/about-us/pub cat ons/nat ona - statement-eth ca -conduct-human-research-2007-updated-2018>.

ethical standard for human research could be mandated by the Exposure Draft in circumstances where the research, if conducted through the university system, would require such review. This could include mandatory review by a HREC or equivalent. The failure to do so would put individuals at risk of unethical research, and create a significant disparity between commercial entities and research institutions with a strong ethical framework, such as universities. In the absence of HREC review, we are not sure how data custodians can be in a position to assess the ethical implications of a project. In many cases we assume they would not be experienced in conducting such reviews.

Accountability for decisions

17. In relation to research in the public interest, the optional nature of data sharing under the Exposure Draft means that improvements in data sharing are not guaranteed with its implementation. The National Data Commissioner does not have powers to compel data sharing in certain circumstances and similarly the Exposure Draft does not provide for merits review of data sharing decisions (whether favourable or otherwise). Decisions by data custodians to accept or reject proposed data sharing arrangements should be transparently reported, including reasons supporting that decision, with the ability of requesting parties to seek review, perhaps via pathways to the Office of the National Data Commissioner (ONDC).

Exclusivity

18. We also note that there is nothing in the Exposure Draft to prevent data users from requesting - and potentially being given - exclusive access to data. This is more likely to be a feature of requests for data for the purposes of commercial research and development than for, say, university-based research. We imagine that an argument could potentially be made by motivated data entities that exclusivity is in the public interest, suggesting that commercial actors may invest less in research and development if data is not made exclusively available to them.

19. However, 'locking up' data in exclusivity arrangements would be in clear contradiction of the intent of the Productivity Commission report behind the Exposure Draft and would raise ethical concerns about the privatisation of public data. Exclusivity is not currently prohibited in the Exposure Draft. At the very least, we would suggest that an extremely high bar of public interest would need to be cleared for any entity seeking exclusive access to data. We find it hard to imagine that exclusivity would be appropriate, but appreciate that we may not be able to foresee all circumstances. It may be that an additional hurdle, such as, for example, a special certificate from the ONDC, could be required before exclusive access would be contemplated.

Improved service provision in Australia: will this benefit be achieved?

20. A modern data-sharing scheme would arguably address improved public services through secure and meaningful data exchange, an intended outcome of the Exposure Draft.[13] This is compared to the current context in Australia, in which an individual can currently expect to engage in a great deal of lengthy government

[13] For examp e, a med a re ease by the nter m Nat ona Data Comm ss oner expresses a key outcome of the B as "The Austra an Government s work ng to deve op better, more seam ess serv ces to the pub c. To do th s, we need to modern se how we manage the wea th of nformat on supp ed by Austra ans to var ous government agenc es." Off ce of the Nat ona Data Comm ss oner, "Modern s ng government data shar ng", Med a Re ease, 14 September 2020: <https://www.datacomm ss oner.gov.au/med a-hub/modern s ng-government-data-shar ng>.

administration steps following a single life event such as a change of name, or the death of next of kin.[14]

21. However, "one-stop shop" service provision is unlikely to result from the implementation of the Exposure Draft for a number of reasons:
    (a) the receipt of data by an agency providing services is optional - a "tell us once" approach, such as the pre-population of government forms is unlikely to be achieved without mandatory sharing between certain key service provision agencies;
    (b) the scheme is limited with respect to state agencies, who will not be data custodians under the Exposure Draft. but which provide a great number of the services impacting the daily lives of most people, including education, transport, health care, aged care, and fair trading;
    (c) the proposed data sharing scheme is designed around decentralised data custodianship, without capacity for a single source of truth for key personal data;
    (d) no obvious provision is made for appropriate capability building and resourcing of agencies other than the ONDC, which are tasked with providing and receiving data; and
    (e) it is unrealistic to expect that enactment of this legislation will itself resolve a risk-averse information sharing culture in the public sector.

22. The decentralised and voluntary accreditation-centric design of the Exposure Draft, misses an important opportunity to equip appropriate Australian agencies with the ability to access single-source-of-truth data for the purpose of genuinely seamless e-government service provision. Data redundancies are not addressed, but are potentially further proliferated as a greater number of entities foreseeably share and store the same data, including potentially inaccurate data.

23. This absence of clear material benefit to members of the public, when balanced against the privacy risks amplified through the Exposure Draft, through the potential sharing of personal information, disproportionately disfavours individuals in a risk/benefit analysis of the scheme as a whole.

24. It is submitted that the design of the scheme should be reassessed with a view to planning an intentional digital integration infrastructure with an increased focus on efficiency and consumer benefit at its core, subject also to improved privacy and safeguards considerations as discussed further in this submission. Some international examples of modern e-government provision include Estonia, Singapore and Sweden.[15] We refrain, however, from engaging in detailed analysis of those schemes or whether they would be suitable models, because the Exposure Draft is not based on this kind of approach.

Scope expansion risk

25. The Exposure Draft is shaped around three "intentionally broad" purposes: (i) delivery of government services; (ii) to inform government policy and programs; and (iii) for research and development, and **precludes** data sharing for the purpose of

---

[14] See, for examp e, the engthy check st ava ab e at <https://www.serv cesaustra a.gov.au/s tes/defau t/f es/who-to-not fy-check st.pdf>, wh ch sts a number of government agenc es that must be not f ed separate y.

[15] Un ted Nat ons Department of Econom c and Soc a Affa rs, *E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development (with addendum on COVID-19 Response* <https://pub cadm n strat on.un.org/egovkb/Porta s/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Fu %20Report).pdf>.

enforcement, compliance, and assurance purposes; and any purpose that is related to or prejudices national security.[16]

26. There is some risk, however, that a broad interpretation of the above purposes could result in an unacceptable expansion in relation to collateral and secondary data use. For example, while Australian Privacy Principle (APP) 7 creates some protections for the public against direct marketing, there are insufficient controls in the scheme design to protect against personal data being used for market research purposes more generally. It is unlikely that this use, and potentially any commercial use of personal data, would be supported by the Australian public; it follows that the commercial use of personal data under this scheme should be carefully limited. This view is also reflected in the commissioned 2020 Privacy Impact Assessment, which expressed concerns regarding adequacy of present controls to prevent collateral or expanded use of data.[17]

27. It is therefore submitted that, as a minimum, the following additional controls be considered:
    a) that commercial entities applying for accreditation be wholly or substantially involved in the business of research or Australian government service provision to better align potential outcomes with the intent of the Exposure Draft, to better align with the apparent intent of the original Productivity Commission Report;
    b) the Exposure Draft should restrict commercial use of data, at least in relation to any personal information;
    c) if limited commercial use of the data is nevertheless permitted, the threshold to demonstrate the public benefit must be set an appropriately high level and some standardisation regarding the definition of the public interest should be attempted; and
    d) Data Sharing Agreements must be specific with respect to the intended use of data to help protect against collateral use and disclosure of data, and must also be appropriately overseen and enforced (see further below).

Response to proposed accreditation framework

28. Anticipated accredited entities under this Exposure Draft are expected to include, but not necessarily be limited to, government, business, academia, think tanks, and not-for-profit sectors.[18] The framework for this accreditation will be established through Rules from the minister. Key safeguards described in the draft Exposure Draft include the independence and oversight of the ONDC, two-step accreditation, the use of Data Sharing Agreements, public registers of scheme data, and Commissioner enforcement powers. Other safeguards referenced include using de-identified data "where possible", use of privacy impact assessments and "other safeguards outlined by the data sharing principles can be dialled up to protect privacy".[19] Privacy considerations are discussed below.

29. The Accreditation Framework Discussion Paper asks **Question 11** with respect to whether the timeframes for accreditation seem unreasonable. In response, we submit that this period is too long, particularly for an initial accreditation follow-up.

---

[16] Consu tat on Paper 2020, 14

[17] Informat on Integr ty So ut ons, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020* 6 September 2020 (here nafter, 2020 Pr vacy Impact Assessment).

[18] Consu tat on Paper, 13.

[19] Consu tat on Paper, 21.

30. With respect to **Question 12**, whether it is appropriate to notify parties to Data Sharing Agreements of an accredited entity's suspension, it is proposed that it should not only be appropriate but mandatory so that data custodians can suspend data sharing activities in a timely manner. The effect of not having this notification would practically create an onus on a data custodian to perpetually ensure accreditation of a counterparty, which may not be reasonably practical.

31. With respect to **Question 13**, regarding information that must, or must not be made publicly available though the registers of accredited entities, we draw your attention to paragraph 39 of this submission, which calls for greater detail to be included in s 116 of the Exposure Draft.

32. Some further concerns that should be further addressed in the legislation or the Rules include:

    a) Further guidelines in support of s 30 of the Exposure Draft with respect to types of entity changes that would cause an accredited agency to notify the Commissioner;
    b) Additional support to smaller entities, such as not-for-profits, seeking low-risk data (other than personal information): the bureaucratic processes being established are likely to disproportionately suit certain kinds of data applicants, such as large research institutions, but also commercial actors;
    c) Measures to ensure that particular entities are not discriminated against for reasons other than system safeguards: The system appears to establish no obligation on the part of data custodians to treat accredited entities equally; and
    d) minimum standards for data encryption and the requirement for accredited agencies to have appropriate cybersecurity policies and data breach response processes.

Comment on Scheme Transparency

Additional detail at the legislative level

33. The scheme involves principles-based legislation supplemented by:
    - Regulations (made by Governor-General): prescribing when sharing is excluded;
    - Rules (made by Minister): establishing the accreditation framework;
    - Data codes (made by the ONDC); and
    - Guidelines/Guidance: published by the ONDC, that data custodians and accredited entities must have regard to.

34. This approach creates some flexibility to enable rapid response to changes in technology and other circumstances, however it also exposes potential gaps in the safeguards by allowing for excessive ambiguity as follows:
    a) although consistency with the data sharing principles is required (s 13), the data sharing principles are so generally expressed (referring to 'appropriate' persons, and projects etc) that consistency would be very simple to express, even if not well-founded. As noted, it is not at all clear that decisions made by a department whether data-sharing is consistent with those principles can be challenged effectively;
    b) insufficient definitions or parameters for key terms required to understand the principles in s 16; and

c) deferral of key scheme details to the Ministerial Rules, including the details of the accreditation framework itself (per s 74).

35. It is submitted that more detail should be prescribed at the legislative level, or at least in publicly available guidelines, including but not limited to:
    a) further definition and guidance, for example (i) in the s 16 principles for "Appropriate persons", controlled environment", and "appropriate protections; (ii) s 30 reference to "any event or change in circumstances"; and (iii) the "public interest"; and
    b) including a requirement to conduct ongoing accreditation assurance activities,[20] and powers for the ONDC to respond to non-compliance, such as by restricting accreditation.

36. The Consultation Paper notes that "The data sharing agreements – which will capture how all of the safeguards are applied – will be published on a public register. This transparency promotes accountability across the scheme, putting the onus on decision-makers to demonstrate to the public how the public interest is served by the sharing".[21] This implies that the public can expect that data sharing agreements will be published in full to enable such assessment; the ONDC is requested to provide confirmation in this regard.

37. The legislative requirements for public registers in s 116 of the Exposure Draft should be expanded beyond names of accredited entities and mandatory agreement terms to also include a description of any personal information captured in any data sharing arrangement. This should permit members of the public to assess where their information may be held so that they may potentially exercise their privacy rights, not least APPs 12 and 13.

Legislation title

38. While not a control in itself, we also suggest that the title of the Exposure Draft, referencing "Data Availability and Transparency", is somewhat misleading - a cynical view may be that this title change is made to allay public alarm at the previous title "Data Sharing and Release". Data availability and transparency also implies freedom of information, which the proposed scheme is intended to complement, but also be intentionally independent from.

39. The Exposure Draft is in fact about data sharing and release, including the sharing and release of personal information, and should be appropriately titled for the benefit of the public.

Privacy and Ethical Concerns

40. With respect to any process that involves the sharing of personal information, it is worth noting that Australian legislation does not provide for a tort for loss of privacy, ownership of personal data, or even a general right to privacy. A breach event of personal information may be subject to some repercussion for a breaching entity, but provides for minimal or no remedy for a person whose information has been inappropriately released, particularly where that information is breached 'into the wild'. As stated above, the risk implications of the Exposure Draft must be carefully

[20] See a so 2020 Pr vacy Impact Assessment Recommendat on 2.

[21] Consu tat on Paper, 18.

balanced against perceived benefits, and appropriate reform and harmonisation of privacy safeguards addressed in advance.[22]

Privacy legislation reform

41. The proposed scheme relies on pre-existing privacy legislation in Australia to act as a key safeguard. The adequacy of this safeguard should be understood in the context of the ACCC's Digital Platforms Inquiry Final Report[23] which recommended a number of specific changes to strengthen Australian's privacy landscape, including, fundamentally, strengthening the definition of personal information (Recommendation 16(a)). It also recommends introducing a statutory tort for serious invasions of privacy (Recommendation 19). The Issues Paper for this review has only just been published, and changes to address concerns about Australia's privacy rights are some time away from being enacted.

42. Certain recommendations by the ACCC relate directly to the operation of the scheme proposed by the Exposure Draft including:
    (a) strengthening collection notice requirements (Recommendation 16(b));
    (b) strengthening consent requirements ("Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed… different purposes of data collection, use or disclosure must not be bundled") (Recommendation 16(c));
    (c) Requiring APP entities to erase personal information (Recommendation 16(e)); and
    (d) Broad reform of Australian privacy law (Recommendation 17).[24]

43. The potential impact of the introduction of this legislative scheme should be considered against these recommendations. For example, s 16(b) of the Exposure Draft provides that "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". However, without further guidance on how "unreasonable or impracticable" will be interpreted, this exception to consent is potentially very broad (such as impractically demonstrated through bulk data affecting a large class of people) and results in decreasing the risk mitigation effect of s 16(b).

44. The IIS Privacy Impact Assessment states as follows: "IIS notes that poor practice with privacy notices and privacy collection statements results from the conflation by entities of the requirements of APP 1 and APP 5. The Information Commissioner has flagged this as an issue in recent times… many of the usual collection (APP 5) notices would not provide either sufficient or clear information to allow individuals to make informed choices about data sharing for government service."[25]

---

[22] By contrast, the nformat on of data ent t es s we protected through the exc us on n the eg s at on of nformat on where the shar ng wou d nfr nge IP r ghts, where the shar ng wou d nfr nge nternat ona agreements and where the nformat on s commerc a . There s some concern that the key benef c ar es under the B are a so the best protected.

[23] Austra an Compet t on & Consumer Comm ss on, *Digital Platforms Inquiry: Final Report*, June 2019, https://www.accc.gov.au/system/f es/D g ta %20p atforms%20 nqu ry%20-%20f na %20report.pdf> (here nafter, ACCC Report 2019).

[24] "The ACCC cons ders that the Pr vacy Act needs reform n order to ensure consumers are adequate y nformed, empowered and protected, as to how the r data s be ng used and co ected." ACCC Report 2019, 3.

[25] 2020 Pr vacy Impact Assessment, 43.

45. It is submitted that the scheme proposed by the Exposure Draft may have the effect of further weakening these existing elements of (and practices in) Australian privacy law at a time when it is recognised that fundamental strengthening is required. Accordingly, any changes that have the potential to impact collection and use of data, and related informed consent, should follow privacy law reform, and not occur ahead of it. [26]

46. It is both notable and concerning that in the ONDC webinar of 14 October 2020, the Interim Commissioner emphasised the separateness of the data sharing scheme from privacy law. It is submitted that any scheme which has the potential to negatively impact the privacy rights of Australians be closely considered relative to privacy legislation, and not as distinct from it.

47. Fundamentally, greater caution should be exercised to ensure that there is no erosion of the principle in Australian privacy legislation by the proposed legislation. As a general default, individuals should be fully informed, and consent freely given, before their personal information is shared with any party. This is all the more important in the context of public data, where individuals cannot choose whether or not to provide data to the government.

Sharing scheme controls and exclusions

48. The following additional excluded activities related to data sharing should be considered for inclusion in the Exposure Draft:
    (a) Personal information that is mandatorily collected by a data custodian should be classed as information collected without consent for secondary use (consistent with the EU's *General Data Protection Regulation* ('GDPR') Recital 42);
    (b) Data that has been de-identified must not be re-identified by a scheme entity;[27] and
    (c) Data must not be used for the purpose of profiling or producing an automated decision such as insurance, credit, or recruiting decision (consistent with GDPR Recital 71).

49. We also express concern over the scheme being subject to a "principles-based" risk management framework which controls "can be 'dialled up' or 'dialled down' as necessary to manage risks and provide safe data sharing".[28] While this may provide potentially positive flexibility, the lack of mandatory minimum controls is also troubling. As stated in the 2020 Privacy Impact Assessment[29], this increases the need for the ONDC to maintain close oversight of the operation of the scheme under Data Sharing Agreements, including regular audits conducted by the ONDC.

---

[26] :... there's another techn ca ang e from a pr vacy aw perspect ve, around opt-out, for those of you that come from that sort of f e d d sc p ne. Peop e ta k about opt-out around the genera data protect on r ght, that's n the European Un on. So our eg s at on sn't about do ng deep reform of pr vacy aw, n fact, there's a separate rev ew com ng up about that. So those are quest ons that no doubt w be contemp ated n that." Off ce of the Nat ona Data Comm ss oner, Data Ava ab ty and Transparency B web nar, 14 October 2020 <https://www.datacomm ss oner.gov.au/exposure-draft/dat-web nar>.

[27] Not ng that research has shown that "99.98% of Amer cans wou d be correct y re- dent f ed n any data set us ng 15 demograph c attr butes": Rocher, L, Hendr ckx, JM & de Montjoye, Y-A, "Est mat ng the success of re dent f cat ons n ncomp ete datasets us ng generat ve mode s", *Nature Communications*, 10 (2019), <https://www.nature.com/art c es/s41467-019-10933-3>.

[28] Consu tat on Paper, 15.

[29] 2020 Pr vacy Impact Assessment, 59.

50. Similarly, the Consultation Paper expresses that safeguards can be "dialled up to protect privacy data" and that custodians may be able to add additional terms to Data Sharing Agreements but also states that "the National Data Commissioner may not be able to enforce them".[30] So-called "dialling up" of safeguards are only meaningful if they are enforceable, other than through contract, and this foreseeable compliance gap must be addressed in the Exposure Draft by giving adequate powers to the National Data Commissioner.

Expand complaint and reporting mechanisms

51. The Exposure Draft at s 75 includes a complaint mechanism for data scheme entities to complain to the ONDC, however it does not include any similar provision for aggrieved parties who are not data scheme entities. This should be addressed and the complaint mechanism expanded to include parties such as individuals and other organisations who may be impacted by sharing activities but not a data scheme entity. It should not be assumed that all non-data entity complaints would fall within the jurisdiction of the Office of the Australian Information Commissioner (OAIC) and this gap should be appropriately addressed.

52. In addition, s 75 of the Exposure Draft should be amended to provide not only an optional complaint mechanism regarding data scheme breaches, but rather a **mandatory reporting requirement** with respect to suspected breaches, including self-reporting. This measure would elevate the expectation of compliance with the proposed legislation and associated rules and agreements, and require entities to prioritise safe data sharing obligations over the maintenance of relationships with other data scheme entities.

Interaction with existing privacy framework

53. The Exposure Draft, particularly s 36, and the Accreditation Framework Consultation Paper indicates an intention for the ONDC to work in conjunction with the OAIC. However, particular attention is drawn to Recommendation 1 of the 2020 Privacy Impact Assessment which indicates that advice and assistance from the OAIC should be incorporated into the accreditation framework, particularly in regard to APP 1. The 2020 Privacy Impact Assessment recommends, as an example, that the development of privacy management plans for data sharing arrangements should be aligned to OAIC advice.[31]

54. Further controls should also be introduced to support alignment with privacy legislation, including but not limited to:
    a) making all elements of the data sharing scheme, in addition to ONDC templates and data sharing terms to be subject to OAIC consultation and advice;[32]
    b) requiring privacy impact assessment reports prior to commencement of any data sharing arrangements involving personal information, in accordance with OAIC advice;
    c) requiring third-party audits into data sharing arrangements involving personal information; and

[30] Consu tat on Paper, 15.

[31] 2020 Pr vacy Impact Assessment, 7.

[32] A so ref ected n the 2020 Pr vacy Impact Assessment, 29.

d) notification to the ONDC by the OAIC in the event of a data breach by a data scheme entity (not least to support risk-aligned priority audits of data sharing arrangements).

55. It is further requested that the ONDC provide clarity with respect to the intent and scope of s 22 of the draft Exposure Draft, which states that the authorised sharing (s 22(a)) or the the authorised collection or use (per s 22(b)), " does not contravene any law of the Commonwealth or of a State or Territory, whether enacted before or after the commencement of this Act." The intended breadth of this section is not immediately obvious from the text itself, nor is it addressed the Consultation Paper.

Provision for innovation and technological change

56. We note that there is some attempt in the Exposure Draft to future-proof the legislation in response to emerging technologies.[33] Nevertheless, the challenges created by rapid emergence technologies is not trivial – the Consultation Paper reference to the use of "facial verification technology" as a positive example of a data use case of government service provision[34] is alarming in the context of the Australia privacy landscape being overdue for reform, and given concerns expressed by many people and institutions, including the Australian Human Rights Commission, in relation to facial recognition technology.[35]

57. It is foreseeable that the broadly-described purpose of "research and development", in addition to ss 8(f) and (g) of the Exposure Draft, would permit large sets of Australian data available to be made available to various entities. As the Exposure Draft is currently presented, this could include sharing with private industry, for use for data analytics and machine learning.

58. On the one hand, this creates an opportunity to support beneficial technological development in these areas, but this also needs to be carefully weighed against other possible outcomes including monetisation of personal data and risks relating to algorithmic bias. There is a risk that public data will be shared in the expectation that it will lead to local investment in innovation, but with few actual benefits redounding to the Australian public. We do not believe that there is currently social licence and sufficient consent for use of personal data in this manner, and that social licence ought to be rigorously proven before sharing of such a kind is approved. This submission makes the argument that, at a minimum, the use of personal information data under this scheme in automated decision making be an excluded use, unless and until appropriate social licence is proven, and appropriate safeguards established.

59. Risk mitigation strategies beyond data anonymisation, including homomorphic encryption, should be considered as a data sharing prerequisite where data may be used for machine learning and other artificial intelligence research and development projects.

---

[33] See Exposure Draft s 113(2)(b)(v), wh ch states that the Comm ss oner may produce gu de nes for the purpose of pr nc p es and processes re at ng to "emerg ng techno og es".

[34] Consu tat on Paper, .

[35] ACCC Report 2019, 24.

Conclusion

60. There is a real concern that the scheme, as it appears to be established by the proposed legislation, will fail to achieve its stated goals, and yet at the same time it risks introducing a number of potential risks that are unlikely to be acceptable to the Australian public, and with few means for members of the Australian public to challenge decisions made and few methods of recourse.

61. In particular, there is considerable risk of further eroding already outdated Australian privacy controls. The proposed scheme, at least as it relates to personal information and information about people, involves inherent risk.[36] A great deal of this risk is borne by individuals who entrust the government with their data, and much of this information they are obliged to provide. It is therefore not unreasonable for the Australian public to expect both greater direct benefits from this scheme in exchange for the risks they will potentially face under this scheme - neither of which are appropriately accounted for in the text of the Exposure Draft or its planned implementation.

[36] 2020 Pr vacy Impact Assessment, 48. See a so n ABS n6: “Every data re ease carr es some r sk of d sc osure, so the benef ts of each re ease (.e. ts ut ty or usefu ness for research and stat st ca purposes) must substant a y outwe gh ts r sks and be c ear y understood”.