LAW BUILDING F8, UNSW SYDNEY NSW 2052 AUSTRALIA
T +61 (2) 9385 2254 | ABN 57 195 873 179 | CRICOS Provider Code 00098G

UNSW | UNSW IFCYBER | AUSCL | AUSTRALIAN SOCIETY FOR COMPUTERS & LAW | Allens Hub for technology, law & innovation

12 March 2021

The Senate Finance and Public Administration Legislation Committee
Submitted online: https://www.aph.gov.au/Parliamentary_Business/Committees/OnlineSubmission

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

About us

The **Allens Hub for Technology, Law and Innovation** ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

The **Australian Society for Computers and Law** ('AUSCL') is an interdisciplinary network of IT and Legal professionals and academics focussed on issues arising at the intersection of law, technology, and society. It is a registered Australian charity with a charter to advance education and advocacy. AUSCL was officially launched in July 2020 by its patron, the Hon. Justice Michael Kirby. The Society has a a proud history, with its member societies being established as early as 1982. AUSCL provides a forum for learned discussion and debate through its Policy Lab, Working Groups and Events Program attracting support and engagement across Australia and globally.

The **UNSW Institute for Cyber Security** is a multidisciplinary Institute which focuses on research, education, innovation and commercialisation that has 'real world impact'. The Institute has over 60 members across each of our faculties. We are ambitious (achieving international impact), scholarly, collaborative and inclusive (acknowledging that cyber security is a new and developing field and seeking opportunities to broaden our understandings of the field by welcoming a broad range of disciplines), entrepreneurial (seeking opportunities to empower academics to be creative), diverse (embracing multidisciplinary and working as thought leaders), and generous and supportive (helping to develop and mentor early career academics, recognising vulnerable groups in society).

About this Submission

We are grateful for this opportunity for consultation on the Data Availability and Transparency Bill (the Bill) which stands, alongside consultation throughout the Bill's development process, as an excellent example of government engagement. The Bill contains some commendable transparency measures such as the public availability of Data Sharing Agreements ('DSA'). It also contains improvements on the Exposure Draft, including in relation to matters raised in the earlier Allens Hub submission.

This submission is not intended as a comprehensive response to all the issues raised by the Bill, but rather focuses on topics on which our research can shed light. We thus limit our submission to the following propositions:

- **Objects of Bill.** A reference to accountability should be inserted into the Bill's Objects. This would strengthen the functionality of existing safeguards and ensure accountability plays a central interpretive role. In addition, the Objects clause should note that consent remains the primary basis for sharing personal information.
- **Private Sector Research and Research Ethics.** Private sector organisations seeking to use data for research should be required to prove a rigorous ethics process.
- **New Data Attributes.** Interaction with the review of the *Privacy Act 1988* definition of "personal information" should be managed.
- **International Data Sharing.** Accreditation of foreign entities should be subject to proof that the relevant foreign country has a comparable privacy law framework.
- **Transparency.** Transparency measures should be put in place with respect to the operation of Clause 15(4). Further, there should be ongoing transparency about flaws in the data protections applied in clause 16(7).
- **Interaction with Other Legislation**. Details of interaction with other legislation should be published, ideally within the Bill. Consistent terminology across legislation should be a long term goal.
- **Handling of Data After Project Completion.** Requirements on termination of a project or suspension of an accredited entity, such as data deletion, should be specified.
- **Accountability.** Transparency and accountability should be enhanced through additional language in privacy policies and a *requirement* for data scheme entities to raise complaints. Data subjects should also be encouraged to make complaints.
- **Consent.** The threshold for circumstances when it is unreasonable or impracticable to seek consent should be incorporated as part of the ethics function governed by the National Data Advisory Council.
- **Data Sharing Controls and Environment.** There should be minimum standards for security and data protection practices, including training.
- **Guidelines to Address Data Procurement.** The scope of guidelines be amended to cover data procurement and pre-processing as well as the operation of clause 15(4).

Objects of Bill

The objects of the Bill, listed in clause 3, fail to include mention of an important objective – accountability. Accountability is a fundamental value requiring government to answer for its actions and decisions, and encompasses lawfulness, fairness, transparency, rationality and, arguably, data protection.[1] In particular, accountability is the *reason why* transparency in government is important – disclosure is not simply to satisfy public curiosity but to ensure the government remains answerable to the public.[2] Further, accountability to the public, including through oversight, is the only basis on which "confidence", referenced in cl 3(d), ought to be achieved, particularly given that the regime in the Bill can bypass informed consent. Including a reference to accountability in the objects not only explains many existing provisions (eg Ch 5, Pt 6.2), but will help ensure the legislation is interpreted in

[1] Janina Boughey and Greg Weeks, 'Government Accountability as a "Constitutional Value"' in Rosalind Dixon (ed), *Australian Constitutional Values* (Hart Publishing, 2018) 99; RIchard Mulgan, *Holding Power to Account: Accountability in Modern Democracies* (Palgrave, 2003) ('*Holding Power to Account*').

[2] Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'The Rule of Law and Automation of Government Decision-Making' (2019) 82(3) *The Modern Law Review* 425; Monika Zalnieriute, Lyria Bennett Moses and George Williams, 'Rule of Law by Design?' [2021] *Tulane Law Review* Forthcoming.

light of this crucial rule of law value. A reference to accountability also provides a useful framework for considering the adequacy and independence of governance and oversight arrangements in the Bill.

To the extent the Bill facilitates use and disclosure of personal information without consent, it is important to emphasise that this is an exception to the usual rule. A provision in the Objects would help emphasise this and assist accountability, with words to the effect:

> "3(f) noting informed consent is the expected basis for access to personal information for purposes other than those for which it was collected, to provide a mechanism for sharing personal information without the consent of the person to whom the information relates, but only where it is unreasonable or impracticable to obtain consent, and only in the circumstances and for the purposes prescribed in the Act. "

Private Sector Research and Research Ethics

"Data sharing purposes" include "research and development" (cl 15(1)(c)). We recognise that data analytics can be useful in private sector research, particularly with access to high volumes of high quality data.

Research involving humans (including through analysis of personal data) has long been an area of ethical concern. As an example, an Australian survey conducted by the Data to Decisions Cooperative Research Centre found that support for government use of bulk social media data to train analytic tools was low, and far lower than support for uses related more directly to national security and law enforcement activities (such as to prevent or respond to terrorism and crime).[3] Having one's data used in *research* in the absence of consent is sensitive, arguably more so than use for policy or service delivery purposes. However, even when these are bundled together in one question, only 9% of Australians are "very comfortable" with their personal information being used by government in these ways.[4]

It is for this reason that universities have human research ethics committees which, while far from perfect, carefully consider the ethical balance involved in human subject research. Such committees are particularly cautious where consent is impossible or impracticable (as in the case of deception studies or studies involving existing data sets). Ethics committees are not typically used in the private sector – thus Facebook is able to do A – B testing on everything from the impact of news feeds on mood to measuring the impact of voting prompts – without consent and without any consideration of the ethics or impact of the research.[5] In the context of the Bill, the private sector will potentially take "research" as including market research, using personal data (without consent) for differential pricing and/or consumer manipulation. This is related to questions as to how the Bill's public interest test will be applied and, in particular, the consistency and rigour of assessment against that test, as well as the details of guidance on application of the test.

In the Bill, "any applicable processes relating to ethics" are one "project principle" to be considered alongside other principles viewed as a whole (cl 16). In a university, it would be unacceptable to contend that obtaining ethics approval was simply one factor among many to be considered in deciding whether a project can go ahead based on overall risk assessment and mitigation. The same should apply here. Where private sector organisations partner with universities in research, university

---

[3] Janet Chan et al, Survey Report (Report D), Project B4: Using 'Open Source' Data and Information for Defence, National Security and Law Enforcement (31 August 2018), available on request.

[4] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2020 (September 2020).

[5] Robinson Meyer, 'Everything we know about Facebook's secret mood manipulation experiment' *The Atlantic* (28 June 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/; Zoe Corbyn, Facebook experiment boosts US voter turnout *Nature News* (12 September 2012), https://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401.

ethics processes will apply, and this can be noted within the accreditation process. In other cases, independent ethics oversight arrangements can be certified as part of the accreditation process.

This can be achieved by a provision that makes having an ethics process in place mandatory whenever the data sharing purpose is that set out in cl 15(1)(c).

We also propose to add additional requirements to the data sharing agreement in cl 19 to incorporate ethics considerations, which echoes with the overarching data sharing principles:

- Add to cl 19(6)(c) – "complete ethics review for the data sharing purposes identified";
- Add to cl 19(7)(c) - "showing relevant ethics reviews have been completed and specifying whether there are any ethics concerns to share the data"

New Data Attributes

In cl 16(2), the Bill provides that the project principle includes (but is not limited to) the following elements:

(a) the sharing can reasonably be expected to serve the public interest;
(b) any applicable processes relating to ethics are observed;
(c) 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;
(d) the data custodian considers using an ADSP to perform data services in relation to the sharing.

The scope of the current definition of "personal information" in the Privacy Act 1988 does not adequately deal with personal attributes, leading to the increased risk of re-identification, either from technical data or by combining datasets (whether accessible to all or some persons). For example:

- data attributes captured from cameras or smart cameras, including skeleton points, location history, gait measure and data points, facial measurement can be reidentified through biometrics databases;
- data attributes captured from Cookies, Pixels, Tags or other online tracking technologies, including session ID, device ID, IP address or unique user identifiers can be reidentified by at least some parties;
- health history or general health data, may not identify a person but may be matched with other data to identify a person, including health data captured by new technology gadgets;
- transaction history or records, may be used for data matching or analytics to identify a person;
- location data captured by various apps, may be used for data matching or analytics to identify a person.

As the Privacy Act and the definition of "personal information" is currently under review, it will be a good opportunity for the Bill to address this issue as part of the ethics function governed by the National Data Advisory Council (cl 61(a)) and provide clarity in relation to the role of the National Data Advisory Council with regards to ethical considerations, for example, when dealing with new data attributes.

International Data Sharing

Under the Bill, foreign entities can be accredited for participation in the data sharing scheme where there is a binding international agreement. It is not clear how exactly the department will enforce the protection of data released offshore to a foreign entity in the case of a particular breach. During our roundtable with Philip Gould and his team on 30 October, it was suggested that if the foreign entity breached its agreement, then Australia would have recourse to send information about the breach to

authorities in the foreign jurisdiction for prosecution under its own laws. This can only work if the entity has data protection laws at least on par with those in Australia. The status of the data protection in the foreign country should be a determining factor in the accreditation of the foreign entity and approval of the agreement. If their domestic laws are insufficient, then no accreditation should be given, and no data should be shared. Subclauses 136(2) and (3) also raise concerns that if the breach occurs outside of Australia, then it may not contravene a civil penalty provision. Although Australia may not have jurisdiction to pursue matters which occur offshore, it is not clear why it is necessary to remove the civil penalty. Even so, given the non-application of penalties against foreign entities, it is questionable whether such entities would be compelled to comply with many of the safeguard mechanisms once accredited.

Transparency

The Bill provides for details of accredited entities and sharing projects to be made publicly available, such as in a register of data sharing agreements which register is intended as a key transparency measure to promote "integrity and trust in the scheme".[6] For the register to be meaningful in furthering this aim, its contents include adequate detail of matters necessary for the public to understand how the scheme is being used, by whom and for what purposes.

An important design feature of the scheme to enhance public trust is that sharing of data must be for specific data sharing purposes, with certain other purposes being excluded from the scope of these data sharing purposes. These "precluded purposes" (cl 15(2)-(3)) include an "enforcement related purpose" which includes investigating an offence, or an act detrimental to public revenue. However, the scope of precluded purposes is in turn limited by the carve-out in Cl 15(4), which may operate to permit sharing of data despite an enforcement link. Although in such cases there must be a data sharing purpose, the purpose involved is nevertheless permitted to relate to a precluded purpose in a "general way". Examples in the explanatory memorandum include data for national security research or to develop a policy or program to protect the public revenue. The boundary between these activities and direct enforcement is not easy to draw. For example, if data reveals that people living in a particular suburb are more likely to cheat on taxes, is a policy to subject the tax returns of people from that suburb to greater scrutiny a "policy or program to protect the public revenue" or does it involve "detecting acts or practices detrimental to the public revenue"? Whether the current wording in the legislation draws the line at an appropriate place can, however, be determined by monitoring the operation of the Act over time. To facilitate this, we propose:

1) That data codes contemplated in cl 126 include guidance as to the operation of Clause 15(4) (this can be added to the list after section 13); and
2) That the Register of data sharing agreements contemplated in cl 130 include an indication of whether clause 15(4) applies in the context of each data sharing agreement. This will allow for better tracking of how the distinction operates in practice over time.
3) That the data sharing agreement should include an additional requirement under cl 19(6)(a) to require parties to "identify and describe the primary purpose of the data sharing covered by this agreement" given the data sharing purposes listed in cl 15(1) are broad.

In addition, we propose an amendment to cl 16, inserting cl 16(8)(c) as follows:

> *Protections applied to the data under cl 16(7) are monitored over time, with any increased risk or breach associated with those protections, or protections of the same type, reported to the Commissioner and made public.*

[6] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 15.

Interaction with Other Legislation

Clause 22 permits authorised data to be shared in circumstances that would otherwise contravene an existing or future Commonwealth, State and Territory law. By permitting a legislative override, unintended consequences may occur as a result of interactions between this Bill and other pieces of legislation. As discussed during the round table, a review of potentially affected legislation has been conducted by the department. We believe that this should be made public, including to the Committee, so that omissions can be identified.

Data breaches captured under the existing Notifiable Data Breach (NDB) Scheme should also be considered in the context of this Bill. Updates may be required for the existing NDB Scheme.

Consideration should also be given to adopting consistent terminology across the Bill, existing privacy legislation, other legislation impacting on data governance, and NDB Scheme to limit uncertainty. For example, there are numerous terms used to describe the entity with control over and/or responsibility for data across legislation governing privacy, government agencies and even particular datasets.[7]

Handling of Data After Project Completion

We are concerned about the ultimate deletion of any shared data, or the revocation of data from an entity who may be abusing that privilege. It is noted that Item 4.8 of the Data Sharing Agreement (DSA) template released by the Office of the National Data Commissioner (ONDC) provides for entities to agree as to how data will be handled upon project completion. It is also noted that cl 19(15) of the Bill requires that the DSA expressly provides how data is dealt with when the agreement ends. However, neither expressly refers to the deletion of data. We submit that the default position should be to require deletion of the data at the end of the agreement or when the data is no longer needed for the agreement, unless otherwise agreed.

We also recommend that all agreements stipulate the exact data deletion time frame and circumstances and how that process will be verified. Thus we suggest cl 19(15) of the Bill be amended: "The agreement must provide for how scheme data covered by the agreement is to be dealt with when the agreement ends and when the data is no longer needed for the agreement, including a timeline for deletion of data and mechanisms to verify such deletion".

Accountability

Given the Bill does not *require* individual consent, we suggest that a clause be inserted to require notifications under future privacy policies reflect the possibility that data collected may be disclosed without consent under a DSA under this Bill. This clause should also stipulate that privacy policies expressly acknowledge that DSAs will be and are published, enabling individuals to view current and historic arrangements to share data. Transparency is the key to consent management. Government agencies need to update their privacy policy and collection statements to state clearly which data will be shared, with which agencies, under what circumstances, and how individual's choices impact already shared data. Full disclosure is an important factor for ensuring informed consent.

A data custodian of public sector data should only be authorised to share data if they can establish that data was collected by fair means following proper consent management rules in the first place. If the information was unsolicited, or if an individual's consent or opt-out was not properly captured, the data should not be shared to other entities.

---

[7] Lyria Bennett Moses, 'Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion' (2020_ 43 University of New South Wales Law Journal 615.

Only data scheme entities can raise a complaint under the current Bill. It is understood that individuals who suspect any misuse of their personal information will have access to recourse under the *Privacy Act*. Most Australians understand "misuse" as a purpose "other than the purpose or manner it was collected"[8] and may thus describe what the Bill enables as "misuse". Given this tension and general public distrust in data governance more broadly, it is imperative that any breaches of the Bill be reported to the NDC, that those affected by the scheme can make complaints directly under it, and that entities are held accountable. Enabling the entities participating in data sharing schemes to hold each other accountable will assist the scheme's transparency, and will help ensure the scheme is effective and warrants public confidence, but it is not sufficient. The primary enforcement mechanism (cl 88) establishes a discretionary complaint system. While a founded "reasonable belief" is an appropriated standard, this clause 88(1) should also be amended to require data scheme entities to raise a complaint where such a belief is held.

There should also be a right to complain under this section for those affected by the data sharing scheme, including data subjects and those who may have obligations to them.

Consent

The Bill does not provide definitions or examples on when it is unreasonable or impracticable to seek individuals' consent. The Privacy Act does not define this concept either. As different government agencies have different rules and policies in place, what may be unreasonable to one agency to seek consent may not be unreasonable to another. In our view, it is important to promote consistency across agencies where possible and provide clarity on when it is unreasonable and impracticable to seek consent, or at least provide certain threshold examples or guidelines.

Our recommendation is that those thresholds be incorporated as part of the ethics function governed by the National Data Advisory Council (s 61(a)). Consideration should also be given to inserting an additional point to cl 61(b), suggested wording: "identifying when it is unreasonable or impracticable to seek consent".

Data Sharing Controls and Environment

In cl 16 of the data sharing principles, the setting principle includes two elements: the data sharing means need to be appropriate for risk management, having regard to the type and sensitivity of the data, and reasonable security standards need to be applied when sharing data." (s16(5) & s16(6) of the Bill).

Data safety and data security are key concerns as technology evolves. It is critical for this bill to take this into account and address these concerns. We recommend that the Bill specify in cl 16 any minimum standards (security measures) for example, encryption for personal information. However, in recognition of advances in technology, the requirement should be drafted with technological neutrality in mind and perhaps with reference to industry standards/best practice.

Ongoing training and awareness should be taken into account. Given the sharing methods need to be compliant with appropriate risk management and data security standards, in our view, it is important for all public sector data custodians to employ the same standard of ongoing privacy and data protection training. This should also be addressed in the Bill.

[8] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey 2020 (September 2020) 36.

Guidelines to Address Data Procurement

The Bill applies to sharing of data that a Commonwealth body as data custodian "controls" and "has the right to deal with" (cl 11(2)). However, it does not address data procurement by Commonwealth bodies: that is, how, from whom, under what conditions and in what formats Commonwealth bodies obtain potentially shareable data in the first place. Similarly, the guidelines for which cll 27, 44 and 127 provide do not currently seem likely to address these matters. While this might appear to be out of scope for the legislation, there are many circumstances in which the terms and conditions under which a Commonwealth body procures data, and the format in which it is procured – from private sector bodies, for instance, or from bodies in other jurisdictions – could condition the sharing of data and the later handling and use of data by accredited users. Having data custodians consider how the conditions under which they originally obtain data might compromise that data's later sharing and use seems crucial to the risk mitigation purposes that the Bill seeks to achieve and its goal of facilitating responsible data sharing. Accordingly, we propose that the permissible scope of the guidelines set out cl 127(2)(b) be expanded so that "matters incidental to the data sharing scheme" expressly include data procurement and pre-processing.

Yours sincerely,

Lyria Bennett Moses, Fleur Johns, Lesley Land, David Vaile, Monika Zalnieriute (Allens Hub members, in alphabetical order)

Marina Yastreboff, Shengshi Zhao, Kim Nicholson and Tim de Sousa (for AUSCL)

Monica Whitty (for the UNSW Institute for Cyber Security)