THE ALLENS HUB
FOR TECHNOLOGY, LAW & INNOVATION

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

6 November 2020

Office of the National Data Commissioner
Via webform: https://www.datacommissioner.gov.au/exposure-draft/submission.

Data Availability and Transparency 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/. Our submissions reflect our views as researchers and are not an institutional position.

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'). Clearly a lot of work has been undertaken since the ideas and concepts of this regime were first floated.

Our 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:

- 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.
- Private sector organisations seeking to use data for research should be required to prove a rigorous ethics process before being granted accreditation.
- Accreditation of foreign entities should be subject to proof that the relevant foreign country has a comparable privacy law framework.
- A tiered roll out of the data scheme should be considered to ensure the mechanics of the Bill operate effectively and as expected.
- Clause 15(4) should be removed from the Bill. In the alternative, it should be expressly distinguished from other permissible purposes in the mandatory terms of the DSA to reflect its true relationship with enforcement related activities.
- Further, the definition of "enforcement related purpose" should be clarified.
- Details of interaction with other legislation should be published, ideally within the Bill.
- Requirements on termination of a project or suspension of an accredited entity should be specified.

- Transparency and accountability should be enhanced through additional language in privacy policies and a *requirement* for data scheme entities to raise complaints.
- The scope of guidelines be amended to cover data procurement and pre-processing.

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. Further, accountability to the public, including through oversight, is the only basis on which "public confidence", referenced in cl 3(d), ought to be achieved. 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 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.[2]

Private sector research

"Data sharing purposes" include "research and development" (cl 15(1)(c)). 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 extremely 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

[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] See, in particular, comments in Representative response on privacy issues in the DAT Bill 2020 (submission).

[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.

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, "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. The same should apply here. Where private sector organisations partner with universities in research, university 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.

International Data Sharing

Under the Bill, foreign entities can be accredited for participation in the data sharing scheme. It is not clear how exactly the department will enforce the protection of data released offshore to a foreign entity. During our roundtable 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 protections 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 122(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.

Roll Out of the Scheme

A tension exists between the free flow of data for research to inform projects, policy and other programmes for the benefit of society, and the protection of the individual or groups of individuals from harm. The complex considerations inherent exemplify the importance of ensuring established ethics processes, as drawn out above. Consideration should be given to rolling out the regime in two parts. For example, roll out could be tiered to universities as the receivers of information, as they already have strong ethics committees and other mechanisms to protect individuals. Should the programme work effectively, government bodies could then be accredited to receive information. This may also alleviate concerns regarding the point at which research for policy development actually becomes enforcement, either through specific information and granularity, or policy development which targets that cohort for enforcement. For instance, this may occur in relation to medical records for substance abuse or drug use, organised by suburb/local government area, age and gender, coupled with policy development that individuals fitting those criteria in those areas will be targeted by law enforcement. Thus, policy development could lead to enforcement. Clause 15(4) appears to anticipate and permit this scenario. It is thus recommended that cl 15(4) be omitted from the Bill. Allowing it to remain in the Bill runs the risk of individuals being reluctant to generate data about themselves, such as attending a medical practice for assistance with drugs/substance abuse.

Enforcement Related Purposes

The 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 the preclusion of investigative and enforcement purposes as permissible sharing purposes, as expressed in cl 15(2)-(3). Clause 15(4), however, permits data to be shared "in relation to matters that relate generally to compliance with or enforcement of laws". A dataset or rationale for proposed data usage may be cloaked as general but nevertheless be targeted or disproportionately affect certain persons so as to have an effect comparable to enforcement. For example, the aggregate represented in a dataset may produce a particular pattern as a result of its inherent characteristics, such as a geographical constraint.

Similarly, it will often be difficult practically to disentangle precluded "detect[ion]" and "monitoring" activities from permissible "delivery of government services". For example, delivery of government services requiring determination of entitlement or a need for reporting will often entail some degree of "monitoring" or "investigat[ive]" activity which could rise to the level of "enforcement". In view of this practical entanglement, and the importance of the enforcement exclusion to the maintenance of public trust and data custodian engagement, the Bill should be drafted to offer as clear guidance as is possible concerning how to distinguish permissible and impermissible data sharing purposes. With respect, we suggest that cl 15(4) unhelpfully muddies these waters. As mentioned above, we propose that it be deleted, and we also suggest that guidelines be developed for data custodians (pursuant to s 113 of the Bill) to aid and inform their distinguishing of permissible from impermissible data sharing purposes.

As an alternative to removing cl 15(4) from the scheme, as argued above, the scheme should at least ensure transparency as to when the sharing of data is permitted under this clause. This could be achieved by inserting a term into the DSA. Given Chapter 2 of the Bill does not require the "data sharing purpose" to be the purpose *of* the collecting entity, it is important to ensure that entities using the scheme for cl 15(4) purposes are published on the register. For example, a data custodian in the delivery of a government service may seek to have their dataset verified to ensure the service is being delivered correctly. Thus, data custodians could reasonably enter into sharing agreements with the *intention* of "correcting" a dataset that is being used by the custodian for general compliance purposes (cl 20(1)(b)). The other entities role might be to match data held by the entity against the custodian's dataset, then returning the "output" having only amended any specific discrepancies. The data sharing framework appears to permit this.The DSA Template in 'Item 2' incorporates check boxes to identify the purposes of the sharing project. These are listed as, "Delivery of government services; Government policy and programs; Research and development; Enforcement-related activities, and; Other". As cl 15(4) is currently phrased as "not an enforcement related purpose", projects relating to compliance or law enforcement generally would be marked for their relevance to one of the first three purposes. The result of this is to create an opacity regarding the true relationship of projects to enforcement related purposes.

Inserting a check box into the DSA for "Activities that relate generally to compliance with or enforcement of laws" would alleviate obscurities in its current form by appropriately distinguishing the circumstances of sharing. This would further promote public trust, encourage voluntary compliance, and strengthen recourse for ex post facto conduct through the agreed terms.

[6] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 6, 16.

Consideration should also be given by the Commissioner as to how and by whom the concept of generality is determined in this context. Given the potential for interpretation permitting whether data is ultimately shared, a note could be inserted into cl 15(4) stating that the Commissioner retains authority to determine whether a dataset falls within this clause.

Additionally, offences punishable by imprisonment are not included as a precluded reason under cl 15 of the Bill. Clause 15 covers pecuniary penalties, misconduct and even proceeds of crime, but fails to mention imprisonment. Thus, data sharing is prohibited where it is for an enforcement related purpose of 'detecting, investigating, prosecuting or punishing an offence or a contravention of a law punishable by a pecuniary penalty', but permissible where it relates to an offence punishable by imprisonment. The *Telecommunications Interception and Access Act 1979* (Cth) uses terms such as 'enforcement of the criminal law',[7] and 'enforcement of a law imposing a pecuniary penalty or protection of the public revenue'.[8] Based on this standard, the Bill lacks sufficient coverage of offences subject to punishment by imprisonment. To be clear, misconduct is not sufficient to bridge this gap and is more associated with the conduct of public servants, employees, politicians, and the professions. The phrasing of law enforcement purposes should be revised to ensure sufficient coverage for offences punishable by imprisonment.

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, however, we suggest the publication of the review for public verification. Further, the Bill should list those interactions. Existing legislation carries with it the intent of Parliament in affording those individual protections contained within separate Acts, yet without publication in the Bill, legislators will not be informed of these interactions when they assess the Data Availability and Transparency Bill 2020, making it more difficult for them to make informed decisions. There is also a risk of unduly burdening the work of future policymakers, where interactions remain unaccounted for or datasets similar to the COVIDSafe app are not afforded deserving protections.[9]

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 DSA template makes provision for entities to agree as to how data will be handled upon project completion and cl 18(1) item 14 of the Bill requires that the agreement contain information on what will happen to the data when the scheme ends, but is not specific to the deletion of data. 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 the Bill be amended to specifically address the following questions:

- What mechanisms will ensure the data will be deleted after its permitted use has been satisfied?
- Where an entity is de-accredited, what process will ensure that the data is deleted/revoked from the entity?

[7] *Telecommunications (Interception and Access) Act 1979* (Cth) s 178.

[8] *Telecommunications (Interception and Access) Act 1979* (Cth) s 179.

[9] Melanie Marks et al, "Representative response on privacy issues in the DAT Bill 2020" (6 November 2020) 5 [8].

- How will the process of suspension of an accredited entity work as far as data which has already been shared with it?
- Will the shared data be removed/revoked/deleted where an entity is suspended?[10]

Transparency and Accountability

Given the Bill does not *require* individual consent, we suggest that a clause be inserted to require future privacy policies reflect the possibility that data collected may be shared under a DSA under this Bill. This clause should also stipulate that privacy policies refer to the fact that DSA's will be/are published, enabling individuals to view current and historic arrangements to share data.

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"[11] 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 and that entities are held accountable. Ensuring data scheme entities hold each other accountable will be integral to the scheme's ultimate success and will help ensure the scheme is effective and builds public confidence. The primary enforcement mechanism (cl 75) establishes a discretionary complaint system. While a founded "reasonable belief" is an appropriated standard, this clause should be amended to require entities to raise a complaint where such a belief is held.

Guidelines to Address Data Procurement

The Bill applies to sharing of data that a Commonwealth body "controls" or "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 26, 43 and 113 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 113(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, Genna Churches, Fleur Johns, Lauren Parnaby (intern), Monika Zalnieriute (listed in alphabetical order)

[10] Cl 17(7).

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