Submission to the Senate Standing Committee on Finance and Public Administration

on the proposed

Data Availability and Transparency Bill 2020

12 March 2021

DIGITAL RIGHTS WATCH

Overview

We welcome the opportunity to submit comments to the Senate Committee on Finance and Public Administration on the draft of the *Data Availability and Transparency Bill 2020.*[1] Attached to this cover letter are the comments which we initially submitted to the Office of the National Data Commissioner's consultation on the exposure draft of the bill. We give full consent for these comments to be used in the Senate's inquiry as only minor changes have been made to the text.

We remain concerned that this bill is moving ahead in parallel to the review of the *Privacy Act 1988* which the Attorney-General's office is currently heading. The update to the act was recommended as a result of the ACCC Digital Platforms inquiry which made extensive recommendations regarding the need for a data protection framework and improved protections for privacy in order to protect Australians.[2] As such, we would recommend that this bill does not preclude any data protection and sharing standards that may be imposed by the Privacy Act update, as the draft currently attempts to do under Chapter 2: "The authorisation for data custodians to share data overrides other laws that would otherwise be contravened by the sharing, with some exceptions." We are further concerned about the edits that have been made to section 15(4), the re-wording of which has opened up the room for certain law enforcement/compliance activities to be included.

Given the topical overlap and potential for new privacy reforms to fundamentally impact the way data protection and ownership is viewed in Australian legislation, it should remain a priority to anticipate an updated *Privacy Act* before proceeding with any other fundamental changes to the way that personal data of Australians is treated. Some of our submissions relevant to the topics covered:

- Privacy Act review issues paper consultation, November 2020 https://digitalrightswatch.org.au/2020/11/27/submission-privacy-act-review-issues-paper/

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[3]

[1] The full text of the draft Bill: https://www.datacommissioner.gov.au/exposure-draft/dat
[2] The ACCC Digital platforms final report provides several recommendations on how to strengthen the rights of consumers in the digital space, including stronger privacy protections and data rights: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
[3] Learn more about our work on our website: https://digitalrightswatch.org.au/

General remarks

At Digital Rights Watch we have welcomed the findings of the ACCC Digital Platforms inquiry, published earlier this year, which have made extensive recommendations regarding the need for a data protection framework and improved protections for privacy in order to protect Australian consumers.[4] We strongly believe that the first actionable outcome(s) of the extensive ACCC inquiry must focus on updating the Australian privacy and data protection framework.

As the draft text stands, the *Data Availability and Transparency Bill 2020* (the Bill) threatens to further erode the limited protections enshrined in the existing Privacy Act. The Bill would make it easier for government agencies to share data containing personal information with each other, allowing any government entity to access any and all the information the government holds about an individual. The draft also permits the government to share data with accredited third parties and researchers. In absolute terms, the Bill almost constitutes an amendment of the Australian Privacy Principle 6 by redefining and altogether eliminating the limitations and protections the principle currently imposes on the data custodians.[5]

Research

Sharing data with researchers is an important part in building evidence-based public policy and benefits society at large. It is also an important part of data protection laws and discussions internationally; the European Union's General Data Protection Regulation (GDPR) provides for a research exemption under Article 89 for scientific and research purposes. However, access to personal data must be restricted and privacy of individuals must still be upheld and respected—even for research purposes.

In that spirit, under the GDPR such sharing is subject to safeguards, including: data minimization, technical and organizational measures, privacy by design and default, and pseudonymization/further processing.[6] Especially given the sensitive nature of the data held by government agencies, it is paramount that the Bill tightens up its provisions to ensure that the data is secure, individuals' privacy remains protected, and all data remains anonymized.

In 2017 the Productivity Commission recommended that ss 95 and 95A of the *Privacy Act* be reformed in order to expand the categories of data that can be shared for research purposes.[7] This approach would allow for appropriate sharing of data which includes personal information, while offering individuals protection under the *Privacy Act*, which is

[4] The ACCC Digital platforms final report provides several recommendations on how to strengthen the rights of consumers in the digital space, including stronger privacy protections and data rights: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
[5] A great analysis of this was written in October by Salinger Privacy: https://www.salingerprivacy.com.au/2020/10/22/data-sharing-dilemma/
[6] For more on GDPR rules for data processing: https://www.ncbi.nlm.nih.gov/books/NBK543521/
[7] Recommendation 6.16 in Productivity Commission, *Inquiry Report: Data Availability and Use,* No.. 82, 31. March 2017.

preferable to allowing personal information to be broadly shared under the proposed scheme in the draft Bill.

Consent

The Bill and explanatory documents further specify that any sharing of personal information is to be done with the consent of the individuals, unless it is "unreasonable or impracticable" to seek their consent. This completely fails to secure individuals' control of their data because a) the overwhelming majority of personal data shared with government agencies is legally mandatory to engage in those services, b) if a data custodian already owns a dataset (as all government agencies do by default), it will always be impractical to seek individual consent as it will always create an additional bureaucratic burden to the status quo. In this way, the Bill seems to glaze over the right of the individuals to give informed consent any number of times over the course of their lifetimes, in order to optimize data sharing across the accredited parties. This is an unacceptable proposition that threatens to fundamentally alter how personal data is treated and viewed in Australia.

There is a legal basis for the government to collect data on individuals as it allows the government to then provide critical services (taxes, pensions, drivers licenses). While the consent given for this type of data processing is mandatory, it is informed and understood by the individual. It's informed consent. In weakening that concept of consent, the draft Bill is eroding trust in government services (trust that has been repeatedly damaged)[8] and completely removing the notion of "informed" from consent as individuals will have no control or understanding of how their data is being handled, by which agency, or for what purposes.

We recognise that consent is not a panacea when it comes to empowering individual control over personal data. It is well understood that consent-based models are not an effective method of minimising harm for individuals where there is an imbalance of power, or when dealing with systems that may not fully understand. The reluctance to rely on consent as it is currently conceptualised is demonstrated in the terms of reference for the current review of the *Privacy Act* which includes consideration of the effectiveness of consent when managing personal information. Further to this, individuals are already bombarded by privacy messaging every time they engage with an app or service, and it is well established that people do not actively read terms of service, and generally suffer consent fatigue. In that way, the current draft of the Bill risks an over-reliance on consent as a green light for organisations to do whatever they wish with personal information. Robust privacy and data protection principles should be in place when sharing personal information, complimentary to the consent ostensibly obtained.

As it stands, the Bill would enshrine data sharing by default into public services. There would be no ability for individuals to opt out of having their data shared across the government and with third parties. Given the sensitive nature of data held by the government as well as the current weak privacy and data protection environment—this approach is hazardous.

[8] More on My Health Record from Australian Privacy Foundation: https://privacy.org.au/campaigns/myhr/

Recommendations

- **Prioritize the update of the *Privacy Act* (as currently underway by the Attorney-General) in order to modernize Australian data protection and privacy practices before proceeding with the DAT Bill.**
- **Restrict the access of accredited parties** from the single-application full access system proposed in the draft Bill to instead require individual authorizations. This will ensure that the security, integrity and purpose of the data use is respected. Datasets containing personal information must be reliably anonymised.
- **Define consent in line with international standards** as presented under the GDPR or California Consumer Privacy Act to be explicit in all cases. Ensure that it remains meaningful by eliminating the exception of "unreasonable or impracticable"—a test which has nothing to do with individuals' rights.
- **Maintain liability for data breaches, and ensure a resolution mechanism** is present for individuals who may want to seek redress if their data and privacy is compromised through the scheme.