New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

SUBMISSION TO THE SENATE FINANCE AND PUBLIC ADMINISTRATION COMMITTEES

DATA AVAILABILITY AND TRANSPARENCY BILL 2020 [PROVISIONS] AND DATA AVAILABILITY AND TRANSPARENCY (CONSEQUENTIAL AMENDMENTS) BILL 2020 [PROVISIONS]

12 March 2021

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Data Availability and Transparency (DAT) Bill 2020

The NSW Council for Civil Liberties (NSWNSWCCL) thanks the Senate Finance and Public Administration Committees for the opportunity to make a submission concerning its inquiry into the Data Availability and Transparency (DAT) Bill 2020.

Bill is fundamentally flawed and violates community expectations

The proposed sharing of 'public sector data' began with good intentions but in its current form is an unacceptable carve out from basic privacy principles and out of line with community expectations. It would fundamentally change the way personal information is handled in Australia.

NSWCCL comes to this Bill with a clear-eyed awareness of how government agencies and other organisations function in the real world. How they seek to increase their power, how drives for efficiency and data-driven results lead to unfairness and discrimination for ordinary people.

It must be remembered the 'robodebt' scheme, now recognised as unlawful and responsible for untold stress and suffering, was an automated data-matching scheme using data shared between two government agencies – Centrelink and the Australian Taxation Office (ATO).

This Bill ignores that real world experience and gives unjustified priority to a technocratic vision of 'improved service delivery'.

The Bill gives a green light for government agencies to share data with each other and the private sector exempt from the law (Australian Privacy Principle 6) which governs and limits how personal information is used and shared. This will have enormous consequences for individuals and is unnecessary to achieve the aims of delivering better government services, informing government programs and research.

The Privacy Act was initially enacted to regulate the activities of Commonwealth agencies – only later was it extended to the private sector. To exempt agencies from a key principle would fundamentally undermine the original purpose of the Act.

The latest Government survey of Australians' privacy concerns shows 84% consider it to be a **misuse** of their information when they supply it to an organisation for a specific purpose and it is then used for another purpose.[1]

Yet this is exactly what this Bill proposes to make possible.

[1] OAIC 2020 Australian Community Attitudes to Privacy Survey https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/

Is it really 'public sector' data?

The term public sector data gives the impression that data contemplated by the Bill is aggregated and de-identified statistics when it in fact includes personal information. The definition is extremely broad, encompassing "all data collected, created, or held by the Commonwealth, or on its behalf."

This includes detailed personal information we are compelled by law to disclose to government. Examples of this kind are information about our living arrangements, our relationships and our finances we disclose to Centrelink to receive a pension or to Immigration as part of a visa application for a partner.

Indeed, currently people are revealing the most intensely intimate parts of their lives to Border Force as they beg for permission to be allowed to *leave the country* to see a partner overseas.

The term also implies a view of data as a collective resource owned by the government, when it is better characterised as the personal information collected and held 'in trust' by the government, as a custodian, for specific purposes.

The data in question is therefore not adequately described by the term public sector data. It can be, and often will be, our personal information.

Why is it a threat to civil liberties?

Basic fairness and civil liberties are under threat when personal information we are compelled to disclose to get one outcome from a government agency is then spread silently, behind the scenes, to other agencies or private companies and is able to be used in surprising and unexpected ways when we engage with those other agencies for some other purpose.

The term 'transparency' in the Bill's name is the opposite of the outcome achieved – an absence of transparency on what happens to personal information inside government.

The Bill enables the 'robodebt' scenario in an accelerated form. It defines the permitted purposes of sharing broadly. Government services are "government activities that provide coordinated and structured advice, support, and services to individuals". Government policy and programs are to be "interpreted broadly" and "[d]ata shared under this purpose could help enable the discovery of trends and risks".

While the Bill does not allow sharing public sector data for law enforcement investigations and operations, it is silent on sharing to "help enable" the making of administrative decisions like whether one should be granted unemployment benefits or penalised for over-claiming, whether one is entitled to a pension or whether one should be allowed to leave the country or be granted a spouse visa.

The data sharing principles in the Bill require 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".

As the Senate Scrutiny of Bills Committee noted, the circumstances in which it will be 'unreasonable or impracticable' to seek a consent for sharing personal information is not defined.[2]

We suspect it will almost always be impracticable for a large government agency to get individual consent to sharing of data from large datasets. It is disingenuous to suggest information individuals provide to government agencies because it is mandatory means those individuals have consented to it being shared with other agencies and organisations.

Outside the narrow exclusions centred on law enforcement and national security, there is no purpose limitation, whilst the accreditation requirements for agencies are easily met.

Undermining the Privacy Act

The Privacy Act review launched by the Attorney-General's Department (Oct 2020) is focused on the ways in which our privacy protections should be strengthened given the new capacities of big data.

This Bill contradicts that purpose by exempting the most high-risk types of data sharing from the protections offered by the Privacy Act. It also undermines the original purpose of the Act at the same time another arm of government is ostensibly looking to strengthen the Act.

Recommendations

If the Bill is to proceed, there must be fundamental changes made.

- NSWCCL joins other privacy organisations in calling for the scope of the DAT Bill to exclude personal information. For other types of data there should be minimum standards for anonymisation.[3] In many cases of data matching, so-called anonymisation may be insufficient to protect privacy, as it often does not amount to permanent and irrevocable de-identification.
- We join other privacy professionals and organisations in noting the inherent conflict of interest in having the NDC as a regulator when the body's mandate is to encourage data sharing. The Office of the Australian Information Commissioner (OAIC) must have oversight and be funded to perform this job effectively.[4]
- There should be no carve-out from Australian Privacy Principle 6 which is the key protection for Australians on the use of their personal information once collected.
- The clear limits set out by APP 6 must not be replaced with imprecise concepts open to wide interpretation such as 'de-identify where possible'. Government agencies sharing data between them must adhere to at least the standards in the Privacy Act, not weaker standards.

[2] https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2021/PDF/d03_21.pdf?la=en&hash=6555B86B49E65FA6A0528E06C56AA58ADF5134FB

[3] Representative response on privacy issues in the Data Availability and Transparency Bill 2020', 6 November 2020 https://www.datacommissioner.gov.au/sites/default/files/2020-11/13-edsubmission-elevenm.pdf

[4] Ibid.

- The National Data Commissioner (NDC) should be made independent of the Minister.
- There should be no Ministerial power to require that an organisation be accredited.
- The NDC should have real independence guaranteed by tenure.
- Data sharing permitted purposes as defined in Clause 15 are too broad. There must be a purpose exclusion preventing personal information being shared without express consent and preventing it being used to make an administrative decision about a person which harms or disadvantages a person.
- There should be a prohibition on data sharing that would breach privacy promises made to individuals in the past, or would not come within reasonable expectations.
- There must be opportunity for redress under the Privacy Act

We urge the Government to take seriously the questions posed by the Scrutiny of Bills Committee and the Parliamentary Joint Committee on Human Rights.[5]

In particular we highlight the questions posed by the Committee on Human Rights at section 134 and urge these be substantively addressed by a significantly amended Bill:

- why the Australian Federal Police is not listed as an excluded entity under proposed subclause 11(3), noting that it is a law enforcement body;
- in what type of circumstances is it likely that data will be shared, or not shared, for a data sharing purpose (with examples provided as to what is, and is not, likely to be considered to be for 'the delivery of government services'; 'informing government policy and programs'; and 'research and development')
- what considerations would be considered relevant (and irrelevant) in an assessment of the 'public interest' for the purpose of proposed subclause 16(2), and why does the bill not specifically reference the need to consider the right to privacy;
- in what circumstances, and based on what factors, would it be considered unreasonable or impracticable (under proposed paragraph 16(2)(c)) to seek the consent of individuals whose personal information would be shared, and would the provision of any government service be contingent on the individual giving their consent to the proposed sharing of their data;
- whether and in what manner accredited entities would be subject to ongoing monitoring (or auditing) of their continued compliance with the data sharing scheme, and their suitability for continued accreditation
- why the scheme would not permit an individual to complain to the National Data Commissioner about a matter associated with the data sharing scheme, such as to report a suspected breach or data misuse, or to express concerns as to the sharing or use of their data in a specific context;
- noting the requirement that the sharing of personal information be minimised as far as possible without compromising the data sharing purpose, in what circumstances would the data sharing purpose be compromised by not sharing personal information;
- in what circumstances does the bill provide, and is it intended that the rules will provide, that a data sharing agreement may allow the accredited user to provide shared output data to a third party, and what protections apply to protect personal privacy in such circumstances; and
- why other, less rights restrictive alternatives would not be effective to achieve the intended objectives (such as amendments to individual pieces of legislation to invoke this data sharing

[5] Parliamentary Joint Committee on Human Rights – Human Rights Scrutiny Report – Report 2 of 2021

scheme which take into account the specific data to be shared and the specific circumstances in which it is appropriate to share such data).

Conclusion

The Bill as proposed is alarming in the context of Australia's absence of a statutory tort of privacy and absence of human right protections either in statute or constitution. It would also fatally undermine the foundational objectives of the Privacy Act. It must be fundamentally altered or abandoned.

This submission was prepared by Jonathan Gadir on behalf of the New South Wales Council for Civil Liberties.

Yours sincerely,

Michelle Falstein
Secretary
NSW Council for Civil Liberties