Senate Finance and Public Administration Committees
PO Box 6100
Parliament House
Canberra ACT 2600
fpa.sen@aph.gov.au

12 March 2021

Data Availability and Transparency Regime

This submission responds to the Committee's invitation to provide advice regarding the proposed Data Availability & Transparency regime under the *Data Availability and Transparency Bill* (Cth), *Data Availability and Transparency (Consequential Amendments) Bill* (Cth) and *Data Availability and Transparency Regulations*.

The submission is made by the Australian Privacy Foundation, the nation's preeminent civil society body concerned with privacy. Information about the Foundation is at privacy.org.au.

The proposed regime provides transparency about Australians but **not** about government and the partners of government. Despite reference to 'safes' and supervision by a statutory body it does not provide adequate safeguards, instead eroding an already weak data protection regime. It does not provide transparency about how governments (and the partners of those governments) are sharing and using information about people, in particular data that was collected on a mandatory basis. The Bills should accordingly be rejected.

The proposed regime has been promoted as fostering a range of social goods. There has been no indication of the achievability of those goods and whether they might more respectfully effected through mechanisms other than comprehensive, open-ended data sharing.

The proposed regime – in terms of statute, regulations and administrative implementation – is a fundamentally retrograde step regarding data protection in the absence of strengthening the *Privacy Act 1988* (Cth), which is the subject of a concurrent consultation, and a broader updating of Australian law regarding privacy, confidentiality and other data protection. The community's experience in recent years regrettably proves there is little reason to trust assurances that all will be well. The regime exacerbates ongoing balkanisation of privacy law, something that is of particular concern given the mandatory nature of much data collection, the incapacitation of watchdogs and the unavailability to Australians of specifics regarding what data is being shared.

Civil society has deep and substantive concerns regarding the potential for inappropriate commercialisation as a secondary consequence of gifting researchers with data that is then aggregated for commercial gain.

At a functional level it is inappropriate to have a Commissioner "as an independent statutory office holder" who is both charged with overseeing the data sharing scheme as "its regulator" and also acts as its "champion". This is a blatant conflict of interest and is particularly concerning given both balkanisation of the regulatory regime and the under-resourcing that has been recurrently highlighted by the Office of the Australian Information Commissioner.

Dr Bruce Baer Arnold
ViceChair
Australian Privacy Foundation

Data Availability and Transparency Regime

The proposed regime has weak legitimacy

There are community benefits in access to and analysis of information acquired by public sector bodies on a mandatory or other basis. Neither the Australian Privacy Foundation nor other civil society bodies such as Electronic Frontiers Australia are necessarily opposed to sharing.

It is axiomatic however that such sharing must be legitimate. Legitimacy involves collection, use and disposal of personal and other data within a coherent legal framework. It involves necessity and proportionality, in other words not data analysis on the basis that technology is available or data sharing on the basis that sharing is administratively convenient.

A failure on the part of policymakers to respect legitimacy – and more broadly respect the dignity of individuals who are potentially obligated by law to provide sensitive personal data on a mandatory basis in order to exercise rights or access services – leads to community distrust. It also fosters some of the data management problems that are recurrently evident in Australian public administration, including data breaches and misuse of data by employees/contractors.

Legitimacy requires transparency on the part of governments about data sharing activity, something that we address below. It also requires effective legal frameworks at the level of principle and practice.

The proposed regime erodes trust

The proposed regime represents a major change to Australian law at the national level and will presumably be emulated by state/territory Governments, with NSW for example consulting about extension of that state's data sharing framework. The regime is predicated on community trust, with the national Government relying on unsubstantiated assertions regarding benefits and weak assurances about safeguards in what amounts to a new privacy landscape.

That landscape is one in which government agencies will in practice be free to share personal, commercial and other information with each other. It is a landscape in which national agencies will be able to share with state/territory entities and with the private sector. It is a landscape in which trust is fundamental. It is, regrettably, a landscape in which the proponents of system weakening of privacy protection have recurrently acted in ways that bring trust into question.

The 2019 *Australian Election Study* from the Australian National University signalled that community satisfaction with democracy is at its lowest level since the constitutional crisis of the 1970s. Trust in government has reached its lowest level on record. Only 25% of Australians believe people in government can be trusted. 56% believe government is run for 'a few big interests'. Only 12% believe the government is run for 'all the people'. That disquiet is increasing, with for example a 27% decline since 2007 in stated satisfaction with how Australia's democracy is working. Overall trust in government has declined by nearly 20% since 2007; three quarters believe that people in government are looking after themselves.

It is unsurprising that Australians are wary about reiterated commitments to integrity and accountability when they encounter what critics have characterised as Taylorgate and note the incapacitation of key agencies such as the Australian National Audit Office through

funding restrictions after those agencies delivered bad news. The Office of the Australian Information Commissioner plays a key role in the proposed regime but as it has acknowledged is hobbled by ongoing under-resourcing. Its effectiveness is also inhibited by its corporate culture, which is inward-looking and lacks inhouse expertise (a concern when dealing with entities such as the Department of Home Affairs and Australian Bureau of Statistics). Civil society is particularly conscious that the OAIC was on 'death row' under Attorney-General George Brandis on the basis that it was both expensive and unnecessary. The Government has never given the OAIC the resources needed for meaningful privacy protection. Balkanisation of regulators will further erode the OAIC's capability and foster distrust.

The proposed regime provides uncertain benefits alongside a history of underperformance

In promoting the proposed regime Minister Stuart Robert, who has recurrently denied that there was a problem with 'RoboDebt' and refused to apologise for that initiative, stated on 14 September that the legislation will

> establish the foundations of a seamless and proactive experience of government services, by enshrining in legislation privacy and security safeguards that set out modern foundations for use of data across the Commonwealth government.

There has been no independent scrutiny of whether the objective of a 'proactive experience of government services' (jargon whose meaning is unclear) must be achieved through further balkanisation of the Commonwealth privacy regime, which now has multiple agencies with overlapping responsibilities and competing agendas and through erosion of the *Privacy Act 1988* (Cth) and protections that are agency/use specific. That statute is not fit for purpose. It is disquieting, albeit unsurprising, that the Act is now under review alongside establishment of the sharing regime.

There has been no independent evaluation of whether the objective could be better achieved through a more nuanced mechanism, in particular one that does not tell agencies to forget about restrictions on large-scale sharing for whatever purpose, just be trusted.

Given the history of underperformance in large-scale IT initiatives in Australian government (typically over budget, over deadline, underperforming and often cancelled) people are entitled to be wary about unsubstantiated claims of benefit.

Given the disregard of technical challenges within government, for example with the COVIDSafe App (critiqued by experts such as Teague and Leins) and CensusFail, people are also entitled to be wary about promises regarding performance, especially where ministers have sought to punish critics.

As a society in which there are legitimate expectations regarding government accountability we should not be using visions of data sharing to avoid the necessary rigorous review and redesign of administrative processes on an agency by agency basis. So far the various government grand initiatives have obfuscated rather than resulted in fundamental improvement.

The foundations of the proposed regime are weak, the superstructure is weaker

The Minister further states

> Australians rightly expect different parts of the government to talk to one another and this legislation will put in place the strong privacy and security foundations to make this happen.

The proposed regime does **not** provide the necessary 'strong privacy and security foundations'. Instead it embodies values of bureaucratic convenience that are antithetical to strong privacy protection.

The Government has **not** engaged with recommendations by successive law reform bodies calling for establishment of a statutory cause of action. Penalties for data breach are insufficient to ensure best practice.

The Office of the National Data Commissioner, in practice the advocate of data sharing alongside the Digital Transformation Agency (recurrently criticised for under-performance and marginalised in bureaucratic turf wars), states that the regime will

> help maximise the value of our public sector data, supporting our modern data-based society, driving innovation, and stimulating economic growth.

There is **no** evidence that the erosion of privacy protection will indeed support our 'modern data-based society'.

There is **no** evidence that the sharing within government and indeed sharing by government with non-government entities will substantively drive innovation. The mantra under successive ministers that 'new' equals better and 'digital' necessarily results in innovation has not been substantiated and is indeed questioned by authoritative analysts such as Robert J Gordon and Nicholas Carr. What's good for service providers such as Oracle and KPMG and IBM is not necessarily good for ordinary Australians.

Claims that sharing will stimulate economic growth are problematical. Sharing within government will of course benefit information technology solutions providers, with much of the revenue going offshore because of the shape of the IT services sector and many agencies continuing to be locked in to incumbent service providers rather than being 'agile', to use some bureaucratic jargon.

Observers who watched the UK care.data debacle – the abortive UK government initiative to cash in the remaining 'family silver' by selling population-scale health data to insurers and life sciences enterprises – might wonder whether the plan to 'maximise the value of our public sector data' is a matter of getting ready to sell information about most Australians.

Such a sale under the sharing regime is of concern for two reasons. The first, obvious, is that Australians dealing with governments typically have no choice. They are often legally obligated to provide data and to ensure the data is correct. They are increasingly forced to provide that data through portals such as MyGov that are badly designed, badly supported and coercive. It is, at best, naïve for government representatives to state that if you don't want benefits you don't need to use those portals and you don't need to share your private lives with government. Benefits are in fact entitlements rather than rewards.

People who will be treated as data subjects under the proposed regime will not have an opportunity to opt out. They will **not** be informed that data concerning them is being shared within government and across governments and with non-government entities. They will have to assume that data is going to be shared and will have to trust that data will not be misused. They will have no scope under the regime to deal with misuse. They will have to trust that everyone performs well. Experience with the egregiously punitive approach taken by the Government regarding RoboDebt suggests that trust is misplaced. Damning judgments such as *Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs v PDWL* [2020] FCA 1354 also suggest that trust is misplaced.

Submissions to the National Data Commissioner's consultation highlighted a range of concerns such as privacy creep, ie resounding statements by ministers about strong protection for privacy followed by ongoing exceptions (whether through statutory provisions or through regulations) that progressively erode that protection and that are exacerbated by permissive interpretations on the part of bodies such as the Office of the Australian Information Commissioner that foster the erosion.

The proposed regime's reliance on self-assessment is inadequate

This submission began by highlighting an issue that goes to trust. There is no requirement in the proposed regime for independent privacy impact assessments and for comprehensive reporting on government practice.

What we have seen over several years is that government agencies at the national and state/territory levels either have not engaged in privacy assessment exercises or have instead engaged in 'privacy assessment theatre'. They have self-interestedly conducted self-assessments that are lack substance and lack legitimacy.

Irrespective of the digital 'jam tomorrow' assurances by Stuart Robert, the proposed regime needs a strong foundation in practice. Reference to various Safes is inadequate if sharing is in practice a matter of agencies telling themselves and each other that they are safe, trustworthy, diligent, competent and otherwise doing the right thing.

There are benefits from data sharing but that sharing must occur within a coherent privacy framework.

The proposed regime mandates transparency about citizens, obfuscation about Government

The legislation will provide agencies and their partners with access to a wide range of data collected on a mandatory basis. It is in essence a mechanism for transparency *about* all Australians, an open sesame.

The legislation does **not** enshrine transparency and thus accountability about what is being done with the data … and indeed what data is being shared. It obfuscates ministerial and bureaucratic accountability in favour of claims that governments can be trusted. Observers watching ongoing denial about governance failures regarding major IT and other programs and indifference to perceptions of ministerial impropriety are entitled to be wary about such claims.

We accordingly urge the establishment of a statutory reporting requirement that covers statements on an agency by agency basis identifying –

- what data is being shared
- how it was derived
- which entities are receiving that data
- why the data is being shared
- how the data is being used

The statements should be readily accessible. They should be timely and comprehensive. They are a matter of legitimacy. They reflect the mandatory nature of much data collection. They provide a basis for official accountability. They a more than the vague 'Register' referred to in section 130 of the Bill.

Such accountability is salient in an environment where there is growing community distrust of governments and where the behaviour of senior officials and politicians raises questions about corruption. It is consistent with the values enshrined in the *Freedom of Information Act 1982*, an accountability mechanism that some Ministers and agencies disregard.

Governments are prone to justifying erosion of privacy by asserting "if you have nothing to hide you have nothing to fear". In relation to population-scale data sharing the Australian government should embrace that assertion by –

- providing transparency of what, how and why its sharing is taking place
- empowering regulators to effectively address those instances where behaviour is inappropriate.