THE CONVERSATION

Academic rigour, journalistic flair

Lukas Coch/AAP

Towards a post-privacy world: proposed bill would encourage agencies to widely share your data

September 16, 2020 5.30pm AEST

The federal government has announced a plan to increase the sharing of citizen data across the public sector.

This would include data sitting with agencies such as Centrelink, the Australian Tax Office, the Department of Home Affairs, the Bureau of Statistics and potentially other external “accredited” parties such as universities and businesses.

The draft Data Availability and Transparency Bill released today will not fix ongoing problems in public administration. It won’t solve many problems in public health. It is a worrying shift to a post-privacy society.

Author

Bruce Baer Arnold

Assistant Professor, School of Law, University of Canberra

It's a matter of arrogance, rather than effectiveness. It highlights deficiencies in Australian law that need fixing.

Read more:* *Australians accept government surveillance, for now

---

Making sense of the plan

Australian governments on all levels have built huge silos of information about us all. We supply the data for these silos each time we deal with government.

It's difficult to exercise your rights and responsibilities without providing data. If you're a voter, a director, a doctor, a gun owner, on welfare, pay tax, have a driver's licence or Medicare card – our governments have data about you.

Much of this is supplied on a legally mandatory basis. It allows the federal, state, territory and local governments to provide pensions, elections, parks, courts and hospitals, and to collect rates, fees and taxes.

The proposed Data Availability and Transparency Bill will authorise large-scale sharing of data about citizens and non-citizens across the public sector, between both public and private bodies. Previously called the "Data Sharing and Release" legislation, the word "transparency" has now replaced "release" to allay public fears.

The legislation would allow sharing between Commonwealth government agencies that are currently constrained by a range of acts overseen (weakly) by the under-resourced Australian Information Commissioner (OAIC).

The acts often only apply to specific agencies or data. Overall we have a threadbare patchwork of law that is supposed to respect our privacy but often isn't effective. It hasn't kept pace with law in Europe and elsewhere in the world.

The plan also envisages sharing data with trusted third parties. They might be universities or other research institutions. In future, the sharing could extend to include state or territory agencies and the private sector, too.

Any public or private bodies that receive data can then share it forward. Irrespective of whether one has anything to hide, this plan is worrying.

Why will there be sharing?

Sharing isn't necessarily a bad thing. But it should be done accountably and appropriately.

Consultations over the past two years have highlighted the value of inter-agency sharing for law enforcement and for research into health and welfare. Universities have identified a range of uses

regarding urban planning, environment protection, crime, education, employment, investment, disease control and medical treatment.

Many researchers will be delighted by the prospect of accessing data more cheaply than doing onerous small-scale surveys. IT people have also been enthusiastic about money that could be made helping the databases of different agencies talk to each other.

However, the reality is more complicated, as researchers and civil society advocates have pointed out.

In a July speech to the Australian Society for Computers and Law, former High Court Justice Michael Kirby highlighted a growing need to fight for privacy, rather than let it slip away. Shutterstock

Why should you be worried?

The plan for comprehensive data sharing is founded on the premise of accreditation of data recipients (entities deemed trustworthy) and oversight by the Office of the National Data Commissioner, under the proposed act.

The draft bill announced today is open for a short period of public comment before it goes to parliament. It features a consultation paper alongside a disquieting consultants' report about the bill. In this report, the consultants refer to concerns and "high inherent risk", but unsurprisingly appear to assume things will work out.

Federal Minister for Government Services Stuart Roberts, who presided over the tragedy known as the RoboDebt scheme, is optimistic about the bill. He dismissed critics' concerns by stating consent is implied when someone uses a government service. This seems disingenuous, given people typically don't have a choice.

However, the bill does exclude some data sharing. If you're a criminologist researching law enforcement, for example, you won't have an open sesame. Experience with the national Privacy Act and other Commonwealth and state legislation tells us such exclusions weaken over time

Outside the narrow exclusions centred on law enforcement and national security, the bill's default position is to share widely and often. That's because the accreditation requirements for agencies aren't onerous and the bases for sharing are very broad.

This proposal exacerbates ongoing questions about day-to-day privacy protection. Who's responsible, with what framework and what resources?

Responsibility is crucial, as national and state agencies recurrently experience data breaches. Although as RoboDebt revealed, they often stick to denial. Universities are also often wide open to data breaches.

Proponents of the plan argue privacy can be protected through robust de-identification, in other words removing the ability to identify specific individuals. However, research has recurrently shown "de-identification" is no silver bullet.

Most bodies don't recognise the scope for re-identification of de-identified personal information and lots of sharing will emphasise data matching.

Be careful what you ask for

Sharing *may* result in social goods such as better cities, smarter government and healthier people by providing access to data (rather than just money) for service providers and researchers.

That said, our history of aspirational statements about privacy protection without meaningful enforcement by watchdogs should provoke some hard questions. It wasn't long ago the government failed to prevent hackers from accessing sensitive data on more than 200,000 Australians.

It's true this bill would ostensibly provide transparency, but it won't provide genuine accountability. It shouldn't be taken at face value.

Read more:* *Seven ways the government can make Australians safer – without compromising online privacy

---

Federal Government Data sharing Privacy law Data privacy Australian Information Commissioner Information commissioner Government transparency Data ethics Draft picks Liberal National Coalition data access