5 March 2021

The Committee Secretary
Senate Review of the Data Availability and Transparency Act
Parliament House
Canberra
Australian Capital Territory
Australia

Dear Secretary,

We highly recommend the Data Availability and Transparency Bill to you as an enabler of Australian citizens and their democratic government, in the data age.

Executive Summary

- The Data Availability and Transparency Bill is a critical **productivity driver** for Australia's government and for improved citizen outcomes. With its origins in a review by the Productivity Commission, we are pleased to have contributed to the entire development journey of this Bill
- Competing interests in a society such as our own are always being balanced by our democratic process, under the rule of law. We contend that it is crucial for government data to be mobilised, in an appropriate manner, to address societal problems and opportunities. The pandemic has demonstrated the high efficacy of data-driven policy and management, over ideology and opinion. Privacy cannot be used as a continued basis for saying 'no' to data access for good purposes. Why not have **more privacy AND enable data to be put to beneficial purposes**? This is a technology question to be solved, and should not be an ideological position
- The Bill is **principles-based, offering a longevity advantage** over a highly-codified piece of legislation. Practitioners will require some ongoing guidance (in development at the Office of the National Data Commissioner), which should be expected, especially as the rate of change in data and technology spheres continues to increase
- The Bill is aimed at Australian Government departments and authorities, all of which are in existence for the *betterment of Australia and her citizens*. These departments are already making data sharing decisions, and would under this Bill, be **supported in making better decisions about data sharing**, supported by the Office of the National Data Commissioner.

Introduction to Data Republic Pty Ltd

Data Republic is an Australian technology company, supplying products which assist organisations who need to share access to data in a conscious, considered and controlled manner.

Our team of 50 is largely based in Sydney, although we now have sales and service representation in Singapore and the United States. We have US patents for our data collaboration technology, and for our secure matching (linkage) technology.

During the last five years, we have been privileged to learn a lot about how serious organisations are about their custodianship of valuable and sensitive data, and about the formative effect that Australia's Privacy Act has had on our data culture and international competitive advantage in the data sphere.

We have also observed the risk points around legislation that is designed to protect privacy - some organisational cultures simply find it easier to say "no" to any external access to their data, no matter the strength of the case for application of the data, or the protections provided for the data itself. What is particularly powerful about this Bill is that it delivers an enabling toolkit for getting to 'yes', and should prove influential beyond government (where the legislation is directed).

Productivity Driver

Australia is currently taking some world-leading reforms that will serve the nation well in an increasingly digital and data-driven world. For example, our new Consumer Data Right, a reform designed carefully to give consumers more control over their data and so-derive better value in the banking services (and other sectors such as energy and telco as the CDR is rolled out) they select.

Through the Data Availability and Transparency Act, as a nation we can take further leadership; by deploying the right data to complex and intractable social, medical and policy challenges; rather than leaving the explanatory data locked up in departmental data systems. Look at what New Zealand is doing to tackle intractable social problems as a result of multi-dimensional data views: Role of Data (treasury.govt.nz). NSW Gov has also taken steps on multi-department data analysis to tackle the most difficult problems arising from 'blind' single-department data outlooks and policies.

One of the key problems with missing the opportunity presented by this Bill, is less inter-departmental collaboration to tackle the toughest problems; less research and innovative solution development; and fewer social good outcomes for Australians. Let's not delay, as it's the least privileged in our society who suffer the most from our policy failures.

More privacy and data applied to noble purposes?

For all of us (other than a few individuals and organisations with a particular ideological position on privacy), privacy is not an absolute concept. For example, social media is filled by people sharing a range of personally identifiable information, that information is traded widely in return for a social utility that the people contributing the data find valuable.

Citizens in a secure and democratic society like Australia are generally concerned about privacy in the context of marketing that they find invasive, data breaches and their potential impact on financial security, and (possibly) the use of data for discriminatory purposes. There is increasing understanding that (i) data can be applied to social good outcomes (NSW Gov is actively promoting understanding of this concept online and through events); (ii) data is neither good nor bad, and that the application of data is the pertinent focus.

In our conversations across enterprise and government we observe high levels of care and concern about how data is applied. Custodianship of data requires concern for all the stakeholders in the capture and creation of that data, whether individuals, citizens or the data holder. Sustainability is a particularly pertinent concern that leaders in large organisations bring to any consideration of a data sharing activity.

The Data Availability and Transparency Bill is designed to ensure that both the application of data to a purpose (permitted use) and the steps taken to ensure the privacy and security of the data are also considered carefully by data custodians (the Bill providing an enabling process for that consideration).

Data sharing is already happening in government. Personal data de-identification processes and data linkage processes (between different departmental data holdings and external holdings) have been underway for years (refer to Health, the Australian Institute of Health and Welfare (AIHW) and Australian Bureau of Statistics (ABS) for examples). This Bill

provides the required guidance on data sharing, helping to ensure best practice, and giving confidence to public servants who have, in the past. found it more comfortable to say no to data sharing, regardless of how compelling the outcomes of the data application might be.

The Bill is not concerned with public release of data; the level of risk in exposing data more privately to limited and known persons/entities, under controlled conditions is an entirely different prospect to public release. The OAIC has provided a range of guidance in the risk management of personally identifiable information in a contextual sense. The standard of de-identification has to be higher for public release than in a secure IT environment, with access by a known and trusted user.

The technology that is applied to both secure-access data sharing, and de-identification is rapidly changing. Privacy may not be an absolute, as mentioned above, but it is increasingly a risk that can be managed.

Data Republic clients including health insurers, banks and airlines leverage our technologies. With sensitive data to protect, they leverage our data segregation and de-identification technologies, and avoid surrender of their data to other parties by using our access-only analytical environments. While we are a US Patent holder for these solutions, Data Republic is far from being the only organisation to go to for secure and privacy-protecting technology.

There are many other organisations working on technologies for secure, private and controlled data sharing. This emergent software category of technology is making it possible to have both more privacy AND more data sharing.

A principles-based Bill for longevity

With rapidly changing technology, the collection and application of data is evolving quickly. Few Australians will remain troubled, from a privacy perspective, by the arrival of personally addressed direct mail in their letterbox in 2021, whereas this was an issue just twenty years ago. While the channels evolve, the Privacy Act (1988), another principles-based Act, has remained as relevant today as in the past. The APPs remain relevant and effective. This is regardless of the views of large digital platforms who seem to find it difficult to comply with our privacy legislation and have driven our lawmakers in fresh directions.

By sending the Data Availability and Transparency Bill to review, the Senate has expressed its desire for more specificity in the Bill, whereas those responsible for the development of the Bill are working on guidelines, regulations and other support materials for data custodians who want to apply the principles of this Bill.

(i) Flexibility on consent

The Bill requires consent of citizens to be in place, in order for a data application to be permitted. This is consistent with the Privacy Act, and Data Republic agrees that consent should be at the centre of data application decisions.

We advocate for a universal consent management system, enabled by technology, to place citizens in charge of the use of their data. As the government moves to offer more and more of its services to citizens digitally, there is increased scope for consent solutions to enable data sharing.

In the absence of a fast, easy to understand and revocable consent system, data custodians need a transitional path to mobilise data to noble purposes. The Bill sets a high bar for waiver of the consent requirement - that it is ‘unreasonable or impractical’ to gain consent. This high bar will serve to encourage government departments to make progress on their capture of citizen consent for data sharing. It is important to retain this exemption from consent into the future, for example, since health data stored over time (including records of deceased individuals), are of high value for researchers working on more intractable health issues.

Equally, data sharing for urgent, high value (to Australians) purposes which might for example, be required under pressure from unforeseen health threats, could be undertaken using the data sharing provisions of the Bill.

(ii) 'Trespass on the Right of Privacy'

Australian citizens require their government departments to act in the interests of Australians. Where there is no legislative enabler for sharing information between departments and with researchers, we are asking public servants to achieve desired outcomes, with 'one hand tied behind their back'. Consent from the subjects of the data is the ideal standard to meet but is not in place right now for Australian government departments. Privacy of individuals can be managed through data access control and de-identification techniques, and should not be a reason to stop data from being applied to noble purposes in areas like health, social welfare, veterans affairs and 'closing the gap' for our indigeneous citizens.

(iii) De-identification

Rather than simply requiring 'de-identification' as codified law, we implore the Committee to consider the expertise and technologies available in data de-identification and re-identification risk management. This is a complex and developing area of technology, and there are few absolutes.

Personally identifiable data is not limited to names, email or physical addresses, or mobile phone numbers. Attributes on anonymised records can be re-identified, if other data is brought to the task. Although this Bill is not concerned with Open Data, Victoria's Myki case is highly indicative of how much care is required in the case of public release Information Commissioner investigates breach of myki users' privacy - Office of the Victorian Information Commissioner (ovic.vic.gov.au). A de-identification requirement could have the unforeseen effect of diminishing the efficacy of all data sharing by the government.

There are trade-offs between permanent de-identification of data, and the usefulness of that data in research and policy formulation. For example, if data is synthesised or varied (permutated) it may no longer provide all of the accurate insights that are desired.

There are also huge differences in the risk of re-identification in a public release of data, as compared to a highly-restricted data access provided to a known researcher or a second government department. The OAIC has highlighted that management of re-identification risk is contextual (how is data access occurring) and ongoing piece given changes in technology and data access continue to occur. As such, Data Republic recommends similar application in the context of this Bill, to consider re-identification and de-identification of data as a wholly contextual exercise including legal or technical controls, not just those applied to the data itself. Practitioners value such guidance from the OAIC, as they are making careful decisions about data sharing on an ongoing basis.

(iv) Public Interest

Government departments exist under Australian law, and our observations suggest they have a good understanding of what is in the public interest. Through a considered data sharing process, a range of input from different public servants will be drawn into data sharing decisions, helping to ensure that a consensus view on the public interest is developed for each project. Guidance from the Office of the National Data Commissioner will also assist. The definition of public interest should not require codification, but would ideally remain dynamic over time.

(v) Permitted Use of Data

We would again implore the Committee to avoid adding a highly codified approach to permitted use in the Bill, which over time would serve to narrow the beneficial effects of this Bill. The data custodians making decisions about data sharing use cases (projects) are those responsible public servants within our own government departments. They are restricted from a range of data sharing applications (including law enforcement) by this Bill, and further

limited to purposes within (a) the delivery of government services, (b) informing government policy and programmes and (c) research and development. Having observed the application of permitted use in data collaboration over the past five years, we believe that the Bill, as drafted, provides the right scope.

Better decisions about data sharing

At the core of this Bill is the potential enablement of government to share data between departments and to produce better policy, and thereby outcomes, for citizens.

Data sharing is already happening, sometimes between government departments and their instruments, with researchers and between departments. The Australian Bureau of Statistics (and others) have greatly assisted with the process of sharing in some cases, with de-identification and linkage technologies.

This Bill creates a framework for better decisions about data sharing, which will enable more effective use of government data to achieve public interest outcomes in areas like health and welfare. Data Republic has observed the challenges that data sharing can represent to responsible organisations, who are compelled to sufficiently cover protection of privacy, confidentiality, commercial interests, the sustainability of the permitted use of data and data security. This Bill provides a process to government departments who may otherwise be unable to act on data sharing.

In addition to the Bill, the regulators including the Office of the National Data Commissioner are developing a range of additional guidance, which over time can remain responsive to changes in the environment for data sharing. In our submission 63-edsubmission-data-republic-dat-bill.pdf (datacommissioner.gov.au), provided as part of the wide-ranging consultation undertaken by the National Data Commissioner in the development of this Bill, we recommended the provision of additional guidance materials, particularly around the exemptions to the consent requirement.

All speed in your review of this transformational Bill. We have great belief in its construct.

Regards,

Data Republic