UNIVERSITY OF SOUTHERN QUEENSLAND

# Submission to the Office of the National Data Commissioner – Data Availability and Transparency Bill 2020

**Dr Lynda Crowley-Cyr, School of Law and Justice USQ and Ms Carole Caple, Solicitor.**

## USQ School of Law and Justice

The University of Southern Queensland (USQ) was established in 1992 and is a regional university with a global perspective, expert in distance and online education. It provides higher education to one of Australia's most diverse student cohorts and has a strong reputation for maximising student potential, academic and personal.

The USQ School of Law and Justice was established in 2007. It is the second-biggest law school in Queensland, with students enrolled in Bachelors of Laws, Bachelor of Laws with Honours, Juris Doctor, Masters of Laws and Doctor of Philosophy programs.

Academics in the School of Law and Justice are located on both Toowoomba and Springfield campuses. A very high proportion have doctoral qualifications and the School has a strong commitment to quality legal research and publication and to retaining a close research-teaching nexus.

### Submission by Dr Lynda Crowley-Cyr and Ms Carole Caple

Dr Lynda Crowley-Cyr, PhD (USyd), LLM (JCU), LLB (QUT), is a lawyer and Associate Professor at the School of Law and Justice at the University of Southern Queensland.

Ms Carole Caple, LLB (Hon) and LLM, is an Australian legal practitioner and accredited anti-money laundering specialist.

[redacted]

*This submission represents solely the individual views of the authors, and should not be taken to represent the views of any persons, employers, or organisations that she is affiliated with.*

# Part 1 Background Introduction

The authors welcome the opportunity to comment on the Office of the National Data Commissioner's (ONDC) consultation (Consultation Package) on:

- Data Availability and Transparency Bill (DAT Bill) Exposure Draft Explanatory Memorandum;
- Data Availability and Transparency (Consequential Amendments) Bill and Explanatory Memorandum;
- Data Availability and Transparency Regulations and Explanatory Statement; and
- Accreditation Framework Discussion Paper.

**Overview of data sharing under the proposed ONDC scheme**

The ONDC Consultation Package creates a scheme for data sharing. Essential elements of the proposed scheme are that public sector agencies (*'data custodians'*) will be able to disclose public sector data in their possession to recipients who are an '*accredited user'*. The National Data Commissioner accredits would-be recipients under the scheme. Would-be recipients need to demonstrate capacity in governance and administrative frameworks; security and privacy of data; and technical skills and capacity. The Accreditation Framework creates a single control point for entry into the scheme, which then determines access. In other words, once accredited, an organisation can access data for '*permitted purposes'* on multiple occasions, from many data custodians. Permitted purposes include the delivery of government services; to inform government policy and programs; and research and development.

There are '*precluded purposes'* which are not authorised by the DAT Bill. Specifically excluded purposes from the scope of the DAT Bill, are national security data and enforcement related purposes, as well as sharing that would infringe intellectual property rights, international agreements, or where intelligence agencies are involved. Also precluded, is the sharing of operational data, evidence before courts, tribunals, or 'certain agencies with oversight or integrity functions to protect the independence and confidentiality of their core functions'. Also omitted from the Bill's

override are legislative provisions that '*preserve protections*' around national security, as well as MyHealth Record data, COVIDSafe app data and more.

The scheme's risk management framework is arranged around '*principles*'. Once in the scheme, in order to share data, the five data sharing principles (adapted from the Five Safes risk framework for data access) must be considered. The principles act as safeguards for the adequacy, appropriateness or agreement of a decision to grant access to data. The principles are organised around a broad structure of matters relating to Project, People, Setting, Data and Outputs.

# Part 2 Responses to the Bill

### 1. Concerns

The authors are concerned for the inadequacy of the privacy risk controls and safeguards of the proposed ONDC scheme.

Research undertaken in universities, for example, must adhere to strict standards of ethical review. Generally, the personal information of participants must be aggregated or de-identified to protect their privacy. Greater safeguards are required when dealing with information pertaining to vulnerable groups. Under strict guidelines, this can be waived if the researcher can demonstrate a sufficient element of beneficence. Every effort is to be made to obtain the consent of participants.

However, none of these risk controls or safeguards are present in the proposed ONDC scheme. These concerns are exacerbated by the scheme's intention that '*accredited users'* would include other government agencies, and more broadly, research bodies and private sector entities.

The scheme envisages the possibility that entities could be charged a fee to become accredited. This will enable accredited users to access the personal information of Australians collected by government. The authors find this proposal questionable.

In realising the myriad of benefits of data sharing, significant challenges will emerge and need to be addressed. Under the scheme, there does not appear to be any overarching rationale or philosophical statement to underpin how information will be shared equitably and effectively. There is no plan evident for dealing with cultural,

legal and ethical issues that may arise. The authors query how effectively the challenges have been identified under the Consultation package.

There is an emphasis in the literature on the need to develop trusted collaborative networks between the government, the private sector, and the public at large whose information is in the balance. Such networks are characterised by substantial investment in the potentially difficult work of building trust and relationships.

## 2. Uncertainty to be resolved

Australian Privacy Principle 6 generally governs how personal information can be used and disclosed. Pursuant to the DAT Bill, the entire data-sharing scheme is excised from the operation of the APPs. Instead, the proposed scheme establishes an alternative authority to govern disclosures. This would effectively circumvent the Privacy Principles, and override other privacy mechanisms in secrecy and non-disclosure prohibitions. In this regard the DAT Bill represents a fundamental and significant change to the way information privacy is understood and implemented in Australia.

Moreover, the authors note announcements that the *Privacy Act 1988* will also undergo substantive review. In terms of timing, this review of the legislation and the proposed introduction of a data sharing-scheme is confusing. How will the review intersect with the proposed ONDC scheme? Taken together, these initiatives overturn some 30 years of privacy jurisprudence which governs how and when personal information can be disclosed by government agencies.

## 3. Timeframe

The ONDC Consultation creates a complex and novel regime. Despite this, the proposed scheme has only been available for comment for 40 working days.

The authors are concerned that this truncated timeframe does not allow for proper and fulsome public consultation. The timeframe for comment disregards the time required for meaningful engagement with the ONDC Consultation package and the reforms proposed by the scheme.

## 4. Trust and public expectations around privacy

The DAT Bill and ONDC Consultation Package collectively build on the recommendations of the 2016 Productivity Commission enquiry into Data Availability and Use. The PC's report sought to highlight the 'full potential of public sector data in Australia' and suggested unknown opportunities lie within the untapped data. The PC's recommendations centred on the creation of the Data Sharing and Release Bill and a National Data Commissioner to oversee the new scheme.

However, the authors believe that in the space of the last three or four years, community attitudes have shifted towards increased privacy protection for personal information. This, in part, results from recent scandals and incidents such as the Cambridge Analytica and ongoing Facebook revelations; RoboDebt; CensusFail; and numerous data breaches involving publicly held personal information. The concurrent sharp rise in cases of fraud and identity theft have all converged to eroded community trust, leading to a shift in public consciousness.

This shift was likely influenced by multiple factors. For instance, in September 2020, the Australian Government's first annual cybersecurity threat report noted 2,266 cybersecurity incidents and 59,806 cybercrimes over the last financial year. It also indicated a rise in COVID-19 themed scams from March 2020 onwards.

At the same time, researchers at the Optus Macquarie Cyber Security Hub published their report on a three-year cybersecurity audit of government websites. The report reviewed 1,862 externally-facing websites across Australia's federal, state and territory governments. Despite improved cybersecurity, many of these sites were found to be vulnerable to malicious attacks and insecure data. Further, the report notes that these websites did not have basic HTTPS website protocols installed. This increases their exposure to vulnerability.

Another potential factor that threatens public confidence is the misuse of confidential information by public sector agencies. This is a recognised corruption risk. In February 2020, two government reports on misuse of information by public sector entities were released. These include the Queensland's Crime and Corruption Commission report titled *Operation Impala - A Report on the Misuse of Confidential Information in the Queensland Public Sector*, and the report by the Victorian Independent Broad-based Anti-Corruption Commission titled *Unauthorised Access*

*and Disclosure of Information Held by the Victorian Public Sector*. Importantly, the IBAC found that public sector agencies could better prevent and detect misuse of information if they implement a number of measures. This includes establishing comprehensive audit programs to identify and deter misuse, and raising awareness of risks, and of the importance of reporting incidents when they occur, among government employees and the community.

## 5. How concerned are Australians about privacy

The Office of the Australian Information Commissioner recently released the results of the *2020 Australian Community Attitudes to Privacy Survey.* The survey, last performed in 2017, documents the aforementioned shift in community attitude.

The Survey defines information sharing as personal information or user data that is passed from one organisation to another for government, commercial or other purposes. Around 70% of Australian respondents stated that protection of their personal information is a major concern. Governmental use of people's personal data, for specific purposes, was significantly less likely to make Australians uncomfortable. The level of discomfort with some practices though is high, and increases where government agencies share personal information with businesses (only 15% comfortable) in Australia for commercial and other purposes.

Overall, Australian's levels of trust in the ability of institutions to properly handle their personal information is down by 14% since 2017 for Australian Government organisations, with a steady decline in trust over the past 13 years. Another notable finding of the Survey was that a vast majority of Australians across most demographic groups want the government to do more to protect the privacy of their data.

The findings on community attitudes are also consistent with a rise in the number of privacy related complaints made by Australians (up 12 % to 3306 in 2018-19). According to the OAIC in its Annual Report, the increase was driven by privacy practices of the finance industry, Australian government entities, health service providers, telcos, and others. What this highlights is that the finance industry and government accounted for the two sectors that attracted the highest number of complaints at 13 % and 12% respectively.

The total number of FOI requests to Australian government agencies and ministers grew by 13% in 2018-2019 to 38,879. Of those, 83% were for documents containing personal information. This further suggests that Australians are becoming more concerned about privacy than previously.

## Conclusion

The authors acknowledge there are vast potential benefits in leveraging publicly held datasets. Such data have the power to enable government to deliver more effective services, design better programs and make improved decisions. The potential of data sharing also creates substantial value for the public, private, not for profit and research sectors.

What is required is a single unified and ethical approach to improve the fragmented, and at times unclear, approach that currently exists. As such, the authors support the reduction of complexity and removal of unnecessary barriers on government data sharing.

Recurrent themes in literature on data sharing, point to the need for balance between a regard for the public good that would arise from permitted purposes and reserving respect for the sensitive and personal nature of information entrusted to government. Multiple examples abound that demonstrate that analyses of pooled data from different studies, in different locations, have led to new approaches to solving persistent and emerging problems more rapidly. There is also evidence of areas where the failure to share data has disrupted efforts to respond as well, or in as timely a way, as might have otherwise been the case.

## Recommendations

The authors recommend:

1. The loosely controlled environment for data sharing created by the ONDC DAT Bill requires revision and strengthening. The regulatory requirements should create greater privacy protections for use of data, including personal information.

2. The proposed data-sharing scheme should be subject to the *Privacy Act 1988.* There is a need for consistency and a single unified and ethical approach. The ONDC Consultation Package should be located within that streamlined framework.
3. The *Privacy Act 1988* should be reformed and strengthened to meet community expectations and technological advances. This would better enable ethically approved data sharing in the public interest.
4. A proposed data-sharing scheme should contain protections that include comprehensive audit programs to identify and deter misuse. To help restore public trust, the scheme should be subject to a federal Integrity Commission oversight.
5. A proposed data-sharing scheme should be subject to adequate, fulsome consultation. This would allow better understanding of community expectations and the electorates' need for privacy to be properly accommodated within the proposed scheme.