10/09/2018

Mr Daniel McAuliffe

Structural Reform Group

The Treasury

Langton Crescent

PARKES ACT 2600

Dear Mr McAuliffe

**Consumer Data Right – Treasury Laws Amendment (Consumer Data Right) Bill 2018**

Thank you for the opportunity to comment on the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (CDR Bill).

At the outset I would like to record my thanks to the Treasury staff who have been involved in this consultation process. The consultation session I attended in Melbourne was helpful and informative and Treasury staff have been available and willing to engage in debate and discussion about the CDR and the CDR Bill.

Although submissions are primarily sought about the CDR Bill and not its underlying policy settings, both policy and drafting issues are so closely connected that any meaningful commentary requires consideration of whether the CDR Bill is the most effective means of addressing the relevant policy issues.

**Submission Summary**

Overall, this submission supports the creation of a Consumer Data Right (CDR) but argues that the CDR Bill’s approach is flawed.

The reasons are:

* Its incremental, sector-by-sector approach undermines and delays the competition and innovation dividends the Bill is designed to promote. It places Australia at a competitive disadvantage
* The CDR Bill is complex framework legislation that inappropriately confers powers and responsibilities on a number of unaccountable entities to ‘make up’ and vary the law. It empowers them to make rules and legislative instruments in a manner that is not transparent. It creates conflicts of interest and imposes significant regulatory and compliance burdens
* The CDR scheme lacks an overall governance framework
* It uniquely creates a quasi-right to privacy for commercial enterprises
* The Bill does not account for risks posed by advanced data analytics (Big Data)
* The Bill does not adequately address security issues
* The Bill does not adequately address intellectual property issues.

The Bill will produce an onerous CDR that will favour established, entrenched data holders at the expense of consumers. It needs to be significantly streamlined and rebalanced in favour of the individuals whose interests it is designed to serve.

**Background**

Individuals have had a right of access to their personal information held by the Commonwealth public sector since 1988. Since 2001 they have had a right to access their personal information held by the private sector organisations covered by the *Privacy Act 1988*. State and Territory privacy (and health privacy) legislation confer similar rights. There is nothing new about individuals having a right to access their personal information.

The effectiveness of these rights has been criticised because:

* public sector organisations have been able to charge a fee for access and for processing a request;
* private sector organisations have been entitled to charge a fee for processing an access request;
* for both public and private sectors, the access regime has been paper-based and has lacked incentives to invest in providing access in a digital form.

The CDR Bill does not adequately resolve any of these reform issues.

The CDR is an attempt at designing a data portability framework for Australian consumers. Its aim is to empower consumers by enabling them to obtain their own personal information in digital form and/or to direct its transmission to third parties. It is designed to diminish information barriers – digital ‘lock-in’ - that currently impede consumers from changing service providers.

It is also intended to facilitate the development of new digital enterprises – providers of financial services known as ‘fintech’ – as well as new and innovative forms of data intermediaries, platforms and service providers, aimed at providing consumers with novel product and service offerings.

The CDR is the first Australian initiative that straddles previously disconnected areas of rights and public policy, these being banking and finance policy, competition policy, security policy and the fundamental rights to privacy. This creates a unique policy dilemma: how to go about providing robust and meaningful protection of the privacy and security of personal (and other consumer) information whilst incentivising its greater use and disclosure to enhance competition and encourage innovation?

As a data portability right the CDR can be compared to Article 20 of the EU’s *General Data Protection Regulation* (GDPR) but it differs from it in important ways. GDPR data portability only applies to information provided by the data subject. It does not apply to directly or indirectly derived data or associated data (see cl. 56AF). Article 20 is not limited by sector whereas the CDR is. Article 20 does not establish elaborate technical standards for data portability: data must be provided to the data subject ‘in a structured, commonly used and machine-readable format.’

The GDPR’s data portability regime is simpler and more comprehensive than the CDR. It is not mediated by opaque discretionary decision-making and complex consultation mechanisms. Because of this it is:

* more ‘consumer friendly’;
* likely to be more effective; and
* unlikely to produce the high compliance and regulatory costs that will be associated with the CDR.

The GDPR is also recognised as an international benchmark. Australian enterprises that control and process EU data or provide services to EU citizens have already been required to take steps to comply with it. Many of Australia’s trading partners in the Asia-Pacific region and elsewhere are actively considering enacting data portability legislation. This suggests that adopting a *sui generis* incompatible Australian CDR is inadvisable unless there are compelling contrary reasons.

**2. Commentary**

**2.1 Objects**

The Bill’s objects are set out in cl 56AA. Although objects clauses are not definitive guides to the interpretation of legislation, courts often take account of them where there is uncertainty or ambiguity about the operation of a law. Objects clauses shape and inform the exercise of discretionary powers.

Clause 56AA(b) appears to contradict many of the aims of the CDR – significantly its aim to provide individuals with robust privacy protection – by stating that one of the two main objects of the proposed Part IVD of the *Competition and Consumer Act 2010* is to ‘enable any person to access any information…that does not relate to any identifiable, or reasonably identifiable, consumers..’ Apart from this objective extending beyond the policy basis of the CDR Bill, it raises complex and highly contested issues about the efficacy of de-identification. It can be interpreted as supporting de-identification as a technique when there is a significant body of expert opinion that casts doubt on it’s efficacy.

This object should be deleted.

**2.2 Complexity**

The Bill is framework legislation that leaves the substantive determination of legal rights and obligations to an array of entities. These include:

* the Minister - sectoral designation, determining what CDR data is, determining who a data holder is, determining who an accredited data recipient is
* the ACCC - non-exhaustively, consulting with the Minister on sectoral designation, making the consumer data rules, determining whether the consumer data rules should not apply to particular persons, rules about reviews of decisions made under the consumer data rules, determining whether particular consumer data rules are civil penalty provisions, determining access fees, enforcing data standards)
* the Data Recipient Accreditor (DRA) - making decisions to accredit persons under the consumer data rules
* an Accreditation Registrar (AR) - keeping and maintaining a register of accredited data recipients
* the OAIC – producing guidelines relating to the privacy safeguards and undertaking awareness raising and educational programs, conducting assessments of the management and handling of CDR data, investigating breaches and undertaking enforcement activities
* a Data Standards Body (DSB) – to determine and regularly review data standards, including the power to determine different standards for different sectors, different classes of CDR data, different classes of persons for a designated sector, different classes of accredited persons

This is an extraordinarily complex, expensive and unwieldy implementation of a straightforward concept – enabling consumers to obtain their personal information in digital form and/or to direct it to be provided to a third party. It can also lead to perverse and absurd outcomes. For example, there is no automatic right for an individual to receive his or her data unless accredited.

This complexity appears to have been influenced by the UK’s approach to open banking. But there are significant differences between it and the CDR. UK open banking is designed to underpin payment requests and remittances. Financial institutions rightly need to know that they are being validly instructed to make payments and that the recipient meets minimum regulatory standards in a payment scheme. The CDR does not establish a payment regime.

The complexity of UK open banking has led to substantial delays in obtaining regulatory approvals and significant entry costs for new participants which are in the vicinity of £20,000.

Despite this the Bill says little about how the discretionary powers it confers on such a broad array of actors are to be exercised or limited. For example, it provides no direction to the DSB, which appears free to develop standards such as security standards that are impossible or impracticable for new market entrants to meet. It does not have to comply with any timelines. The only discretionary guidance in the Bill is cl 56AD which applies to Ministerial sectoral designations (and by extension to ACCC consultation).

Much of the Bill’s complexity could be remedied – and its policy objectives better achieved - by:

* removing sectoral designation and applying the CDR across all of the private sector
* developing data standards *before* the CDR comes into effect and establishing effective and simplified means by which recipients can be accredited as well as ensuring that individuals who seek to access their data do not need to be accredited
* embodying the consumer data rules in the Bill or removing them entirely and relying on the APPs
* removing the privacy safeguards and relying instead on the APPs (suitably amended to adopt the Bill’s definition of ‘personal information’).

**2.3 Inappropriate conferral of powers**

As outlined in paragraph 2.2, the ACCC is given responsibility for establishing laws and rules, regulating them and enforcing them. This is an inappropriate mixing of functions. It amounts to an unmanageable conflict of interest. It is not unlike empowering law enforcement agencies to determine the criminal law as well as investigating and prosecuting breaches.

**2.4 Governance**

Although the Bill establishes new offices and functions (such as the DRA) and confers new and additional functions on a variety of offices and existing organisations (such as the ACCC and the OAIC), there is no provision for governance and oversight of the CDR scheme *as a whole.*

As currently configured, responsibility for key issues such as overseeing the effectiveness of the CDR scheme, assessing whether it is achieving its goals, whether it is delivering value for money, that risks are properly identified and addressed, and that it operates in a way that minimises friction between participants is not covered by the CDR Bill.

Each of the main government participants in the scheme are subject to mandated functions and responsibilities, for example in relation to competition outcomes and privacy protections such as disclosure, use and the security of CDR data. Some of these are overlapping powers. There is no mechanism for coordinating these.

It is recommended that the Bill be amended to establish an office, independent of each of the government participants, whose role is to undertake these functions, to receive comments and complaints, provide coordination and to provide public reports on a regular basis on the operation and effectiveness of the scheme.

**2.5 A corporate right to privacy?**

A right to privacy is an *individual* not a corporate or business right yet cl 56AD(1)(a)(iii) refers to a requirement that the Minister, in making sectoral designations, must have regard to ‘the privacy of consumers, whether the consumers be individuals *or other persons such as businesses’* (emphasis added).

It is inappropriate to include a provision that appears to confer privacy rights on corporations such as Australia’s banks. The CDR is designed to serve individual, not corporate interests. Consumer rights will be weakened by requiring discretionary decision-making to take account of a corporate right that does not otherwise exist in Australia or anywhere else in the world. There is nothing in any of the policy analysis or material that supports a corporate right to privacy.

Clause 56AD(1)(a)(iii) should be amended by removing the words ‘consumers, whether the consumers be individuals or other persons such as businesses’ and replacing them with ‘individuals.’

**2.6 Big Data**

Although neither the Bill nor the associated explanatory materials explicitly refer to it, the CDR is designed to fuel Big Data. It will be responsible for the widespread circulation of personal and other information in machine readable form that can be used by advanced data analytics to profile consumers, draw conclusions about them from multiple sets of data correlations and pattern recognition techniques and to manipulate their preferences and behaviours.

This is likely to occur using the data put in to circulation by the CDR in its own right or in combination with data obtained by other means, almost certainly using sources that include social media, search data, location data, preferences and meta data.

Participants in these techniques will almost certainly include corporations located outside Australia such as Facebook (which currently offers financial services through its WhatsApp application in certain territories) and that are, despite the accreditation regime outlined in the Bill, for all practical purposes beyond the regulatory capability and capacity of any of the entities vested with responsibility to oversee and administer the CDR.

Unlike the EU’s data portability regime, Australia has not developed sufficient or appropriate safeguards to enable consumers to manage these risks. For example, EU data portability is accompanied by a right under Article 22 of the GDPR that enables individuals to opt out of automated decision-making. Every member country of the OECD other than Australia has some form of ‘anchoring’ rights such as enforceable human rights obligations that support privacy and/or civil law actions for privacy infringement.

The absence of these countervailing rights and their corresponding remedies gives rise to significant uncontrolled risks that are not addressed. The Bill constitutes a *disincentive* to the development of innovative approaches to the control and management of personal information, for example, Privacy Enhancing Technologies and services that, for example, manage and enforce consent, use and disclosure processes or that provide consumers with security solutions.

**2.7 Intellectual Property**

The Bill does not address intellectual property issues – these primarily relate to copyright – that may be raised by data holders to impede the free flow of information within the CDR environment or to impose costs on it.

Although data derived only from information provided by a consumer is unlikely to satisfy the originality requirements of the *Copyright Act 1968,* the position is less clear in the case of value-added data (i.e., data that has had applied to it by advanced analytic techniques designed to provide insights into individual consumers and/or which has been combined with other data).

The CDR legislation should address this issue. There are a number of methods of doing so including the development of a compulsory licence under the *Copyright Act 1968* or by removing the CDR scheme from its infringement provisions. There is precedent for taking this latter approach in recent amendments to the *My Health Records Act 2012.*

It is recommended that the CDR be amended by removing sub-clauses 56AF(2) and (3). Such an amendment would also function to address the question of access costs that are left open for determination by the ACCC under cl 56BC(d) and (e). If copyright does not subsist in the CDR data and there are standardised data formats determined by the DSB at taxpayers expense, there is no justification for the imposition of access fees.

**2.8 Security**

Although the CDR Bill does not explicitly confer security functions, it enables the ACCC to make consumer data rules that cover security. Equally, the DSB may make standards about security under cl 56FE(1)(c). Both powers appear to enable the relevant agencies to impose rules that are equivalent to legal rules and obligations. It is incongruous that these rule making powers have legal effect but there are no legally binding rules imposed on security within the private sector or on the Commonwealth public sector.

This submission supports the need for appropriate security safeguards for the CDR. That said, security obligations must reflect the variability of risk in the CDR system, including the fact that new participants may have a risk posture that is significantly different from those of banks, telecommunications providers and energy suppliers.

The rules should also reflect the fact that while individuals have a legitimate right to expect that their personal information will be supplied to them in a secure form, such as being encrypted in transit, they should have the right to store received data in any manner they think fit: security standards should not function as an impediment to individuals exercising access rights.

Please let me know if you require any further information or clarification.

Yours sincerely,

**David Watts**

**Professor of Information Law and Policy**

La Trobe Law School

College of Arts, Social Sciences and Commerce | La Trobe University | Bundoora Victoria 3086

T: 03 9479 1979 | W: [www.latrobe.edu.au](https://unite.latrobe.edu.au/sites/lm/FBELMarketing/Public%20Documents/Faculty%20Templates/Email%20Signature/www.latrobe.edu.au)