Response to Treasury Laws Amendment (Consumer Data Right) Bill 2018 – Exposure Draft

Dr Katharine Kemp and Dr Rob Nicholls

7 September 2018

A joint initiative of

Allens › ‹ Linklaters

UNSW SYDNEY

The Allens Hub for Technology, Law and Innovation is a community of scholars at UNSW Sydney aiming to add breadth and depth to research on the interactions among law, legal practice and technological change in order to enrich scholarly and policy debates and enhance understanding and engagement among the legal profession, the judiciary, industry, government, civil society and the broader community.

This submission is made by Dr Katharine Kemp and Dr Rob Nicholls who lead the "Data as a Source of Market Power" Research Stream for the Allens Hub.

The views in this submission are our own, based on our research, and do not represent the official views of UNSW Sydney or Allens.

Support for improved consumer access to data, with caveats

We support consumers having a data access right, which is more user-friendly and meaningful than the current right to access under the *Privacy Act 1988* (Cth) and Australian Privacy Principle 12 in particular. Properly framed, such a right could make the quality and price of services in a number of markets much more transparent, aiding consumer comparisons and switching between providers. Reduced information asymmetries and reduced barriers to switching should in turn intensify competition between providers to the benefit of consumers.

However, if the government intends to encourage consumers to disclose their personal data more broadly for these purposes, it must also place appropriate limits on the new providers' use of that data to ensure that consumers are not in fact disadvantaged in the process of this increased disclosure,[1] as explained further in this submission.

"Legal transplants" and the different context of UK and EU regimes

In explaining the benefits of the proposed Consumer Data Right (CDR), Treasury has pointed to the recent implementation of "open banking" regimes and "data portability rights" in the United Kingdom (UK) and the European Union (EU). However, it is important to appreciate the UK and EU data portability rights have been implemented in very different regulatory contexts, which provide much stronger data protection and privacy regulations than those which exist in Australia.[2]

For example, in the UK, the law includes significantly higher standards for consumer consent, a right to require the erasure of personal information, and very substantial financial penalties for the infringement of data protection regulations. There is also a tort of misuse of private information under UK law, which does not exist under Australian law, although the Australian Law Reform Commission recommended the enactment of a similar tort in 2014.

Comparative law scholars have long cautioned against the adoption of "legal transplants" from other jurisdictions without sufficient consideration of the context in which those laws were created. In both the UK and the EU, a data portability right is part of a broader package of data protection rights which help to ensure that consumers are not in fact disempowered in the process of disclosing their personal data to new entitites.

This has two implications for the current proposal in Australia. First, it would be more accurate to call the measure a "data portability regulation", clarifying that it is not part of a similarly broad bundle of general data protection rights. Second, the Bill should incorporate further measures to ensure that consumers are not disadvantaged by the disclosure of their data to new providers, as explained in this submission.

[1] See K Kemp and D Vaile, Submission to the Australian Treasury on the Review into Open Banking in Australia Final Report (23 March 2018).
[2] See S Esayas and A Daly, 'The Proposed Australian Consumer Data Right: A European Comparison' (2018) 2 *European Competition and Regulatory Law Review* (forthcoming).

Primary legislation vs rules

The Exposure Draft Explanatory Materials (Draft EM) emphasises that "it is not practicable to place all of the detail that wil be contained in the consumer data rules in the primary legislation" [1.163] and the Bill instead provides "substantial scope for the ACCC to make rules about the CDR … because it is important to be able to tailor the consumer data rules to sectors and this design feature acknowledges that rules may differ between sectors" and that "[v]ariance between sectors will depend on the niche attributes of the sector" [Draft EM 1.82].

We accept there may be a need for the rules to be tailored to specific sectors in many respects. However, there are some core principles which should be consistent across all sectors which are not currently incorporated in the primary legislation.

Critically, **any consumer consent under the Privacy Safeguards should be explicit, unbundled, voluntary, fully informed, time limited, revocable and require action on the part of the consumer**. There is no niche attribute of any sector which requires lesser standards for consent. At this stage, the default position under the *Privacy Act* is that consent need not even be explicit, a standard which is increasingly out of line with international best practice.

There is also a strong argument that consumers should have a **right to erasure** in respect of any personal data transferred under the CDR regime, similar to the right to erasure under the EU General Data Protection Regulation (GDPR). Accredited Data Recipients (ADRs) will have a greater incentive to retain the trust of consumers in their data handling practices if a right to erasure is provided along these lines.

Transfer to non-accredited entities

The Draft EM states that "[i]n certain circumstances, CDR consumers can direct that their CDR data be provided to a non-accredited entity" which would then be "regulated via the APPs, if applicable" [Draft EM 1.47]. This proposal is problematic. While we appreciate the aim of avoiding the cost of accreditation for those entities not wishing to become fully-participating ADRs, the provision of CDR data to non-accredited entities under the CDR scheme would create a significant loophole that would likely be exploited by entities seeking to avoid the more stringent protections provided by the CDR scheme.

It would also potentially lead consumers to believe they were disclosing their information in controlled circumstances under the CDR regime, when the actual default application of the *Privacy Act* would provide lesser protections, such as the possibility of implied, bundled consents and the absence of the CDR civil penalties. In fact, if the non-accredited entity were a small business, the *Privacy Act* would provide no protection at all, given its general small business exemption.

Given that the Bill already contemplates tiered accreditation for lower risk uses of CDR data, in our view, the risks of permitting transfers directly to *non*-accredited entities would outweigh the benefits.

Effect of non-compliance on underlying transactions

The Draft EM states that a failure to comply with the consumer data rules will not invalidate the underlying transactions, for example, between a consumer and their bank [Draft EM 1.167]. We accept that transactions on a consumer's account should not be affected by such non-compliance. However, it should be made clear that failure to comply with the consumer data rules will invalidate the consumer's consent to a data holder's or ADR's handling of the CDR consumer data, as the case may be.

De-identification as an alternative to destruction

Under Privacy Safeguard 11, "if a person has collected the CDR data pursuant to privacy safeguard 3 or has data that is derived from the primary data, and the person is no longer using the data as permitted by the consumer data rules, then the redundant data must be destroyed *or de-identified* according to the consumer data rules applying to the relevant type of data" [Draft EM 1.219, emphasis added].

In our submission, at this stage, de-identification should not be permitted as an alternative to destruction of personal data when a person is no longer using the data as permitted by the consumer data rules.

Purportedly de-identified data is currently shared by numerous companies via data aggregating platforms in Australia and, since it is not considered to be personal information, few limits are imposed on the use of such data. However, data security experts warn that attempts to de-identify data will increasingly fail, particularly when supposedly de-identified data is combined with data aggregated from multiple alternative sources. Given the breadth and depth of data transferrable under the CDR regime, re-identification could reveal highly detailed and sensitive information about consumers. The re-identification of data will only increase with advances in machine learning and the accumulation of larger datasets from multiple sources. This is particularly problematic in the absence of the tort of serious invasion of privacy recommended by the Australian Law Reform Commission, as noted earlier.

If the objective of the CDR is to empower consumers in the use of their own data, the de-identification of data as an alternative to destruction should not be permitted until there has been thorough consultation on the feasibility of such de-identification and whether it adequately protects a customer who has shared their personal information for a limited purpose. The presumption should be that methods of de-identification will be reduced in effectiveness over time, and most will ultimately fail, so any reliance on them should come with very clear liability for this foreseeable mode of data breach.

Timing

Treasury has noted the ambitious timeframe for the passage and implementation of the Bill. In our submission, the greatest priority should be given to the proper consideration and implementation of rules, standards and systems that provide adequate protection for consumers before the CDR is implemented. While there will be no irreversible harm from a "slow and steady" approach to the construction of this important access right, there will be irreversible harm if implementation is rushed before appropriate protections are in place. Once personal information is disclosed and broadly shared, it cannot be made private again. Due caution and consideration are paramount, as evidenced by public response to the My Health Record.

Dr Katharine Kemp and Dr Rob Nicholls

7 September 2018