Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/about/contacts

29 August 2021

Strategic Assessment Team
Consumer Data Right Division
The Treasury
data@treasury.gov.au

Dear Treasury

Re: APF submission on CDR Strategic Assessment Consultation

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

We attach a Submission in relation to the above matter.

We request that you acknowledge receipt, that you pay attention to the points we make in it, that you reflect the content in your report and in your decision-making, and that you publish the document.

Thank you for your consideration.

Yours sincerely

David Vaile
For the Board of the Australian Privacy Foundation
0414 731 249 David.Vaile@privacy.org.au

Australian Privacy Foundation

Submission in relation to the CDR Strategic Assessment consultation

29 August 2012

Introduction

We remind Treasury of our multiple previous submissions on the Consumer Data Right (CDR), most recently on 16 October 2020 on the then proposed legislative amendments.

The major concerns we have repeatedly raised have been largely ignored. We therefore have a large query mark over the level of confidence we can have that you're actually listening.

We are making this further attempt to drew attention to some fundamental flaws in the design of the CDR, and the privacy risks, before a premature decision is made to extend CDR into other sectors.

APF rejects the underlying premise of the consultation paper that accelerated economy-wide implementation of the Consumer Data Right (CDR) is in the public interest.

Of the 12 specific consultation questions posed in the Consultation Paper, the only one that does not simply presume the extension of CDR is Q11 – Are there any datasets or kinds of data that may or may not be suitable for CDR designation? To this we answer emphatically – Yes! We submit that the case has yet to be made for *any* further extension of CDR until at least there has been a review of the costs and benefits of CDR in the banking sector.

The fact that 2 years into the CDR initiative, there are still only 13 accredited data recipients, and no published information about the number of consumers participating in CDR suggest there is as yet wholly inadequate evidence of the value of the scheme, either for individual consumers or even for the small business consumers whom the scheme is also designed to benefit.

There has been no credible evidence that CDR has resulted in meaningful competition in the financial sector. Absent robust action by the Australian Competition & Consumer Commission and Australian Prudential Regulation Authority to prevent dominant actors from acquiring potential competitors we consider that the benefits of the CDR scheme will remain unproven.

We urge the federal government to press 'pause' on its headlong rush to implement the CDR broadly across multiple sectors of the economy.

The accelerated implementation now being considered sets arbitrary deadlines (one new sector each year), without acknowledgement that this might be both unrealistic and undesirable.

Other reforms a higher priority

Further CDR implementation is also premature in the absence of some other regulatory reforms that are necessary pre-conditions. These include enhanced privacy safeguards that should emerge from the current review of the Privacy Act, and, in many sectors, improved disclosure requirements, long-overdue standardisation of definitions, terms and conditions, and enhanced sharing of product information.

Some of these other changes, which can and should be implemented independently of CDR, would directly enhance competition and are much 'lower-hanging fruit' than a complex, technically difficult and costly scheme to compel sharing of customer data which is of dubious benefit and carries many other risks.

Unacceptable Complexity

The benefits to consumers of Open Banking – the first manifestation of CDR – have yet to be proven. Progress in implementing CDR in the banking sector has been much slower than planned – partly because of an excessively complex scheme design which is proving difficult for consumers and businesses alike to understand and operate.

Implementation of CDR in banking has involved the invention of a completely new 'ecosystem' of interrelated entities and roles, with its own vocabulary of jargon and acronyms. It also envisages the creation of a set of 'apps' and interfaces, including 'dashboards' which individual consumers are supposed to use to indicate their preferences and intentions.

It appears that consumers will be expected to install and use separate 'dashboard' apps for each accredited data recipient (ADR) which asks them to authorise access CDR data about them from a data holder (DH). We submit that even if consumers can see 'in-principle' benefit in allowing this access, most are unlikely to be willing to climb the steep learning curve and devote the time required to make the scheme operate as designed, with each ADR.

Dubious claims that CDR is 'consumer-centric'

The government's continuing 'sales pitch' of the scheme as being primarily about consumer benefit ('consumer-centric') is a smokescreen.

The direct consumer benefit has already been significantly undermined by the deferral of direct access for consumers to their CDR data which was heavily promoted during the legislative process. Legitimate but predictable concerns about technical difficulties and security concerns have provided a convenient excuse for ditching of this major component of the scheme as originally envisaged.

This leaves the scheme as almost exclusively focussed on facilitating innovation and greater competition in different business sectors, as part of the Government's Digital Economy Strategy. While this may well have indirect benefits for consumers, it will also have disbenefits and risks. We do not accept, unquestioned, the assumption that more products, services and competition are an unqualified good thing for consumers. We reject the assumption implicit in the reference on p7 of the Consultation Paper to '…new data-driven products and services that improve consumer outcomes' – there may be some such, but equally likely are new products and services that exploit data to the detriment of consumers.

Based on experience, it is quite likely that greater complexity in some markets will just confuse consumers, with a risk that mandated data sharing will lead to significant disadvantage, discrimination or simply inconvenience. It is also likely to pose even greater risks for disadvantaged and vulnerable consumers. The Consultation Paper suggests that CDR offers opportunities to better support such consumers – we will be very interested to see if consumer representative groups can provide practical examples of use-cases which support this optimistic assessment – we fear the opposite result is more likely.

The increasing emphasis by Treasury on cross-sectoral sharing of CDR data compounds and re-inforces our concerns. It is far from clear how the increased complexity of consumers authorising simultaneous access to data holders in different sectors could be operationalised with the current Rules and Standards, which have been designed for relatively simple direct transactions involving one ADR and one Data Holder. Cross sectoral application of CDR would in our view inevitably require significant re-design of the scheme, with strict privacy and security safeguards likely casualties in pursuit of the primary innovation and competition objectives.

The Consultation paper flags increased government and business interest in cross-sectoral data sharing centred around 'life journey' events '… from cradle to grave', '… enabling third parties to identify the best products and services to meet consumers' needs…' (p15). While superficially appealing, the approach set out in the shaded box on p15 could all too easily morph into a dystopian future of 'we know better than you what you need', re-inforcing already disturbing trends in what has been described as 'surveillance capitalism'.

Safeguards largely illusory

The government asserts that many of the concerns we have repeatedly raised are addressed by the role of consent that has been embedded in the legislation and design of the scheme, and by the strong privacy and other safeguards.

These assurances are a cruel delusion. The sheer complexity of the CDR Rules and Standards already on display in the banking sector means that there is no realistic prospect of consumers being able in practice to exercise genuinely free and informed consent.

We note detailed criticism by scholars such as Huggins, Suzor and Burdon regarding the ambiguity of the CDR rules and the difficulty facing consumers, enterprises and courts who will need to make sense of the rules by reading across several technical documents that enshrine discretion for overlapping regulators and industry stakeholders.

The Consultation Paper envisages 'higher engagement' and 'informed decisions' by individuals (p16). We submit that this is unrealistic, flying in the face of years of experience.

We already know that most consumers simply 'click through' to obtain a product or service without even reading the privacy statements or policies to which they are implicitly consenting.

The CDR regime adds an additional level of information that it is assumed a consumer will consider before giving their consent to an ADR and data holder for exchange of their data. It seems highly unlikely that many consumers will be able to realistically engage at this level and much more likely that they will continue to simply 'click through' if presented with a superficially attractive service offering.

This existing problem will be compounded if the CDR continues to evolve (as it is in banking) in favour of more complex arrangements and authorisations, more use of 'trusted agents', replacing opt-in with opt-out to overcome low voluntary participation rates, and assumptions that parties to joint accounts can be assumed to consent to sharing CDR data.

Other ways of addressing unregulated data-sharing

Proponents of CDR assert that there are already large volumes of sharing of consumer data, sometime without the consumer's knowledge and sometimes with their knowledge but without consent. (Consultation Paper p17 and Consumer Roundtable 20 August 2021). This can involve inherently unsafe practices such as requiring consumers to provide their user-names and passwords, and 'screen-scraping'.

While we acknowledge that these undesirable practices are widespread, we submit that they can and should be addressed directly with other policy levers, and by better enforcement of existing regulations. The OAIC and ACCC could and should be devoting far more resources to monitoring and auditing data handling practices in the private sector for compliance with existing rules, in the Privacy Act and in other regulatory regimes.

The imposition of another layer of complex privacy and security safeguards specifically for CDR data is a clumsy and inefficient way of addressing a range of known problems in data-sharing, and for reasons we have already set out, may not even be effective.

CDR design counter-productive

There is a fundamental contradiction in the design of the CDR scheme to date. The elaborate framework of Rules, Standards and Privacy Safeguards requires a level of resourcing from intending business participants that is beyond the reach of most of the smaller 'new entrants' that CDR is supposed to encourage in pursuit of the increased competition objective.

Two different unintended consequences are likely – neither of them in the public interest.

The first is that the compliance overheads will actually favour large incumbent providers, increasing the barriers to entry and reducing competition. The second is that pressure will inevitably mount for relaxation of some of the requirements, standards and safeguards, as is already evident in the Open Banking context with current proposals for joint accounts and for so-called 'trusted third parties'.

Privacy Impact Assessment

If there is any future extension of CDR (if and when evidence of net consumer benefit is available), it should be also be conditional on a separate independent Privacy Impact Assessment (PIA) as part of any sectoral assessment, with publication of the PIA report sufficiently in advance of any designation decision to allow for proper consideration and further input.

While PIAs are essential, we are concerned that the two carried out to date by Maddocks only serve to compound the problems we have identified. The PIAs correctly identify many of the issues of concern. But their recommendations, as accepted and implemented in the Rules and Privacy Safeguards, are simply too complex to be workable in practice, and are unrealistic and potentially ineffective. As with so many aspects of the CDR scheme, there is as yet insufficient experience to judge, but we are very sceptical of the practical value of the consent provisions and other privacy measures.

Diversion of OAIC Resources

Alarmingly, OAIC has devoted significant resources to the CDR regime, at the same time as it has been starved of funding to perform its functions under its much more important and mainstream privacy jurisdictions including the APPs, Credit Reporting and Data Breach Notification. OAIC has

also been largely 'missing in action' on a wide range of new threats and important debates about cybersecurity and increased surveillance in both the private and public sectors.

While OAIC has received some additional funding for CDR work, the focus of the staff working on privacy and senior executives must inevitably have been diverted from its other jurisdictions.

It has been impracticable for APF and other concerned NGOs to keep up with the sheer volume of CDR related material emanating from OAIC. We seriously question whether more than 200 pages of Guidelines to the CDR Privacy Safeguards, recently revised without any explanation of the changes yet available, is in any way digestible either by the (few) CDR business participants expected to comply, or by the consumers the Privacy Safeguards are supposed to protect.

We further note the detailed analysis by Huggins et al in *The Legal and Coding Challenges of Digitising Commonwealth Legislation* submission to the Select Senate Committee on Financial Technology and Regulatory Technology Issues. We endorse that submission's comment that given the speed with which CDR is being rolled out:

> 'the courts have not yet reached definitive conclusions about, for instance, what different provisions mean, how they apply in certain cases or the scope of obligations. Importantly, even if a body of case law did exist, the nature of the common law system means that while similar cases will generally be treated alike, future cases with slightly different facts may trigger a reinterpretation of the law'

It is premature to significantly extend the CDR until there is agreement about the legality of the CDR rules and about whether the benefits claimed by the scheme's proponents are being achieved.

In particular extension is highly undesirable until the current review of the Privacy Act has been completed. Fast-tracking what is an essentially unproven scheme without a fit-for-purpose privacy regime is contrary to the experience of both the European Union (notably the General Data Protection Regulation) and the United Kingdom.

Our view is that extension at this time is likely to disadvantage consumers, regulators and industry through a need to either 'retrofit' rules to an updated Privacy Act (and other statutes) or to regard CDR as operating alongside the updated Act on an exceptional basis. The latter will result in uncertainty, litigation and distrust – regulatory friction and consumer disengagement that CDR is meant to avoid rather than exacerbate.

Conclusion

The Australian Privacy Foundation submits that **further extension of CDR into other sectors, including energy and telecommunications, should be put on hold until there has been a detailed independent assessment of the 'Open Banking' experience to judge whether, on balance, CDR is in the public interest, and until improvements have been made to the Privacy Act.**

Urgent need for funding of consumer input

Invitations to provide input to CDR strategic and sectoral assessments, and standards development, are only one set of a significant number of consultation processes underway across government in relation to Australia's digital landscape, including more than one specifically regarding the management, sharing and release of data impacting consumers.

The ability of policymakers to fully consider the benefits and risks of such reforms relies upon the ability for consumer organisations to participate in such processes. Businesses and Industry associations are able to devote significant resources to consultation processes. In contrast, most consumer NGOs struggle to respond even minimally to all the invitations they receive.

In light of the rapid transformation of the digital economy, APF urges the Australian Government to make provision to adequately fund consumer representatives to participate in these processes.

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policy Statements https://privacy.org.au/policies/
- Policy Submissions https://privacy.org.au/publications/by-date/
- Media Releases https://privacy.org.au/media-release-archive/
- Current Board Members https://privacy.org.au/about/contacts/
- Patrons and Advisory Panel https://privacy.org.au/about/contacts/advisorypanel/

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) https://privacy.org.au/about/history/formation/
- Credit Reporting (1988-90) https://privacy.org.au/campaigns/consumer-credit-reporting/
- The Access Card (2006-07) https://privacy.org.au/campaigns/id-cards/hsac/
- The Media (2007-) https://privacy.org.au/campaigns/privacy-media/
- My Health Record (2010-20) https://privacy.org.au/campaigns/myhr/