Deloitte.

Where to now?

The future for the Consumer Data Right

September 2020

In the next few weeks Scott Farrell is scheduled to deliver to the Treasurer the results of his Inquiry into Future Directions for the Consumer Data Right (CDR). To help organisations anticipate how the CDR may evolve, in this paper we summarise the key points noted in the submissions that were made public, including Deloitte's.

This was not straight forward. The inquiry received 73 submissions (two confidential), over 800 pages in total, containing a diverse, and often conflicting, range of observations, comments and recommendations.

For context, in January 2020 Scott Farrell was asked to conduct an Inquiry into Future Directions for the Consumer Data Right. This followed his report in December 2017, 'Open Banking', that set out the design considerations for Australia's Consumer Data Right. Farrell's 2017 report had anticipated the Inquiry and even set out post-implementation issues for it to consider.

However, Farrell had also recommended that open banking be formally evaluated ***12 months after*** it had commenced for banking. Given that open banking will not be fully implemented now until February 2022, some have argued that this Inquiry is being conducted almost ***two years before*** the full commencement of open banking.

Expand, consolidate or terminate?

Over ninety percent of the submissions supported the CDR to some degree. But the view was almost evenly divided between those advocating expanding it now, and those who wanted to consolidate the current position.

Expand

A common theme in those wanting to expand the CDR was the transformative role that data could play in enabling 'a broader, more integrated, and more consumer-centric delivery of Australia's digital economic strategy'. Data was seen as 'the single biggest lever for micro-economic and social reform in the next two decades' and data sharing as part of 'the foundational information flows of the digital economy'.

Submissions supporting this view argued that the CDR should be expanded to apply to all personal information which is collected from consumers, noting that a large amount of personal data is not subject to the CDR regime. This included for some, the extension of the CDR to include data that citizens share with government.

Another theme was the role that innovation and competition enabled by the CDR had in delivering benefits to consumers. Submissions noted that greater volumes of consumer data from across industries would provide greater incentives for consumers to participate in the CDR, along with 'transformative opportunities' from aggregating data from across various sectors and sources.

One submission captured this by noting that the CDR was a 'world-leading data policy initiative' when it was announced in 2017, but cautioned it 'now risks losing its global relevance' as a result of delays to its implementation and its slow expansion.

This 'expansion' view would see Australia's CDR regime encompass a broader range of data rights, and move closer to the European Union's General Data Protection Regulation (GDPR).

In these submissions, the current COVID-19 crisis was seen as a reason to ***accelerate*** the implementation of the CDR and the move to a digital economy.

Consolidate

Another group of submissions noted that while they supported the CDR in principle, it was too soon to expand its functions or the sectors to which it applied. Submissions supporting this view argued that the current position, what they called the 'establishment phase', was critical to building trust in the CDR and establishing 'operational experience'.

One noted that many jurisdictions have underestimated the complexity and scale of open banking implementation, with another expressing concerns that the CDR would struggle to scale across industry sectors.

This 'consolidate' approach was seen to have the added benefits of allowing the results of the full implementation of open banking to be assessed, and providing time to complete an analysis of the costs and benefits from extending the CDR to other sectors.

For this group, the current COVID-19 crisis was seen as a reason to ***decelerate*** the adoption of the CDR and delay its extension to other sectors.

Terminate

A third, smaller group, argued that more analysis was required of alternatives to the CDR, including market-based alternatives. Some questioned the costs of a regulatory-based approach, noting that the behavioural barriers to switching did not apply in other sectors and that the costs would outweigh any potential benefits for consumers. One submission summed up the CDR as 'a solution looking for a problem'.

Regulatory Framework

One of the challenges of building a framework for a digital economy is that the regulatory responsibility is spread across several different regulatory agencies and government departments. This is amplified as the CDR is extended to other sectors.

Submissions commented on the alphabet soup of regulatory agency acronyms with responsibility for some aspect of the digital economy: in addition to the ACCC, DSB and OAIC regulating the CDR other regulators include ASIC, APRA, AUSTRAC, ATO, AEMO, DTA, NPP, Home Affairs and more.

There was a wide range of suggestions on how to address this.

Some called for the establishment of a single regulator to provide a single point of accountability. This has been echoed by the interim report of the Senate Select Committee on Financial Technology and Regulatory Technology, released at the beginning of September, which has pre-empted Farrell's report by recommending that a new national body be established to consolidate regulatory responsibilities in relation to the CDR's implementation (Recommendation 19).

Others rejected this, arguing that no single regulator would be able to fulfil all the regulatory functions needed to support the specific requirements of different industry sectors or the broader data economy needs.

In between there were calls for a co-regulatory approach, greater self-regulation, and greater coordination amongst the regulators.

Irrespective of which approach is adopted, when establishing the regulatory framework for an economy-wide reform, it will be important that the regulators have both the funding and the human resource capability to enable this to be delivered.

Write Access

The ability to initiate payments and to open and close accounts is referred to as write access. Unlike in other areas, such as the EU and the UK, Australia's CDR is currently based only on read access (data sharing) and does not include write access. The original Farrell report noted both the increased risk associated with write access, and the payment initiation capability from the New Payments Platform, and recommended deferring the implementation of write access as part of the CDR until read access was implemented in banking and in use for a sufficient amount of time. This was seen as having the added advantage of allowing consumers to build trust in the CDR framework.

However, several organisations have advocated fast-tracking the implementation of write access in Australia.

As a result, consideration of how the CDR could be expanded beyond the current 'read' access to include 'write' access was a 'key focus' set out in the Issues Paper to the Inquiry.

Opinion was divided here as well. Almost three-quarters of submission supported the introduction of write access.

Of these a little over half thought write-access should be introduced now, with one seeing it as 'the top priority' for the future of the CDR. Write access was seen to address several of the behavioural biases which limit switching. However, the importance of concurrently introducing a 'best-interests' duty for anyone seeking to use write access was also noted.

The support of the others was more lukewarm. They were supportive in principle but concerned with the complexity and material risks of introducing write access into Open Banking. Some in this group thought that read access should be bedded down before embarking on write access. Others that the NPP should be used for write access in payments to avoid duplication. A slower implementation was also seen as providing more time to implement digital identity, electronic contracts and improve data security and fraud controls.

The remaining group, about a quarter, did not support the expansion of the CDR to include write access at all. This group focused on the risks and costs of write access and questioned the benefits.

Intermediaries and tiered accreditation

In June 2020 the ACCC published draft rules which would allow an accredited data recipient to engage the services of another accredited person (a third-party intermediary) under a 'combined accredited person' (CAP) arrangement. The draft rules were published following submissions on the ACCC's consultation paper published in December 2019. The introduction of intermediaries as a class of CDR participants could allow the creation of lower tiers of accreditation.

Because submissions had only just been made to the ACCC on intermediaries, the topics of tiered accreditation and the role of intermediaries were not covered in as much detail in submissions to the Inquiry.

In general, both tiered accreditation and a role for intermediaries were supported. Tiered accreditation was seen as essential if write access was introduced. However, there seem to be different views, even among those supporting tiered accreditation, on how this would work with some arguing that it would be important that minimum standards were still maintained on security, privacy and consent.

The Senate Select Committee interim report has recommended that the roles for intermediary and third-party access to CDR banking data be finalised by late 2020 (Recommendation 20).

Sector Application

The Issues Paper noted that the Inquiry would not focus on the expansion of the CDR to specific new sectors. Notwithstanding this, many submissions provided input on this. To say these views were diverse would be an understatement.

The expansion from open banking to open finance, now underway in the UK, was a theme for many. There were calls for the CDR to be implemented in insurance, investments and superannuation; and for access to this data by mortgage brokers and financial planners. This has also been echoed in the Senate Select Committee's Interim report, which has called for the CDR to be extended to other financial services sectors, starting with superannuation and then including sectors such as general insurance (Recommendation 23).

Some argued that open banking should go further to allow organisations to use data shared under the CDR to meet regulatory requirements for responsible lending and credit risk assessment, something which can currently be done with comprehensive credit reporting (CCR) data.

Energy was still a contested sector. The government announced over two years ago that energy data would be included in the CDR. The ACCC published a position paper on the data access model for energy data in August 2019 and launched its consultation on the rules framework for the energy sector in July 2020. Notwithstanding this, while some submissions supported this process – noting that CDR would bring significant benefits to the energy sector – others were still debating whether this was needed and called for further research and consultation to confirm that there would be material benefits.

Submissions also discussed the expansion of the CDR to other sectors of the economy.

The CDR should be extended to travel and leisure sectors said one submission. But another noted that the potential expansion of the CDR to the aviation sector should not progress in the short-to-medium term.

One argued that CDR was not needed in the retail sector, while another, perhaps with a better understanding of the power of the data captured by loyalty schemes (which has also been noted by the ACCC) argued that it should be extended to grocery stores.

Some, interestingly, highlighted the amount of telematics data currently captured by cars – location data, personal communications, driving habits, service history – with one pointing out that today's cars use the equivalent computing power of 20 personal computers to process up to 25 gigabytes of data per hour.

Some submissions argued that the CDR should avoid a sector-specific approach altogether, and pivot to a consumer focus. A sector specific approach was seen to be potentially creating barriers for new entrants. Another highlighted that location data was the most valuable data element and that the CDR should be amended to focus on requiring this data element to be shared.

Others took the opposite view and noted that because each sector had unique characteristics, opportunities and challenges, a sector-based approach was required.

Privacy and Consent

Privacy

Several submissions noted that the CDR's privacy requirements duplicate the general privacy requirements set out in the Australian Privacy Principles (APPs), creating complexity and compliance costs. The Inquiry was seen as an opportunity to re-assess this.

Others went further, noting that Australia's existing regulatory framework for the collection, use and disclosure of user data and personal information resulted in unanswered questions that go to the fundamental rights of individuals to control data held about them.

They pointed to the findings of the ACCC's digital platform review: that the current privacy framework does not effectively deter data practices that exploit the information asymmetries and bargaining power imbalances between digital platforms and consumers.

Some submissions highlighted that the expansion of the CDR across the economy required centralised rules on how companies handle consumers' data. They saw the CDR as providing an opportunity for centralised legislation. Some concluded that this required Australia to adopt the GDPR as a minimum.

Others introduced a note of caution that an excessive focus on privacy could stifle innovation. Some highlighted the 'privacy paradox' in which people's expressed preferences for privacy do not align with how they behave in practice where people are willing to share information if they receive value in exchange.

Consent

A majority of submissions supported the development of an economy-wide model for consent, a consistent consent taxonomy. Some saw it as a critical infrastructure layer for data sharing which would empower consumers and provide an incentive for them to adopt the CDR.

However, several submissions pointed out that getting to an agreed consent model which was consistent across sectors would present 'a significant challenge'. What will happen to existing consent processes which are already being used? How will consumers understand consent when they are providing multiple consents across a range of data holders and data recipients from multiple sectors?

The potential complexity this creates, and the challenges for consumers to actually understand what they have consented to, in order that consent is truly informed, had already been flagged during the standard setting process.

Some submissions thought this challenge would prove too difficult – that the outcome for successful consent was more important than defining standardised language. In this view any consent taxonomy should be non-mandatory with providers able to determine for themselves how best to implement consent collection.

This prompted a proposal that there should be a consolidated single consent dashboard, with consent becoming designated shareable data. One submission perceptively pointed out that in the absence of this, the complexity of re-establishing multiple consents could inadvertently become a new barrier to switching.

Digital ID

In Deloitte's submission we noted that 'in our digital society, trust is determined through digital identity—the corpus of data about an individual, an object, or an organization that helps identify them through unique qualities and use patterns.' This was echoed in other submissions, with one noting it was 'a foundational capability which is currently absent from the Australian landscape'. Others noted that a digital identity platform, when combined with the CDR, had the potential to create significant consumer benefit.

Views were more evenly divided on whether or not organisations should share the outcome of an identity verification assessment, if directed by the customer to do so. Some argued for just the outcome to be shared, others for key fields such as date of birth and KYC status to be designated data. But others noted that this should not form part of the CDR and should remain part of the AML/CTF framework.

Consumer Protection

As we highlighted in our report Open Banking: Switch or Stick?, trust, along with value, is one of the key ingredients for consumer engagement with data sharing. Consumer trust in information sharing is also an enabler of a healthy digital and data-based economy. This sentiment was echoed in several submissions, with calls for consumer protection to be 'at the centre of the CDR regime'.

Consumer protection is enhanced where they understand how to use data sharing and the value they can realise. Several submissions called for a comprehensive consumer education program, supported by 'active participation and engagement' by existing data holders. Establishing and implementing consumer education was also a recommendation in the Senate Select Committee's interim report (Recommendation 21).

Some submissions noted that the growth of the digital and data economy will raise a broad range of consumer issues which should be addressed in building the foundation for a digital and data economy. These included financial literacy, data literacy, data and AI ethics, AI and algorithmic bias and even access to technology.

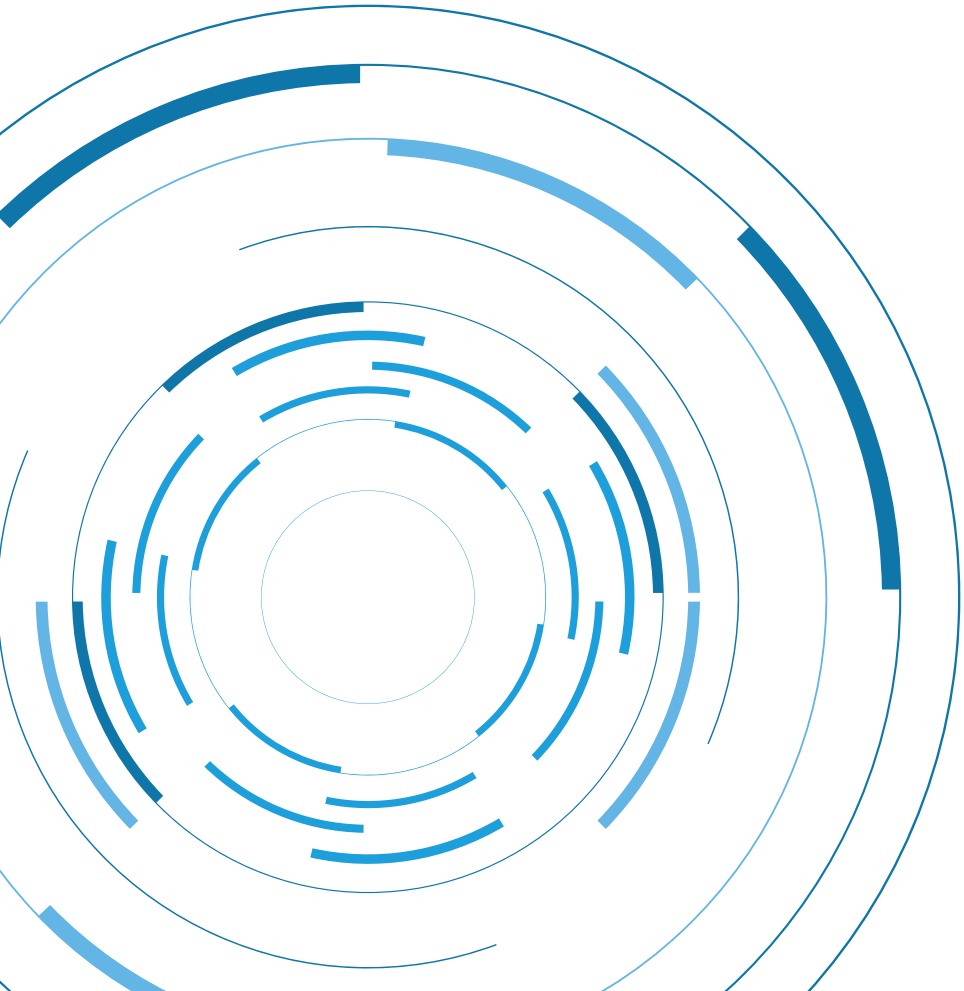
Others noted that existing consumer protection obligations, particularly with respect to vulnerable customers, need to apply to all participants, something that is strangely missing from the fast-growing buy-now-pay-later service offerings.

This was amplified in submissions which recommended 'urgent economy-wide reforms to outdated protection frameworks' noting the recommendations made in the ACCC Digital Platforms inquiry.

International Standards

The broadest consensus in the submissions was that where it makes sense to employ common international standards, Australia should do so, and that more could be done to strengthen international cooperation and inter-operability. There were calls for: common technical standards with the UK, EU and Singapore; a common approach to consent management with similar jurisdictions; and passporting of third-party providers accredited in countries with similar requirements.

As one submission noted, Australia has an opportunity to act as an international leader to create a more competitive and innovative digital economy.



Key considerations

The Consumer Data Right legislative framework is complex with legislation, rules, standards and designation instruments. As one submission noted, the current 'legal and regulatory framework has developed in a staged approach, as regulators and governments have sought to address the regulatory and legislative challenges as they arose.' This has been informed by over a dozen issues papers, inquiries, consultations and reports.

Towards a digital economy

As Deloitte and others have noted, although titled a Consumer Data Right, the CDR is actually only a consumer ***data sharing*** right. The ACCC's reviews of Digital Platforms and Customer Loyalty Schemes have highlighted that consumers have little meaningful control over how their data is collected, used and disclosed. This issue will only increase as we move further towards an economy incorporating the Internet of Things.

Organisations should be ready for a future in which the framework for a digital economy includes a legislative framework over how data is collected and used as well as shared, and could include rights over data on individuals held by government agencies.

Such a future is likely to be supported by a national framework for digital identity, electronic contracts, an enhanced legislative framework for AI and analytics, a renewed focus on an effective privacy framework and updated consumer protection.

AI, algorithms and analytics

AI is already giving rise to new ethical dilemmas, particularly in relation to considerations of fairness. The heightened ethical responsibilities for use of data include how data is interpreted via algorithms. This requires an understanding of unintended consequences and potential biases in algorithms.

While the government has published voluntary AI Ethics Principles, it is not clear, as one submission noted, that 'ethics alone would be enough to ensure accountability for AI design and use as well as for adverse outcomes.'

In preparing for a digital economy, the regulatory framework for AI, algorithms and analytics is likely to be developed in parallel with the CDR. Organisations should be thinking now about how this could impact their business.

A more holistic and comprehensive approach will be needed, which includes improvements in the way models and algorithms are developed, tested and deployed, in addition to the operating model changes that would provide consumers with an ability to challenge or seek recourse on decisions which they believe are unjustified.

Privacy and consent

Privacy becomes increasingly important as a broader range of data is collected and shared.

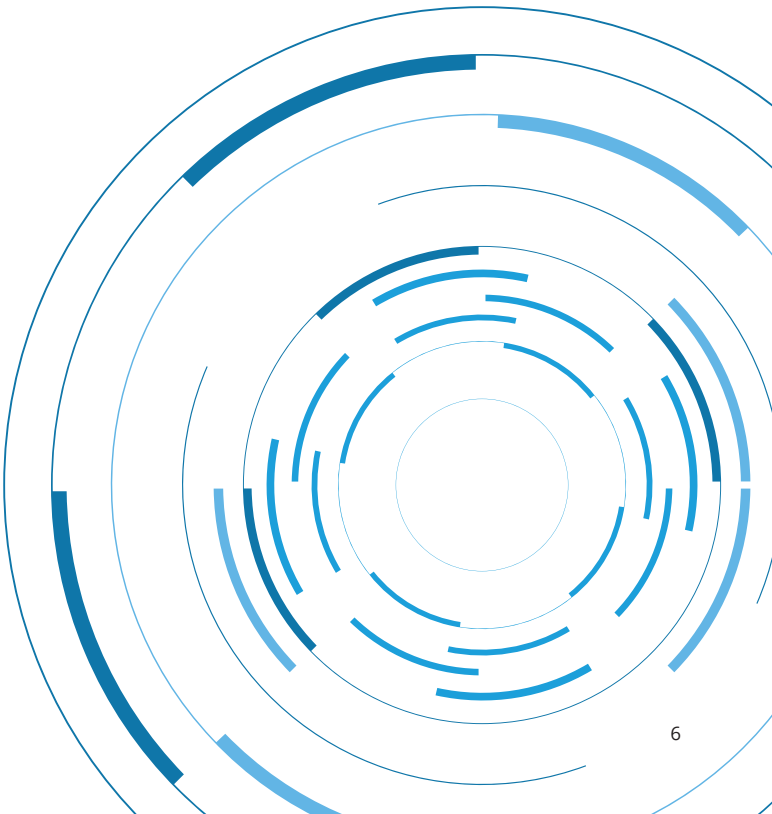
The ACCC digital platform inquiry highlighted that the term 'privacy policy' was a misnomer as these policies 'tend not to outline privacy protections for users but rather tend to set out the extent of permissions granted to digital platforms'.

Insights from the Deloitte Australian Privacy Index 2020 also demonstrate the growing difference between consumer expectations and current consent practices across a range of industries, due in part to the absence of strengthened privacy requirements. For example, the Index found that only 21% of Australia's top 100 consumer brands had provided consumers with a comprehensive consent management portal or equivalent, and that only 7% of consumers said they had a very good understanding of how their personal information would be used after they consented to its use.

As we move towards an open data economy it will be important that privacy policies do not have the same fatal flaw that some 'client protection' policies were shown to have during the Hayne Royal Commission, when they were described as 'Orwellian' and 'entirely misleading'.

The ACCC recommended that the Privacy Act needed to be reformed 'in order to ensure consumers are adequately informed, empowered and protected, as to how their data is being used and collected.'

As we move towards a digital and data economy, organisations should prepare for reforms to privacy legislation which strengthen Australia's data rights and data protection, and more closely align them with those set out in the EU's GDPR regime.



Consumer Protection

One thing that was crystal clear from the Hayne Royal Commission was that the actions of today will be judged by the standards and community expectations of tomorrow.

Organisations need to be anticipating how the move towards a digital and data economy will impact potential conduct considerations of fairness, transparency, vulnerability and suitability. They will need to consider how write access could impact their obligations to act in the best interest of customers. They will need to understand how they prevent AI introducing unintentional algorithmic bias.

And they will need to decide their role in supporting the development of digital and financial literacy and consciousness in their customers.

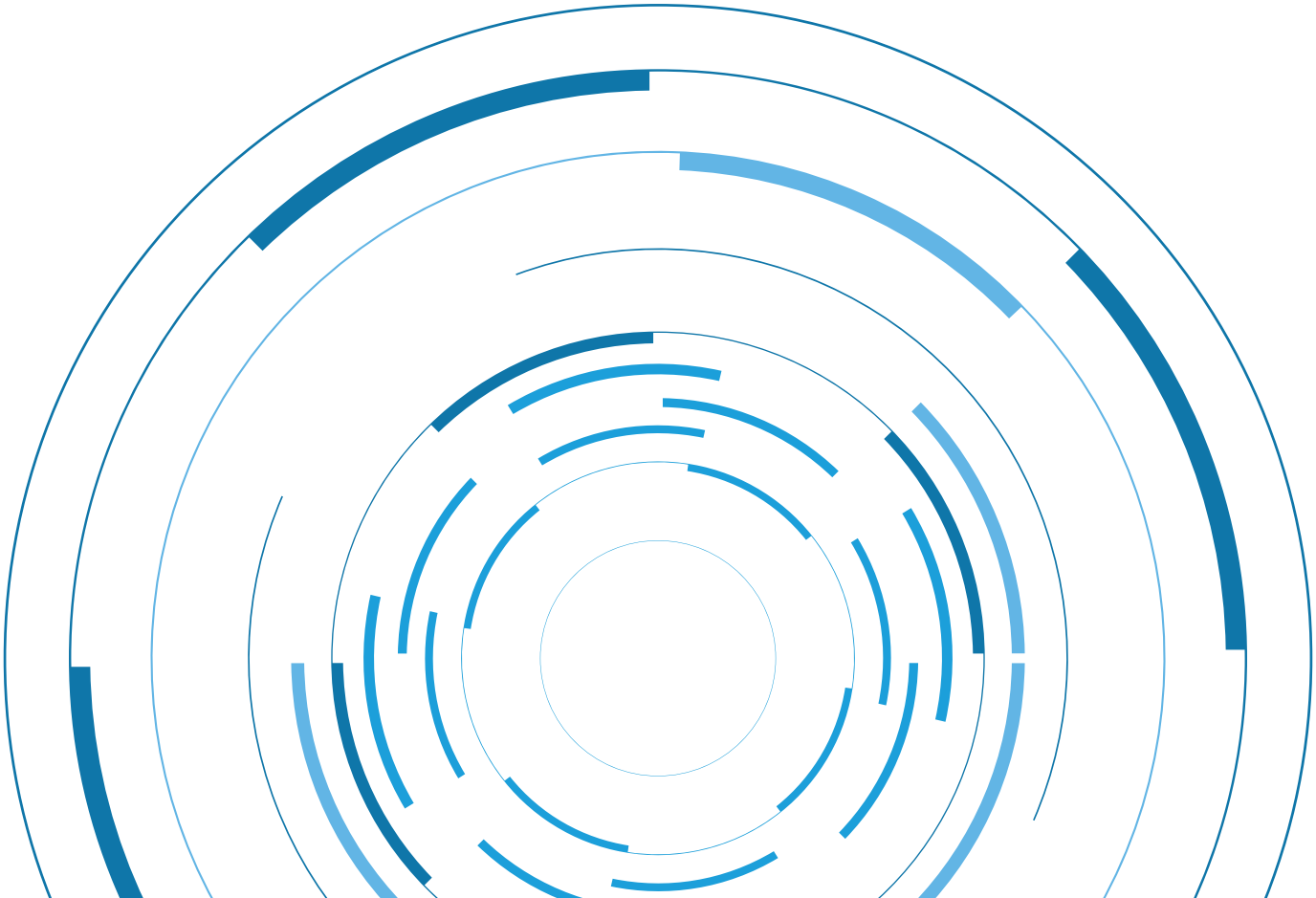
Last word: Where to now?

In the journey towards a digital economy, data rights and data sharing will play a crucial role. The journey towards data sharing has started, and, although its start has been slow with, so far, only two accredited data recipients, its growth has the potential to be exponential, a concept with which we are all now much more familiar.

Within a few weeks we will know the outcomes of Farrell's Inquiry. But organisations should be thinking about data and data sharing as more than just a compliance requirement. Those that thrive will be the ones who see the potential that data provides for new services and products which create value for consumers, whether created by them or through an ecosystem, and are agile enough to make the changes.

Read Deloitte's submission to the Inquiry into Future Directions for the Consumer Data Rights

Visit our website to access Deloitte's Open Banking Survey of consumer behaviour and other articles on a range of related topics including payments, data architecture, analytics and AI, APIs, privacy, pricing, conduct and financial crime.



Contacts

Paul Wiebusch
Open Data Lead Partner
PWiebusch@deloitte.com.au
+61 3 9671 7080

Alon Ellis
Partner, Strategy & Pricing
alellis@deloitte.com.au
+61 3 9671 6381

Ally MacLeod
Partner, Risk Advisory
amacleod@deloitte.com.au
+61 2 9322 7499

Daniella Kafouris
Partner, Data, Privacy and Security
dakafouris@deloitte.com.au
+61 3 9671 7658

Tim Ellis
Director, Payments Assurance & Advisory
timellis@deloitte.com.au
+61 403 923 439

Tim Davis
Director, Customer
tdavis2@deloitte.com.au
+61 3 9671 5585

Melissa Ferrer
Partner, Data Modernisation
meferrer@deloitte.com.au
+61 2 9322 7844

Deloitte.

Designed by CoRe Creative Services. RITM0541678