CONSUMER DATA RIGHT

Applying initially to the banking sector, with the energy and telecommunications sectors expected to follow, the Consumer Data Right (CDR) will allow customers to access data on their own consumption of goods and services. This will enable consumers to direct custodians to share their data with third-party entities. It's anticipated that the implementation of the CDR will significantly increase competition between businesses and could potentially be applied economy-wide. The CDR regime imposes significant obligations with respect to privacy. In-house counsel working for businesses that hold consumer data should consider the impact of the new regime on their business operations and how they should prepare for the new data privacy landscape.

The Consumer Data Right (CDR) was established through amendments to the *Competition and Consumer Act 2010* and the *Privacy Act 1988*.[1] The Murray, Harper, Coleman, and Finkel inquiries all recommended that Australia develop a right and standards for consumers to access and transfer their information in a useable format. The 2017 Productivity Commission report, *Data Availability and Use,* made 41 recommendations, including for the creation of a new economy-wide Comprehensive Data Right. Subsequently, on 26 November 2017, the Australian Government announced the introduction of a CDR in Australia. The CDR legislation was passed in August 2019. The CDR operates under a multi-regulator model, comprising the Australian Competition and Consumer Commission (ACCC), the Office of the Australian Information Commissioner (OAIC) and a new Data Standards Body.[2]

The CDR intends to improve the ability of consumers to compare and switch between products and services, while encouraging competition between service providers.[3] It will give consumers the right to safely access data about themselves held by businesses and be able to direct that this information be transferred to accredited and trusted third parties of their choice.[4] At its simplest, the CDR involves three parties — a consumer, a data holder (which holds the data about the consumer), and a data recipient (which is both trusted by the consumer and accredited to operate as a data recipient).

By exercising the Consumer Data Right, the consumer directs the data holder to make the data held about them by that holder available to the data recipient. There is no obligation on the consumer to request a data transfer—it is an entirely voluntary process. Value is generated if the offer made by the data recipient to the consumer is accepted.

The main objectives of the CDR are that it is consumer-focussed, encourages competition, creates opportunities for businesses, and ensures the security and protection of consumer data.

In the first sector designated to implement the CDR, banking, the regime is referred to as "Open Banking" and initial product reference data, including interest rates, application fees, other fees (i.e. not consumer data) applying to all credit and debit cards, deposit and transaction accounts, were able to be accessed in July 2019 voluntarily by the big four banks. Banking consumer data, such as the customer's own income and payment transaction data, are expected to be made accessible by accredited data recipients with consumer consent under the CDR in February 2020. All other banks will follow suit in July 2020. The energy and telecommunications sectors are expected to follow suit in future.

While the CDR presents a range of opportunities for consumers and businesses, it also presents a range of legal obligations and commercial opportunities for businesses. In-house legal departments will be required to play an increasingly proactive role in, firstly, mitigating those risks for their organisation and, secondly, ensuring they are positioned to prosper in the post-CDR landscape.

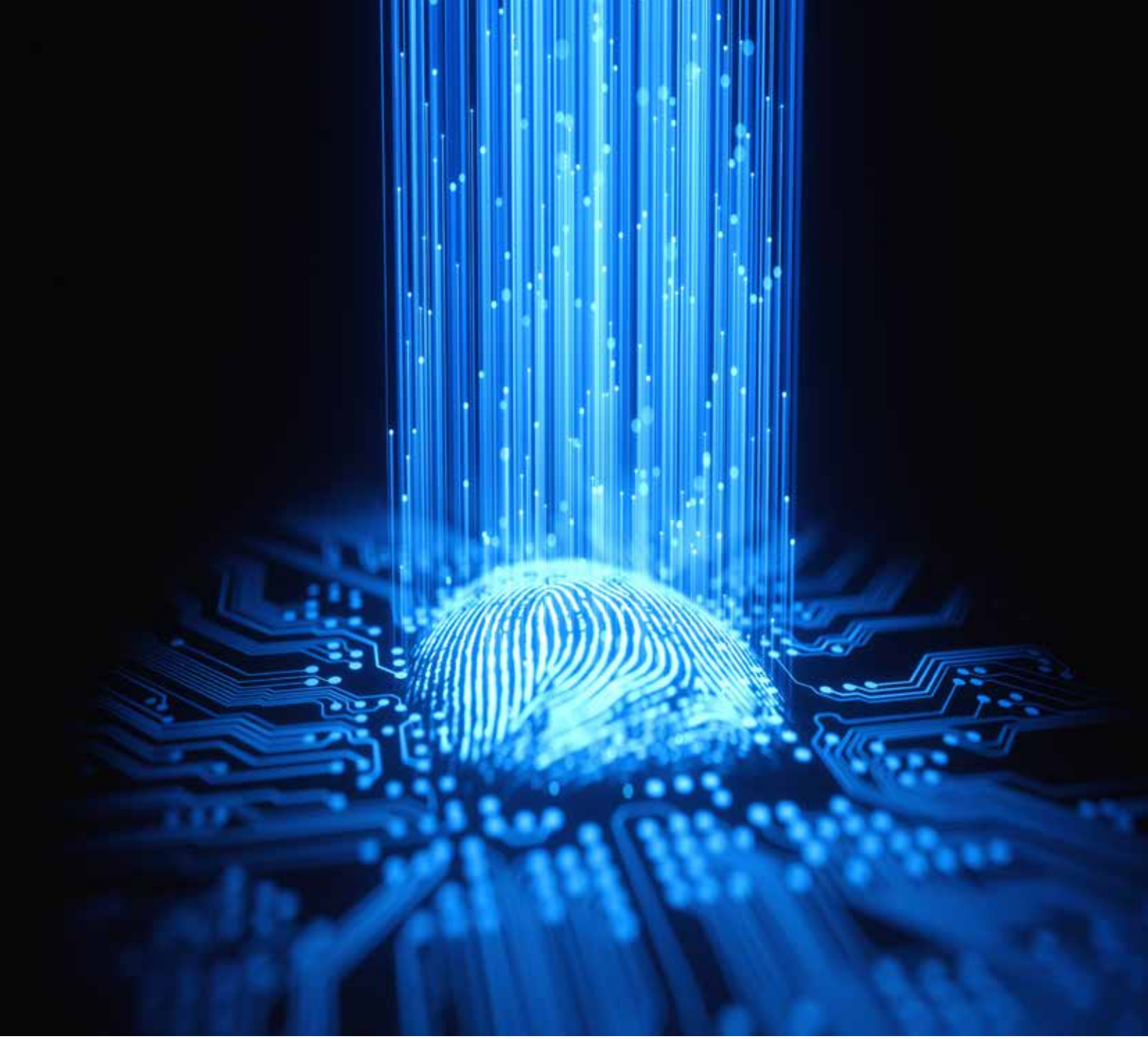
Implications for consumers

A common challenge for consumers across a range of sectors is to have sufficient access to information that enables them to make informed decisions. Often the details of products and services can be difficult to understand and, to make the best decision for themselves, consumers rarely have either great visibility of their own historic spending and consuming behaviour, or the ability to interpret those patterns of behaviour.

The CDR aims to give consumers control over information about themselves, initially in banking, energy and telecommunications, and enable the sharing of that information with trusted, accredited third parties. This could support the consumer in obtaining superior offers in terms of products, services or prices and also in comparing prices and benefits between different services, almost certainly to access lower priced offerings.

Importantly, the CDR is supported by a set of rules and technical standards that support the content, access and interoperability of the data transfer systems. These rules (developed by the ACCC) and standards (developed by the Data Standards Body) ensure consumers are appropriately serviced and protected when exercising their Consumer Data Right.

A major element of the Consumer Data Right regime is the requirement for the consumer to exercise an informed, explicit and complete consent to the data transfer. This is a significant aspect of the CDR reform and will improve the security of consumer data because it requires the consent of the consumer to the uses and transfers of their data. It will also require businesses to inform consumers about the disclosure of data to third parties.[5] The CDR establishes privacy safeguards, which will



be enforced by the OAIC. These safeguards provide consumers with avenues to seek remedies for breaches of their privacy or confidentiality, and also establishes obligations to provide anonymity and pseudonymity to consumers and destroy or de-identify redundant data.[6]

Implications for companies holding the data

The primary rationale for this significant policy change is that currently the value of data is at a micro level, and businesses that hold these data, whether an individual's energy company or financial institution, are monetising that data; hence, the value that is able to be derived from that information accrues to those various companies and institutions.[7] These companies currently monetise these data in various ways; they can sell it; they can use it for targeted advertising; and they can derive insights from the data that consumers are unable to access.[8]

CDR will not only allow businesses to make superior offers to consumers in terms of price, value, and customisation but create new market opportunities arising from the data they will be sharing and receiving. For example, Budgeting and Personal Financial Management use cases will be offered. In addition, it is expected that some customers will be offered lower-cost loans and credit cards because of their specific transaction data and what these data show about them. Once Energy and Telecommunications join Banking as designated sectors, offers that are based on specific consumer data from the three sectors are expected to form the basis of offers rarely seen by Australian consumers. An example here would be for a financed, solar-panel offer, which matched the customer's energy use and their financial standing, to customise the capacity and price to the specific customer — using banking and electricity consumer data.

The multi-sector offers are expected to become commonplace within 5–10 years and demonstrate the difference between an "Open Banking" implementation and an implementation of an economy-wide Consumer Data Right.

Since privacy is a principal concern for both consumers and businesses, organisations must also consider their approach to ensuring compliance with the privacy requirements of the CDR regime. This approach includes deciding whether attempts will be made to segregate CDR data from other data, such as personal information to which the Privacy Act continues to apply, or whether to follow the more burdensome but risk-averse option of managing both CDR data and personal information in accordance with the higher standards prescribed by the Privacy Safeguards.[9]

What should in-house lawyers do to prepare their organisations for the CDR?

As designated CDR 'data holders', Australian based banks will become the first organisations to become legally required to share customer data under the CDR. In-house teams within the banking sector will (or should) already be actively assisting in preparing their organisations for the CDR. In the case of my organisation, a non-major bank, a significant project is underway to ensure that we will be able to comply with a series of CDR related deadlines, with the first significant milestone being February 2021. By this date, we will need to have the systems and processes in place to be able to share our customers' transaction account data with accredited persons in compliance with the Open Banking rules and standards (the major banks will have had to have complied with this obligation by July 2020).

The ACCC has already begun the process of consulting with the energy sector on CDR, so legal teams advising for energy companies - as well as lawyers for companies seeking to disrupt or profit from the data held by energy companies - should already be alive to advising their organisations on the potential obligations and opportunities that CDR presents. As the CDR will subsequently apply to the telecommunications sector, in-house counsel for potentially impacted companies will no doubt also be keeping a close watch on developments in the CDR.

However, it's important for in-house lawyers in all businesses to keep an eye on developments in this space (you can sign up to the ACCC's consumer data right newsletter on their website to receive updates and to learn of any planned public consultations, and how your organisation can make submissions). The Federal Government expects that the CDR will lead to increased competition and innovation across the economy as a whole, and as such intends to eventually roll out the CDR across all sectors. Aside from the potential compliance implications, there may be new commercial opportunities that the CDR may present to your organisation that the business should be alert to. For those organisations who decide to voluntarily seek to participate in the CDR regime, their lawyers should expect to be involved in assisting with an involved accreditation process.

If, and when, it comes time for your organisation to begin preparing for the CDR, it's important to realise that compliance with the CDR requirements will involve a complex and expensive implementation project. You should expect that at least 90% of the cost and effort of such a project will involve building the required IT systems. To ensure success, your organisation should build a strong project team, preferably with regulatory experience.

While the CDR rules will vary from sector to sector, if the Open Banking experience is anything to go by (although the Government has seemingly chosen the hardest industry to begin its CDR experiment with) they will be complex and difficult at times to interpret. One of the key tasks of in-house counsel at the outset of your organisation's CDR implementation project will be to work closely with the project team to assist them to translate the relevant CDR Rules into a workable Business Requirement Document, which they will use to build the necessary systems, interfaces and security solutions to support CDR.

With the IT build underway, the legal focus will shift to uplifting other areas such as: updating product documentation, terms and conditions and other collateral; developing CDR specific complaint resolution procedures and advising on training requirements. Another key focus for lawyers will be on updating privacy related policies and procedures in order to comply with the OAIC's Privacy Safeguard Guidelines for the CDR, which at the time of writing, has been issued in draft form for consultation by OAIC.

George Nguyen, Senior Legal Counsel at Rabobank

Impact on in-house legal departments

The introduction of the CDR will have a significant impact on in-house legal teams, initially within the banking, energy and telecommunication sectors and potentially others, as the CDR applies economy wide.

At a fundamental level, businesses need to consider whether the CDR will affect their existing processes around the collection and use of customer data. While there is uncertainty and the rules of play are still being defined, by participating and innovating in a customer-centric data sector, in-house counsel are able to generate growth and opportunity for their business. However, the challenge will be how this change is accepted and the implications will be in looking at what data are currently held and the degree to which consent has been sought to hold that data.[10] Where consent cannot be informed or where a power balance exists, the changes will have a massive impact on in-house counsel to mitigate these risks for their business.

If in-house were to check the data being held and the utilisation of that data, it will come to light that a few companies will not have received explicit consent for the use of that data. There are two approaches that in-house counsel can take: firstly, a "comply" mentality, which addresses the issue of identifying shortfalls in data security and application and identifies weaknesses or shortfalls in current practice;[11] alternatively, in-house counsel can take a "compete" mentality and ask, what opportunities can we take advantage of here?

Legal departments play an important role in risk mitigation against internal and external threats that will potentially divert the organisation from achieving its strategic and operational objectives. In relation to the CDR, clear data strategies should be implemented to mitigate risk, or else corporations can be at risk of non-compliance. The penalties are serious, being up to $10 million for businesses or 10% of the annual turnover of the organisation. This far exceeds the current penalties under the Privacy Act, which have an upper limit of $2.1 million. Corporations may also be penalised for misleading conduct relating to the transfer of CDR data or breaches of new Privacy Safeguards. Complying with legal requirements and adopting clear strategies to mitigate risk are instrumental in protecting a company's reputation.

There are five steps that can position in-house counsel to take advantage of the CDR regime:	
1	Understand the legislation, rules and data standards and consider the implications for their organisation of their application in their sector/s.
2	Consider the nature of consumer data being held by their business and the nature of consents that have been obtained from consumers for the storage and use of that data.
3	Anticipate the impacts of the CDR in their sector and consider "early adoption" of advanced consent arrangements relating to the consumer data being held.
4	Work with the business to consider "use cases" and potential offers that could develop when the CDR is designated in their sector, and identify other sources of consumer data (in other businesses and other sectors) to enrich this work.
5	Work with the business on preparations to operate as an accredited data recipient (customer segments, channels, systems and organisational implications) to apply a compete mentality. Consider also the accreditation criteria and the business's current ability to satisfy the requirements.[12]

Each form of data raises new challenges and, with the CDR taking shape, it is vital, now more than ever, to not only maintain consumers' trust about the stewardship of data but ensure that the reputations of businesses are protected.

Conclusion

CDR is the foundation of a formal, consumer-driven exchange of data throughout the economy. This private, secure and consented regime facilitates increased sharing and ensures enhanced privacy and security of consumer data. The Government is working towards ensuring consumers are prevented from unfair price discrimination and problematic targeting by marketers and advertisers using CDR-obtained data. In the meantime, in-house legal departments must be ready to play a proactive role in pursuing the opportunities and mitigating the risks that are likely to arise from the CDR regime. Many of these opportunities and risks will be commercial in nature.

Footnotes

1. Australian Government, *Consumer Data Right Overview,* September 2019 <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf> p. 9.
2. Ibid.
3. Andrew Stevens, Danny Gillian, Jamie Twiss and Stephanie Gray, *The Consumer Data Right.*
4. Ibid, p. 1.
5. ACAN, *Consumer Data Right — What Is It and What Does It Mean for Consumers?* September 2018.
6. Coors Chambers Westgarth, *Australia Builds Its Open Data Economy: Consumer Data Right Passes Parliament,* August 2019.
7. Ibid.
8. Ibid.
9. David Benson and Sam Fiddian, *Privacy Obligations Under the Consumer Data Right Regime: What's Changing, and What You'll Need to Consider,* March 2019.
10. Above n 2, *The Consumer Data Right.*
11. Ibid.
12. Belinda Harvey, *It's Time to Act! Consumer Data Right in the Banking Sector is Looming,* June 2019.

Andrew Stevens

Previously the managing Director of IBM Australia and New Zealand, Andrew currently serves as the Chairman of Innovation and Science Australia and the Chair of the Data Standards Body for the implementation of the Consumer Data Right in Australia. He is also a Director of Stockland Group Limited, Thorn Group Limited, the Greater Western Sydney GIANTS and CEDA. He is a member of the Advisory Executive of the UNSW School of Business, and the Male Champions of Change, a group of CEOs and Directors working to make gender equality a reality.