"Datafication of the economy for a post pandemic world"

KPMG Australia Response to
Inquiry into Future Directions for the Consumer Data Right: Issues Paper

In January 2020, the Treasurer announced an Inquiry into Future Directions for the Consumer Data Right (the **Inquiry**). On 6 March 2020, the Inquiry released an Issues Paper for consultation (**Issues Paper**).

As a leading professional services firm, KPMG Australia is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also investors, employees, governments, regulators and the wider community. We strive to contribute to debate that seeks to develop a strong and prosperous economy and welcome the opportunity to provide a response to this inquiry. This response will focus on the legal and regulatory framework that will need to support the Consumer Data Right.

Introduction

With the passing of the Consumer Data Right (CDR) Bill in August 2019, an open data economy will be introduced in Australia. This means consumers will have greatly improved access to, and control over, their own data. The CDR mandates a greater transparency of service and value that will facilitate better informed consumer choice.

This is the first step in what will inevitably be an open data future in which institutions and consumers are all part of a safe, robust and innovative 'data economy'. Open Banking is the first reform to launch in Australia and other sectors, including energy, telecommunications, superannuation, travel and leisure, will follow. This changing regulation means there is an opportunity for Australian organisations in these industries to fully realise the opportunities of open data when the CDR is further legislated.

The trend towards automation and digitisation, and the rise of data, is already well established in Australia and globally, and often described as "The Fourth Industrial Revolution". COVID-19 is strongly accelerating these pre-existing trends – a fact that businesses have been quick to embrace. Digitisation and datafication are already being adopted widely. Business has had no choice. The disruption of COVID-19 has exposed how essential these developments are to maintain shareholder and stakeholder value, and the profound risks of failing to do so.

In this environment, the pandemic creates a major policy challenge and policy opportunity for this Inquiry, and for the Government.

The challenge is to conceptualise, develop and implement an economy-wide and technology-neutral legal and regulatory framework for the efficient and effective digitisation and datafication of business, governments, the public sector and the economy. This framework needs to be flexible and agile so as to evolve with, and adapt to, coming rapid and major changes in business. It needs to empower individuals to control the sharing and use of their personal data and foster strong public trust in the framework. Public trust is particularly important as the need for voluntary take-up of the COVIDsafe app demonstrates.

In our view, these challenges cannot be met, and the potential of the economy maximised, by solely trying to adapt and build on laws written for a different world – a world with profoundly different technology and which, by modern standards, barely used data at all.

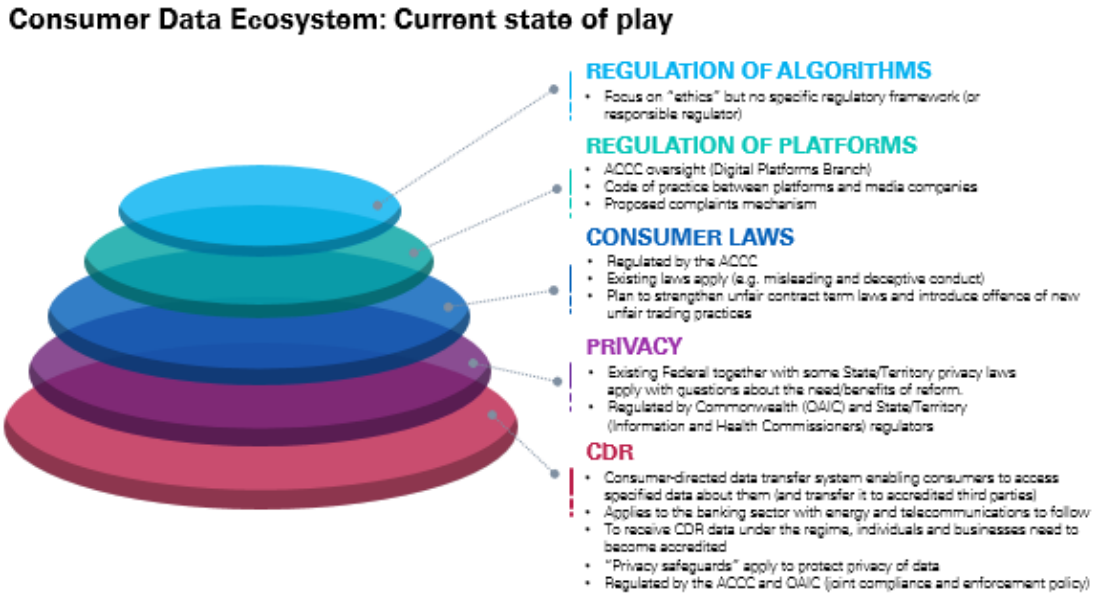
A re-imagined and consistent legal framework is required to support these trends. The opportunity, and challenge, is to support the full evolution of our economy into one which drives productivity, efficiency and growth, and generates abundant skilled jobs for Australians.

This submission considers ways in which the Inquiry can seize and expand upon that opportunity, as it applies to the various elements of the current data ecosystem.

Where are we at now? The current regulation of consumer data in Australia

The legal framework for the regulation of consumer data in Australia encompasses a growing number of fragmented Federal and State laws and regulatory instruments. Although consumer, competition and privacy laws in principle apply to all participants, "data rights" as defined under the CDR only apply to certain industries, and other parts of the legal and regulatory framework are similarly confined (e.g., the new Media Code will only apply to platforms that participate in that industry). Meanwhile, the scope of the legal and regulatory framework for the regulation of AI and algorithms – which are a key part of the data infrastructure – continues to primarily focus on the question of ethics (avoiding the harder, but critically important, questions around appropriate legal, regulatory and assurance frameworks, adverse outcomes and impacts, liability and penalties). [1]

The diagram below illustrates the current consumer data legal and regulatory ecosystem and the fragmentation that underpins it:



This 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. Our submission, discussed in more detail below, is that these problems need to be considered in a fresh and holistic way and a bold new approach is needed in order to create a legal and regulatory data framework that works for business, government, the public sector and consumers in a digital economy.

Privacy

The current privacy information laws were introduced in around 2000 and have been amended regularly since then. The Privacy Act was the subject of an extensive review and detailed report in 2008 as a result of which extensive amendments were made in 2014.[2] The introduction of the Notifiable Data Breaches scheme followed in 2018. The Government has now accepted

[1] We note that Standards Australia has issued a paper and recommendations, available at: https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx

[2] Australian Law Reform Commission, "For Your Information: Australian Privacy Law and Practice (Report 108" (12 August 2008), available at: https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

recommendations from the ACCC in relation to further amendments to address issues identified in its Digital Platforms Inquiry, such as consent and notice and a possible statutory cause of action.[3]

The introduction of the new consumer data right extends information or data rights beyond the privacy framework and gives consumers additional data rights such as data portability. In conjunction with the Inquiry, it also provides the opportunity to rethink whether the current range of data and privacy laws provide the right framework to support the Australian economy and consumers as we move into an increasingly digital and datafied environment in our working and personal lives.

Having an effective privacy regime that underpins the framework for the sharing and use of data is an important element to developing and maintaining public trust. Australian privacy laws currently comprise a range of Federal and State and Territory principles-based laws, which adopt similar but also different approaches to information rights and obligations and which are administered by different regulators. There are also a range of other laws that impact the use, disclosure and protection of data, including laws that allow data to be used and disclosed to protect national security or manage a pandemic. The transformative shift we are witnessing as we move to a digital economy prompts the question – does the existing principles based legal framework provide the right privacy framework for Australia, is a more prescriptive approach required similar to that adopted in Europe by the General Data Protection Regulation (**GDPR**) or is there a better alternative?

The complexity of the legal and regulatory requirements is only increasing through the implementation of the CDR framework, which adds a significant operational burden on those it applies to. The way CDR data is collected and disclosed may already be regulated through industry rules and regulations (the energy sector is a current example), as well as the Australian privacy laws. When that data is shared and used in the CDR regime, then some or all of the Privacy Safeguards will also apply, depending on various factors. The CDR framework also has the potential to amplify as well as address existing privacy risks from data sharing. Understanding what laws apply at what stage of the data lifecycle and to whom, managing inconsistencies and compliance requirements and handling complaints and enforcement all have the potential to impact the success of this new right and the objectives of the CDR regime.

The Fourth Industrial Revolution is not limited to Australian borders. Many of the service providers and cloud platforms Australian organisations use are based overseas. Consumers also move across borders. Therefore data is being shared, stored and used globally in larger volumes. We have seen the GDPR become a pseudo global standard for privacy. Now that it has been in operation for a period of time, there is an opportunity to consider how well it is working and whether such a framework is fit for Australian purposes in order to ensure Australia's privacy and security laws enable Australia to fully participate in those new opportunities.

Disclosure and consents

In data rich environments, consumers share personal data in the process of seeking services that are ostensibly free of charge. Sharing personal data in this way can be of benefit to consumers (e.g., providing access to information or enhanced services, personalised advertisement, etc.). However it can also be used in ways where the consumer benefit is less clear. Either way, the underlying assumption is that consumers are able to understand the benefits and impacts and strike the bargain that works best for them. This model requires the disclosure of the key terms of the bargain, informed choice and customer consent.

However one of the key issues with this model is that the appropriate levels of disclosure are difficult to achieve in a meaningful way that enhances the customer experience. Even if full disclosure is possible at a point in time, the effect of the consent can be limited if a consumer does not have the ability or means to assess the impact of a variety of possible future uses of data otherwise freely shared. The CDR regime tries to address this problem by expressly requiring a consumer's consent

[3] Government Response and Implementation Roadmap for the Digital Platforms Inquiry (12 December 2019), available at: https://treasury.gov.au/publication/p2019-41708

to be "voluntary, express, informed, specific as to purpose, time limited and easily withdrawn". This reflects the approach to consent in the interpretation of current privacy laws. The development of data standards for CDR and CX (consumer experience) guidelines further supports this. However this framework only applies to and supports CDR data and the data sharing framework (so a large amount of data that is collected in the process of digital interactions is not subject to this regime).

For its part, the ACCC has taken the view that incomplete or inappropriate disclosures about data use and sharing practices may be a breach of the prohibition against misleading and deceptive conduct in section 18 of the Australian Consumer Law (**ACL**) (and is testing that view in a current case). While it will take some time to see if the Courts agree, there is potential for a poor outcome if the main impact of the case is to require more detailed consents to be read, and more checkboxes to be ticked, before data is collected and a digital service can be delivered.

Moving forward, a better approach is needed to reflect the challenges of seeking and granting consent in a digital environment. For example, a new approach could include imposing clearer limits on what data is collected by digital businesses or what they can use the data for, or imposing more prescriptive requirements for lawful consent - effectively expanding the CDR model to all data collected online. Clear and consistent consent requirements for digital data will provide business with certainty and enhance consumer experience and rights.

Algorithms and AI: a time to move beyond ethics

To date, the market and the Australian Government has been particularly focused on ensuring that AI is "ethical". The Government published a set of voluntary AI Ethics Principles[4] to help integrate the design and application of AI within the community and entrusted the Australian Human Rights Commission (**AHRC**) with the task of consulting further on human rights and technology.[5]

While the use of AI to process data that concerns individuals or groups of individuals should be ethical, it is unclear how ethics alone would be enough to ensure accountability for AI design and use as well as for adverse outcomes. The AHRC has acknowledged that lack of legal enforceability reduces accountability. Self-regulation has been raised as a solution, but self-regulatory regimes present a number of limitations and difficulties that are common across many industries, as documented in the final report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.[6]

A new regulatory regime for AI should not require an entirely new legal framework, but rather should form part of the overall digitised and datafied economy framework, as AI will be increasingly integrated into technology and other solutions that will be developed within it. In fact, some of the regulatory infrastructure developed for the CDR should be expanded to also apply to AI, using as a model the Privacy Safeguards as well as the approach taken to Accredited Data Recipients. Conceivably, AI Safeguards could address issues such as what standards and testing should be met before an AI system can be used, who is liable if the system fails or produces undesirable outcomes, insurance obligations, and the like. Such a system would provide a degree of flexibility, while still offering enforcement options in appropriate cases. The concept of privacy by design which is an obligation in Australian Privacy Principle 1 of the Privacy Act should also provide a suitable framework.

Whereas Australia is unlikely to be alone in its efforts to establish a regulatory framework for AI and given the nature of machine learning and emerging technologies, developing a flexible legal framework fit for a digital age is key. Europe is moving in that direction and it may well develop a

[4] Australian Government, Department of Industry, Science, Energy and Resources, "AI Ethics Principles", available at: https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

[5] *See* Australian Human Rights Commission, "Human Rights and Technology", available at: https://tech.humanrights.gov.au/

[6] Final Report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Volume 1, at p. 105.

system that becomes, like the GDPR, a type of global standard (and best practice). In that environment, it will be important for Australia to retain the ability to adapt its legal and regulatory system to global trends when needed.

Data rights and the CDR regime

The current privacy laws recognise and protect information privacy rights. The ACL protects consumer rights and as the AHRC's Discussion Paper notes there are other related rights that attach to individuals' information as well as privacy as a human right. With the expansion of the CDR, another small change to sector specific regulation is being made by seeking to give consumers "write" access to their data. This is appropriate, as data is also an asset, of both the individual and of business, which may be used, traded and protected for financial or other benefit.

No right is absolute and there is a trade off at times including between the right of the individual and the public benefit. The nature of digital information, the range of potential use cases and the ability to collect, use and share data to respond to the COVID-19 pandemic, for example, shows that there are public benefits to collection, access and use of digital data by a range of participants. The CDR, and the work of this Inquiry, show how the law has started to reflect these developments.

As datafication of the economy continues, there is an opportunity to reflect and rethink what needs to happen to create certainty for business and governments, and reduce the regulatory burden - while ensuring data rights are clearly identified and protected. In particular, the current sector-specific regulation with overlapping obligations and further piecemeal reform should be avoided. Not only is this fragmentation a burden on businesses, government and regulators, but it is also confusing for consumers seeking to rely on these rights. In addition, the possibility of multiple regulators, including the ACCC and ASIC, enforcing data regulation creates uncertainty for business as well as consumers. Ultimately, the current level of fragmentation needs to be rethought and the possibility of an overarching set of legislation like the GDPR needs to be considered.

If the legislative framework for the regulation of data continues in a piecemeal, sector specific and fragmented way, Australia will miss an opportunity to create a legal and regulatory data framework that works for business, government, the public sector, consumers and for the entire economy. Care will also need to be taken to ensure that the legislation and regulation created enables Australian organisations to operate and compete at a global level.

KPMG Australia Contributors:

Stuart Fuller, Partner, KPMG Australia
Kate Marshall, Partner, Head of KPMG Law, KPMG Australia
Paula Gilardoni, Partner, KPMG Australia
Veronica Scott, Director, KPMG Australia
Caroline Marshall, Senior Manager, KPMG Australia