



Consumer rights to personal data

Data access in the communications sector

Consumer rights to personal data

Data access in the communications sector

James Meese, Punit Jagasia and James Arvanitakis

July 2019



Consumer Rights to Personal Data

Authored by James Meese, Punit Jagasia and James Arvanitakis

Published in 2019

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

University of Technology Sydney

Website: www.uts.edu.au

Email: james.meese@uts.edu.au

Telephone: +61 3 9514 2955

Australian Communications Consumer Action Network

Website: www.accan.org.au

Email: grants@accan.org.au

Telephone: 02 9288 4000

If you are deaf, or have a hearing or speech impairment, contact us through the National Relay

Service: <https://www.communications.gov.au/what-we-do/phone/services-people-disability/accesshub/national-relay-service>

ISBN: 978-1-921974-57-1

Cover image: Design by Richard Van Der Male with images from Markus Spiske@markusspiske and Shutterstock.



This work is copyright, licensed under the Creative Commons Attribution 4.0 International Licence. You are free to cite, copy, communicate and adapt this work, so long as you attribute the authors and “University of Technology Sydney, supported by a grant from the Australian Communications Consumer Action Network”. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>

This work can be cited as: Meese, J., Jagasia, P. and Arvanitakis, J., 2019, *Consumer rights to personal data: Data access in the communications sector*, Australian Communications Consumer Action Network, Sydney.

Acknowledgments

We would like to thank ACCAN for supporting this project and Tanya Karliychuk in particular, for providing guidance, feedback and encouragement throughout the research process.

We also thank our participants for their assistance and Vlora Hoti for editing this report. We also acknowledge the work of Mike Riethmuller who developed the Facebook Data Visualiser (available at <http://visualisefacebookdata.com/>) and Kathrin Kohl for designing the consumer guides. These two consumer-facing outputs also form part of the funded project.

Table of Contents

Acknowledgments.....	i
Table of Contents.....	ii
Figures and Tables	iv
1 Executive Summary.....	1
2 Introduction	2
3 Background	5
3.1 Australian consumers and personal data	5
3.2 Data access rights in Australia	6
3.3 Data access in the European Union	7
3.4 The Consumer Data Right	8
3.5 Our research approach	10
4 Methodology.....	11
5 Data access standards: Best practice	12
6 The data access process.....	14
6.1 Telecommunications companies	14
6.2 Social media	16
6.3 Google.....	19
6.4 Wearables	20
7 Data access: Understanding the results.....	22
8 Assessing the Consumer Data Right.....	25
8.1 CDR terminology	25
8.2 What is consumer data and should consumers pay for it?	26
8.2.1 Recommendation 1.....	27
8.2.2 Recommendation 2.....	27
8.2.3 Recommendation 3.....	27
8.3 Privacy and governance framework	27
8.3.1 Recommendation 4.....	28
8.4 Standardisation	28
8.5 Accreditation.....	29

8.5.1	Recommendation 6.....	30
8.5.2	Recommendation 7.....	30
8.6	Consumer and business attitudes.....	30
8.6.1	Recommendation 8.....	32
8.6.2	Recommendation 9.....	32
8.7	Scope.....	32
8.7.1	Recommendation 10.....	32
8.8	A new Australian data policy framework.....	32
8.8.1	Recommendation 11.....	33
8.8.2	Recommendation 12.....	33
9	Beyond data access: Conclusions and next steps	34
	Authors.....	36
	Abbreviations.....	37
	References	38

Figures and Tables

Figure 1: Telstra’s website section for data access requests.....	14
Figure 2: Making an additional data request through Twitter	17
Figure 3: A sample of the data provided by Twitter	17
Figure 4: A sample of the data provided by Google	19
Figure 5: A sample of the data provided by Fitbit	20
Figure 6: An attempt at providing simplified policies.....	22

1 Executive Summary

This report assesses the state of data access in the communications sector, with a specific focus on data-intensive products and services. Recognising that consumers are becoming increasingly concerned about their personal data, we decided to ask a simple question: can we access our data?

The research team tried to access data from social media platforms (Facebook, Instagram, Twitter), online companies (Google), telecommunications companies (Optus, Vodafone, Telstra) and fitness wearables (Fitbit, Apple Watch).

We found that **access processes were convoluted and diverse and there was no clear standard across each product [i.e. wearables] and/or service category [i.e. telecommunications providers]**. While we could get access to some sort of data, the provision of data was not comprehensive in many cases and the data that was provided came in a variety of formats.

Australia is about to introduce a Consumer Data Right (CDR), which aims to simplify and standardise the process of accessing and transferring data. Our findings have shown that such a reform is needed. **We recommend the introduction of the Consumer Data Right.**

Our other central recommendation is that **Australia needs an equivalent to the General Data Protection Right (GDPR)**. The European Union has introduced a foundational reform that provides citizens with a range of rights, including a right to be forgotten and a right to access data.

While the CDR is an important reform, it is narrowly targeted. It introduces a new definition of consumer data that is broader than the existing definition of 'personal information' in the *Privacy Act 1988*. It also introduces additional legislative obligations. However, these new definitions and obligations only relate to data access and transfer. As a result, Australians will only have a very limited set of rights in relation to their data.

Moreover, a range of other government bodies are conducting reviews of privacy related issues or proposing privacy reforms, alongside the CDR process. This has resulted in a series of overlapping reform agendas. **We recommend that the Australian Government should wait until these reports are complete rather than engaging in patchwork reform.** The CDR should form part of a broader suite of rights that update Australian privacy law for a data-driven economy.

The rollout of the right has been delayed until February 2020. Subsequently, we have offered a series of more specific recommendations relating to the CDR and Australia's broader data policy framework in Chapter 8. The consultation process has finished and the Bill is likely to be introduced as it stands. However, we hope that this analysis can inform the ongoing improvement of the right into the future.

2 Introduction

Australian consumers are engaging with an increasingly data-driven economy. Digital platforms provide free services in exchange for personal data and retailers offer reward schemes to gain a detailed understanding of our purchasing habits. However, while companies know a lot about us, consumers do not know much about how companies collect, use and handle our data (Nguyen & Solomon 2018). It is common for personal data to be shared across a range of companies (Larsson 2018), and we are only informed at the initial stage of collection through technically written and poorly understood privacy policies that are seldom read (Solove 2013).

The problem with this was made abundantly clear in the recent Cambridge Analytica scandal.¹ People thought they were filling out an innocuous personality quiz through a Facebook app. However, the app also collected information from their profiles and the profiles of their friends (Granville 2018; Arvanitakis 2017). It ended up scraping data from around 50 million profiles and this data went on to inform the design of a voter targeting system in the United States (Granville 2018).

In addition to the broader legal and ethical issues that Cambridge Analytica raises, the scandal functions as an excellent (albeit dramatic) example of the broader information asymmetries facing Australians. While consumers hand over data to *one* company, this data regularly passes through the hands of multiple parties (Federal Trade Commission 2014; Nguyen & Solomon 2018). Consumers (the original data providers) have no idea where their data has gone and are rarely directly consulted with regards to this process. As the Productivity Commission has noted, Australians have ‘limited knowledge of what is being collected and why’ (Productivity Commission 2017, p. 126).

In response, the regulation and control of personal data has become a first order international policy issue over the last few years. The European Union has introduced the General Data Protection Regulation (GDPR), which provides European citizens with a range of rights relating to their data (Satariano 2018) and the United States Federal Trade Commission released a detailed report on data brokers (Federal Trade Commission 2014). Alongside these investigations and reforms, a number of ideas are being floated, from embedding privacy by design into production processes (Langheinrich 2001) to data ownership, where people retain some sort of property in their data (Hoeren 2014).

This report contributes to this discussion by focusing on one area of the information asymmetry debate: **consumer access to personal data**. This topic emerges from a relatively functional consideration of the issue. Consumers can give up a lot of data to companies when they sign up to use services or purchase goods and continue to generate data when they use services. We wanted to know if companies returned this data to consumers and how they did it. Our hypothesis was that by returning personal data, companies would at a minimum, give consumers some sense of what data they were sharing, which other researchers note provides a level of ‘transparency to citizens’ (Mahieu, Asghai, van Eeten 2018). Companies that provided their data in specific formats, could also help consumers move between competing companies, addressing concerns around competition (particularly online) (see ACCC 2018).

¹ See ‘The Cambridge Analytica Files’, available at: <<https://www.theguardian.com/news/series/cambridge-analytica-files>>.

More specifically, our research objectives are:

1. To outline how data access requests are currently actioned in data-intensive areas of the communication sector and to develop an evidence base around the quality of these processes.
2. To analyse the value and effectiveness of data access in order to inform current and future policymaking efforts and support effective consumer advocacy.

Our study was influenced by the Australian Government's introduction of the Consumer Data Right (CDR). The CDR will allow Australian consumers to direct companies to share their data with accredited third parties and allow these third parties to analyse this data for the benefit of the original consumer. The Right has been lauded as a transformative solution to some of the problems caused by information asymmetry, with a Productivity Commission report suggesting it would contribute to 'more informed decision making by consumers, businesses and government' and the 'transformation of everyday life through personalised products and services, and a greater variety of choices' (Productivity Commission 2017, p. 170).

By focusing on data access, this project aims to examine the scope and potential of this policy framework and assess the extent to which data access should operate as a foundational element of Australia's data policy into the future.

The project's second motivation is to examine how data access currently operates. The CDR will originally be limited to banking customers, before being rolled out across the telecommunications and energy sectors. Consumers will have to conduct their own data access requests in the short to medium-term for most sectors. Subsequently, our project also examines some current data access procedures in order to identify whether the CDR would be an improvement on existing processes.

Our study contributes to these discussions by focusing on data access in the communications sector, with a specific focus on data-intensive products and services. As a result, the project focused on social media platforms (Facebook, Instagram, Twitter), online companies (Google), telecommunications companies (Optus, Vodafone, Telstra) and fitness wearables (Fitbit, Apple Watch). The team examined privacy policies and data policies before engaging in data access procedures to answer the following simple questions.

Can consumers:

- Find out what data they can access?
- Access all their data?
- Access their data in a relatively easy fashion?
- Talk to staff who can help action data requests?
- Make additional requests for data?
- Move their data to another company?

The team then assessed how each company responded to these questions by using a set of best practice standards, which are based on existing national and international legislation and regulatory

principles. We used these standards to evaluate the processes of each company and product and/or service category.

Our assessment of data access processes revealed a number of issues, so we turned to the proposed CDR to see whether it would solve these problems. This process involved conducting further desk research to produce a critical analysis of the CDR.

3 Background

3.1 Australian consumers and personal data

Over the last few years, numerous studies have shown that **Australians are concerned about their online privacy**. The Office of the Australian Information Commissioner (OAIC) has found that a ‘majority of Australians claim to be more concerned about the privacy of their personal information when using the internet than five years ago’ (Van Souwe et al. 2017, p. 8). These results are supported by a 2017 study conducted by the University of Sydney who found that only 38% of Australians felt in control of their privacy online (Goggin et al. 2017, p. 21).

Though consumers have concerns about how both government agencies and businesses are managing their data, evidence confirms slightly more trust in government (Goggin et al. 2017). Indeed, one key driver for this level of concern in the corporate space is because **companies are collecting lots of information and sharing it with third parties** (see Federal Trade Commission 2014). The same report from the University of Sydney notes ‘57% of respondents were concerned about their privacy being violated by corporations’ (Goggin et al. 2017, p. 13). In a survey conducted by the Consumer Policy Research Centre in 2017, ‘two-thirds of Australians’ indicated that they [...] ‘were uncomfortable with most types of information being shared with third parties’ (Nguyen & Solomon 2018, p. 32). The OAIC survey returned similar results, with only one in five Australians feeling comfortable with targeted advertising and one in six comfortable with social networking companies keeping databases of information on their online actions (Van Souwe et al. 2017, p. ii).

While Australians are concerned about their personal data, **they do not know what is happening to it**. Consumers retain a basic level of knowledge with 91% of Australians aware that companies could follow their activities across different websites (Nguyen & Solomon 2018, p. 28). However, our knowledge starts to falter when questioned on more technical matters. For example, a number of surveys found that most people do not know that mobile apps can collect ‘device data completely unrelated to the app’s function’ (Nguyen & Solomon 2018, p. 29; also see Van Souwe et al. 2017). People were also keen to learn more about ‘what social media companies do with the information they collect, share, keep and use’ (Goggin et al. 2017, p. 18).

Australians are also subject to the privacy paradox, where they are **worried about their privacy but don’t always protect it**. Research nationally and internationally has shown that people do not read privacy policies or terms and conditions (Solove 2013; Goggin et al. 2017; Nguyen & Solomon 2018; Van Souwe et al. 2017). Further, while many Australian consumers know how to adjust their online privacy settings or delete cookies, many do not do so regularly (Nguyen & Solomon 2018).

The research above paints a concerning picture around people’s relationship with personal data. Australian consumers feel uncomfortable about the use of their data but they do not know much about how their data is being handled or shared and only occasionally engage in privacy management strategies. The concept of ‘personal data’ is so hard to grasp that most researchers argue that consumers should not be expected to manage their privacy and that we should instead focus more on the data collection activities that companies engage in (Livingstone 2019). This may

involve regulation, but it also would involve a broader cultural and economic change that focuses on minimising data collection where possible.

We agree with this approach and argue that data minimisation is the most appropriate policy approach going forward. However, we focus on data access in this report, because so many governments and companies continue to promote it. Data access is regularly presented as a partial solution to information asymmetry and a way to rebalance the scales between company and consumer. For example, when Facebook launched its 'Download Your Information' tool, an employee promoted it as the 'flip side' of Facebook 'sharing user data with external developers and websites' (Tsotsis 2010). In a similar fashion, the CDR stands as a salutary example of statutory bodies and government relying on data access to solve some of the ongoing problems associated with a data-driven economy. In the section below, we outline the existing legal framework surrounding data access in Australia and the recent legislative developments around data access.

3.2 Data access rights in Australia

Australians have a limited ability to access their own data. People can access their own personal information through Australian Privacy Principle (APP) 12, which requires an 'APP entity that holds personal information about an individual to give the individual access to that information on request' (OAIC 2014, p. 3).

Government agencies and organisations have to respond positively to the request, barring limitations placed by other legislative instruments or a series of other exceptions outlined by the principles (i.e. 'the request for access is frivolous or vexatious') (OAIC 2014, p. 9). Information must also be provided in 'the manner requested by the individual' (OAIC 2014, p. 9). While government agencies cannot charge for the request, organisations can charge individuals, although this cannot 'be excessive and must not apply to the making of the request' (OAIC 2014).

This right is relatively narrow due to the highly specific nature of the Australian Commonwealth's *Privacy Act 1988*. The first issue is that not every organisation or company has to adhere to the Act. It applies to Australian Government agencies, businesses and not for profit organisations with an annual turnover of more than \$3 million, any organisation that provides a health service, and 'businesses that sell or purchase personal information, credit reporting bodies, contracted service providers for a Commonwealth contract, and employee associations' (Productivity Commission 2017, p. 450). As a result, many small businesses do not need to comply with the legislation. Political parties are also exempt from the act (*Privacy Act 1988* (Cth), s. 6C(1)). This means that numerous companies who may hold data about Australians do not need to comply with access requests, meaning that the solution of 'data access' is limited at best.

The legislation does have some force internationally, so some social media platforms and other international companies who handle data have to adhere to Australian privacy laws. These companies must have an 'Australian link', which usually means that they collect data from Australian citizens (*Privacy Act 1988* (Cth), s. 5B(3)(c)). A link can also be proved through a company simply having a presence in Australia or conducting business in Australia (*Privacy Act 1988* (Cth), s. 5B(2)). However, the legislation still only applies to international companies with a \$3 million annual

turnover. So, while this covers major international companies that handle Australian data,² it may not cover smaller businesses like start-ups.

The second issue is that even compliant companies only have to provide **personal information** (as opposed to data) under Australian law, which is described in the Act as:

[I]nformation or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not *Act(Privacy Act 1988 (Cth), s. 6).*

This means that Australians only have a clear right to access data that identifies them (either directly or indirectly). However, companies collect a range of other data that does not immediately identify someone. For example, social media platforms collect location data and fitness trackers collect heart rate and sleep pattern data. It is currently unclear whether this data, which may only identify someone after being combined with other data, falls under the definition of personal information (see Nguyen & Solomon 2018, p. 9). Judges have suggested that ‘even if a single piece of information is not “about an individual” it might be about the individual when combined with other information’ (*Privacy Commissioner v. Telstra Corporation Limited* [2017] FCAFC 4 at 63). However, this has not yet been established as legal precedent (Johnston 2017).

3.3 Data access in the European Union

The European Union’s GDPR provides a useful point of difference that underlines the limited nature of Australia’s existing data access laws. The GDPR applies to *any company* that processes personal data (GDPR 2016, art. 2(1)), including international companies if they offer goods or services to European Union citizens or monitor their behaviour (GDPR 2016, art. 3(2), emphasis added). Companies cannot avoid the requirements of the GDPR due to the size of their business or their location.

Importantly, the GDPR has an expanded definition for the information that falls under its scope. They call this information ‘personal data’ as opposed to ‘personal information’ and it encompasses more of the data we share every day. They define ‘personal data’ as:

any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR 2016, art. 4(1)).

Due to the specific nature of this definition, indirect data clearly falls under the scope of the regulation, contrasting with the currently uncertain status of ‘personal information’ in the Australian Privacy Act.

² For example, see the OAIC opened an investigation into Facebook, following Cambridge Analytica. See: <<https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica>>.

The GDPR also provides a series of rights to individuals (called ‘data subjects’). Some of those rights mimic those granted by the Australian Privacy Act, such as the right to rectification (GDPR 2016, art. 16; see APP 13), whereas others, such as the right to erasure (also known as the ‘right to be forgotten’) are not addressed by Australian legislation (GDPR 2016, art. 17).³ All of these rights are grounded in a legal philosophy that views data protection as ‘a fundamental right anchored in interests of dignity, personality, and self-determination’ (Schwartz & Peifer 2017, p. 123). They are also situated within a broader human rights framework, through the Convention for the Protection of Human Rights and Fundamental Freedoms.

As part of this suite of rights, the GDPR also features a right to data access. The ‘[r]ight of access by the data subject’ gives individuals the right to request ‘a copy of the personal data undergoing processing’ (GDPR 2016, art. 15(3)). If the request is made electronically, ‘the information shall be provided in a commonly used electronic form’ and an initial copy must be provided for no cost (GDPR 2016, art. 15(3)).

An adjacent right that also falls under the broad notion of data access is the ‘Right to Data Portability’ (GDPR 2016, art. 20). Individuals are able to use this right to request personal data ‘in a structured, commonly used and machine-readable format’ (GDPR, Art 20 (1)). The premise underlying this right is that individuals can transfer (or ‘port’) their data to a competing business or company with limited barriers.

The benefit of the GDPR is that citizens can access a wide range of data from any company that handles their data. As noted above, the framework is also ‘backed by the legal system’s recognition of both privacy and data protection as fundamental rights’ (Esayas & Daly 2018, p. 200). While there are issues with the operation of this law in practice, on paper at least, the GDPR is better equipped to deal with the significant levels of digital data that consumers hand over every day.

3.4 The Consumer Data Right

The Australian Government has recognised the limitations of the current Privacy Act and the increasingly important role of digital data in the consumer environment. In response, they have introduced the CDR, which will operate in the banking sector from February 2020. This Right will then be introduced to the energy and telecommunications sectors before being gradually rolled out to other sectors.

The CDR will allow Australian consumers (and businesses) to ‘to safely access certain [digital] data about them held by businesses’ (Consumer Data Right 2018, p. 1). They will also be able to direct businesses to transfer this information ‘to accredited, trusted third parties of their choice’ (Consumer Data Right 2018, p. 1). To provide some brief illustrative examples, consumers could use this Right to transfer their banking history to new digital-only (or ‘challenger’) banks (see Peyton 2018), or share historical transaction data with a third-party comparison service who could recommend products based on the ‘consumers’ actual spending and repayment patterns’ (Consumer Data Right 2018, p. 2).

³ The ACCC recommended this right in their Preliminary Report from the Digital Platforms Inquiry. We also note that Google and Facebook have made very recent moves in this direction, with both promising to launch ‘clear history’ tools.

On face value, the CDR is an innovative expansion of data access rights within Australia. It expands the Privacy Act's existing data access provisions, and also departs from them at times, in a number of important ways. Firstly, the law covers a larger proportion of data. The CDR 'applies to data that relates to individual consumers, as well as business consumers [and] provides access to information that relates to products' (Explanatory Memorandum 2018, 1.11). This means that data does not need to be about someone, nor does an individual have to provide the data directly to request it (i.e. the data could be generated by their activity with a service). It avoids the confusion between identifiable and non-identifiable personal information and simply allows consumers to request access to any data that is broadly relevant to them.

Secondly, the law encourages individuals and some businesses (that also fall under the definition of consumer) to avoid the direct handling of data. The data access model in APP 12 generally presumes that someone is making a direct request for personal information. After making the request, the agency or organisation will deliver the personal information to the individual. In contrast, the CDR model is keen for the consumer to operate as a data manager rather than a data recipient. They are viewed as a key intermediary who can request and approve the transfer of data from organisation to organisation (i.e. from bank to bank), or from an organisation to an intermediary (i.e. from bank to comparison site).

The proposed regulatory framework sees the CDR operating under a new set of 'Privacy Safeguards' that will supersede the APP. These have been described as 'equivalent' to the APP but also 'more onerous' (Consumer Data Right Privacy Protections 2018, p. 4). This means that small and medium businesses who are not currently bound by the Privacy Act and want to be accredited recipients, must adhere to these safeguards if they are to receive data. In addition, consumers will be able to seek remedies for any data breach, which has been described as 'a major development from the Privacy Act [and] an important step towards the better protection of fundamental rights in Australia' (Esayas & Daly 2018, p. 200). It is also worth noting that the CDR improves the consent standards of the Privacy Act by requiring consent to be 'clear and unambiguous' and 'not open ended or implied' (Consumer Data Right 2018, p. 5).

Currently, we do not know what the impact of this new model will be. It works against the data minimisation approach by giving consumers more value from their data. As a result, consumers may be encouraged to support existing levels of data collection if they get value out of it. They may also agree to the broader spread of their data due to a streamlined request and transfer model that makes data transfers easy to achieve without much consideration on the part of the consumer. The intermediary model also raises a number of issues. While keeping data away from insecure environments is a possible positive outcome (i.e. compared to a direct data request, where requested personal data may be kept on a domestic computer), data could equally be placed at risk due to the amount of data being passed around third-party organisations, which are all equally subject to 'hacking, improper disclosure and access' (Kemp & Vaile 2018). All of these issues and more underline the fact that problems around data access will not be immediately solved following the introduction of the CDR.

3.5 Our research approach

It is possible that in ten years we would not need to write this report. While there are a range of ongoing issues around data rights in Australia (Goggin et al. 2017), the CDR promises to be an innovative solution to the problem of data access. However, the right will roll out slowly. This means that **Australians will continue to face issues with respect to data access for some time**, both in terms of the limitations of the existing legislative framework that supports access requests and the varying industry responses to these requests. Our study provides insight into current data access standards across an important sector and builds a case for the value of a streamlined and well-regulated data access process, which the CDR may provide.

But our study also seeks to test some of the promises made about the CDR and consider some of the decisions made about the scope and remit of the Right. The Right retains a strong presumption of **consumer engagement**. There is a clear expectation that consumers will initially make use of the Right to seek out better deals and draw on their data when engaging in financial management. However, the Australian Community Attitudes to Privacy Survey 2017 conducted by the OAIC found that ‘just over a third of Australians (37%) know that they can request access to their personal information that is held by government agencies or businesses’ (Van Souwe et al. 2017, p. 15). A submission from the Australian Privacy Foundation to the Open Banking Review also noted that ‘there is no reliable data available about rates of access to personal information’ (Australian Privacy Foundation 2017, p. 3).

It is also important to **question some of the claims made about the CDR’s proposed impact**. Public materials explaining the Right are incredibly positive and promise transformative outcomes. The Treasury claims that the Right ‘will improve the flow of information in the economy [...] support innovation and cost reduction in the creation and delivery of the goods and services’ and ‘support data driven economic growth and create new high value jobs in Australia’ (Consumer Data Right 2018, p. 2). Through a detailed analysis of available legislation, stakeholder commentary, scholarly literature and previous studies, we will examine the extent to which the draft bill fulfils these promises and assess the broader impact of the CDR on Australia’s overall data policy framework. As part of this process, we will discuss policy conflicts and gaps that may still be present following the gradual introduction of the Right.

We will also focus on **compliance**, which will only become a more prominent issue as the Right moves throughout other sectors. Research has shown that major digital platforms complied with the letter but not the spirit of the GDPR, with particular platform designs encouraging individuals to not protect their privacy (these are called ‘dark patterns’ in user experience research) (Forbrukerrådet 2018). Other studies on data access in Europe, conducted prior to the introduction of the GDPR, have found that compliance with the right of access ‘is a mess’. They state that ‘[n]on-compliance with the formal requirements of the law is widespread, with some organisations failing to answer at all, and others obstructing transparency in their answers’ (Mahieu, Asghari & van Eeten 2018). We assess compliance through our assessment of data access processes but also analyse current policy settings and assess possible compliance risks in the future rollout of the CDR.

4 Methodology

This project investigates data access across three areas, so we have used a variety of methods in order to capture a reliable amount of data.

Our first task was to examine the data access policies and procedures of specific data-intensive communications companies. As noted earlier, we focused on data-intensive products and services across three subcategories of the communications sector: telecommunications, social media, and wearables. Using a ‘critical case selection’ method (Flyvbjerg 2006), we focused on Australian market leaders in each nominated product and/or service category and analysed the relevant corporate documentation from each benchmark company. This documentation usually consisted of privacy and data policies as well as public information about data access processes.

We then made data requests through our own consumer accounts. We made remote access requests from July 2018 to March 2019. Initial or further requests that required interaction with a customer service operative were made in March and April 2019, following ethics approval (ETH18-2827/3304). When we didn’t hold an account with the service, we asked another person to make the request. When someone from outside the project team made a request, we did not look at their data but talked to them about the request process and asked them to detail what information they received. When there wasn’t a straightforward access process or we weren’t granted complete access after an initial request, we made another attempt to request access to see whether our initial attempt was an isolated occurrence. We drew on these experiences to assess the data access process provided by each company, against a set of standards, which will be explained in detail in the following section.

Finally, we drew on these findings to assess the usefulness of the CDR, before going on to analyse the current CDR legislation and Australia’s overall data policy framework. As part of this process, we consulted Australian and international legislation, recent inquiries conducted by government agencies, surveys conducted by universities and civil society bodies around consumer data and information asymmetry, grey literature and relevant scholarship.

5 Data access standards

Before accessing our data, we established a set of standards which we could use as a baseline to assess each company and product and/or service category. In short, we wanted to decide what were adequate responses for each of our six questions.

Can consumers:

1. Find out what data they can access?
2. Access their data in a relatively easy fashion?
3. Access all their data?
4. Talk to staff who can help action data requests?
5. Make additional requests for data?
6. Move their data to another company?

It is important to note at the outset that we approached these standards contextually. We did not want to produce a ranking system that compared different companies who collect and use data in dramatically different ways. Instead, we aimed to develop a set of best practice standards, which we could use across industries and organisations when interpreting the results of our attempts at gaining access.

These standards were as follows:

i. Transparency of data collection: Can consumers find out what data they can access?

- Before consumers access their data, they need to know what is being collected.
- Best practice would look like a privacy policy that was simple and easy to understand, with limited legalese. This may involve the provision of supporting media to explain terms or concepts.

ii. Ease of Data Access: Can consumers access their data easily?

- Consumers should be able to make data requests easily.
- Best practice would look like any company who allowed consumers to make data requests independently or through a simple process once contacting the company.

iii. Scope of data provision: Can consumers access all their data?

- Companies are collecting more and more data from consumers.
- Best practice would look like any company who provide consumers with as much of this data as they could.

iv. Additional Data Requests: Can consumers make additional requests for data?

- Sometimes companies would have a standard data request process (often for free). However, consumers might want more data than is initially provided.
- Best practice would see companies allowing consumers to make additional data requests either independently or through a simple process once contacting the company.

v. Further assistance: Can consumers talk to staff who can help action data requests?

- While best practice should support independent data requests, consumers who need assistance should be able to get it.

vi. Data Portability: Can consumers move their data?

- Being able to move data between services supports a competitive market and avoids consumer lock-in. Consumers also need to be able to move (or port) data easily.
- Best practice would look like the provision of data in a portable format that could be moved with limited technical literacy or the support of an intermediary service.

6 The data access process

In this section, we reveal the outcome of our attempts to access data from a series of data-intensive communications companies through a series of case studies. We will outline the request procedures of each category (telecommunications companies, social media platforms, wearables) and discuss the strengths and limitations of existing corporate practices.

6.1 Telecommunications companies

In our study the research team or representatives were able to access personal information about themselves. This meant that Vodafone, Telstra and Optus fulfilled their legal obligations under the Australian Privacy Act. However, there was no consistency across the sector, with each company offering markedly different access procedures.

Telstra stood out as an example of best practice for the telecommunications sector and was one of the leading companies across the whole study.

The process to access data is outlined on a consumer-friendly website (see Figure 1). Customers can see what sort of data they will receive, and the associated costs involved with any particular request. They can even view a set of sample data. Impressively, Telstra also go beyond their legal obligations by not just providing ‘personal information’, but by providing a range of pertinent customer information that may or may not be personal information under Australian law (see *Privacy Commissioner v. Telstra*). This includes data on cell tower location coordinates and data sessions for mobile phones.

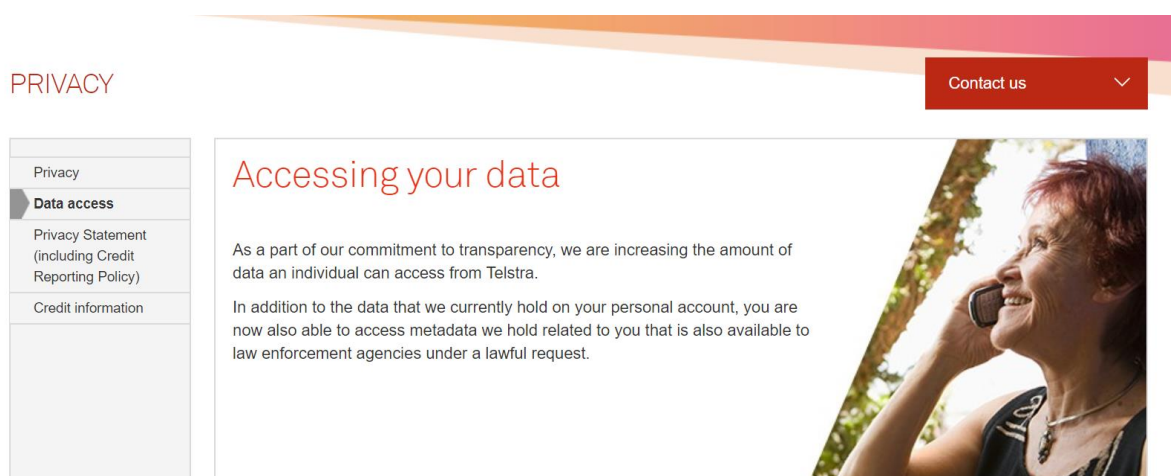


Figure 1 Telstra's website section for data access requests

Consumers fill in a form online where they can request basic customer information. Additional access options are available for a fee (which we chose not to select). While the web form was not particularly well designed, the process was straightforward and relatively quick. We received the basic customer information (or ‘personal information’) within five days in a PDF file.

It was harder to find out how to access personal information from **Vodafone**. Customers have to find a link to a personal information request form within the company's privacy policy documentation. The link takes customers to a form, where they can fill out a request for personal information, which can be subsequently emailed or mailed to the customer. Vodafone provides no information at this stage about what data a customer may receive and is vague about any costs that may be incurred. The request also focuses on the notion of 'personal information' – which suggests that Vodafone is focused on legal compliance rather than allowing customers to access a broad suite of data. We asked to receive 'all the personal information Vodafone holds [...] as well as any related data' but specified that we only wanted what could be provided for free, along with an 'estimated cost for any further data provision'.

Vodafone provided much more clarity after the request was made. A customer representative called and outlined the access process in detail. They explained the types of data that were available, what costs were involved when requesting particular types of data and the types of data that could be provided for free. A follow-up email was sent with a secure PDF file attached. The PDF listed the types of information that Vodafone held about the customer and provided the personal information of the customer. Only personal information was able to be provided for free but further information could be accessed for a cost.

Optus' processes were the least consumer friendly. There was no easy way to make a data request. Customers cannot fill in a form and there is no central website. Instead, Optus encourages people to speak to a representative on live chat or on the phone to access your 'personal information'. This makes some sense as people are familiar with the process of speaking to customer service operatives. This also avoids processing time as questions can be answered immediately.

However, the request process is not transparent at all. Optus does not provide access to all the personal information that they hold on you. Customer service representatives will respond to specific customer requests about personal information and in one case, directed us to their *My Account* page, where a range of personal information is held. The problem with this method is that it places the obligation back on the customer, who has to guess what information Optus may hold about them and then request it. It is important to note that under Australian law, companies are able to give customers their personal information in various formats (including via voice) (see OAIC 2014, APP 12.69). It is also likely that Optus would have fulfilled their obligation to 'give access to personal information in the manner requested by the individual' (see OAIC 2014, APP 12.68), if we had attempted a more formal request method, such as a letter to a privacy officer. However, the standard request method is opaque and likely to be confusing for the average consumer. The process of escalating a request was also unclear. Optus was only willing to share 'personal information' as required by law.

Furthermore, requests were not handled by a dedicated privacy team and customer representatives seemed unfamiliar with the issue when requests were made. There may well have been more formal channels available where we could have sought clearer advice, but we were not directed to these when consulting public facing documentation or talking to customer service.

In addition to these specific access processes, there were some tendencies that emerged across the sector with respect to our rankings. **None of the data provided was portable**, with companies providing information via soft-copy (Telstra, Vodafone), text (Optus Live Chat) or over the phone

(Optus). Telstra and Vodafone provided additional data for a fee but **Optus only provided personal information** and did not offer any additional data (at least in our interactions). This is not a criticism of Optus per se, as they *did* fulfil their legal obligations. However, it does point to the limitations of APP 12 and the benefits of the CDR, which will potentially allow consumers to access more meaningful telecommunications data in a portable format.

It is important to note at this point that the telecommunications sector does support some data provision and exchange. The *Mobile Number Portability Code* (2015) provides a simple way for customers to move between telecommunication providers. However, this process is business-to-business rather than consumer facing. The *Telecommunications Consumer Protections Code* (2012) also requires telecommunications companies to communicate clearly with customers and provide overarching summaries of important information (such as services, pricing and volumetric information). Indeed, the code stands as a good foundational document. However, our experience suggests that there is more scope to engage with consumers around data and mobilise that data in more innovative, consumer-facing ways.

Telstra, Vodafone and Optus offered relatively comprehensible privacy statements and policies, although there was scope for information to be presented in a **less legalistic fashion**. All three companies did not allow customers to access data independently, but Telstra and Vodafone provided a clear process that customers could follow with relative ease.

6.2 Social media

Social media platforms have made it easier to access at least some of the data they hold about you. As a result, we were able to successfully download data from Facebook, Twitter and Instagram – the three social media platforms this project focuses on.

People have been able to download some of their data from **Facebook** since 2010 (Tsotsis 2010). The feature is currently called *Download Your Information* and it allows people to request data from a range of categories associated with their activity on Facebook. Once a request is made, consumers are sent an email directing them to a ZIP file, which is temporarily hosted on the *Download Your Information* page for a few days. This process usually occurs across 24–48 hours and ours took under a day.

Instagram has made a data download tool available since early-2018 (Murphy 2018). If consumers navigate to the *Data Download* section of the *Privacy and Security* settings category, they are able to make a data request. Instagram does not allow you to select specific categories. Instead, they prepare a data file for you within 48 hours. When the file is compiled, all you need to do is to log in to your account and download it. Ours was prepared in matter of hours.

Twitter allows you to request your archive from their *Settings and Privacy* page (see Figure 2). Consumers have been able to use this feature since 2012 (Vandor 2012). Consumers are not able to select what they would like to receive. Instead, a general request is made and then a ZIP file of information is delivered via email (usually within 24–48 hours). However, consumers can request additional information through their *Privacy Policy Inquiries* form.

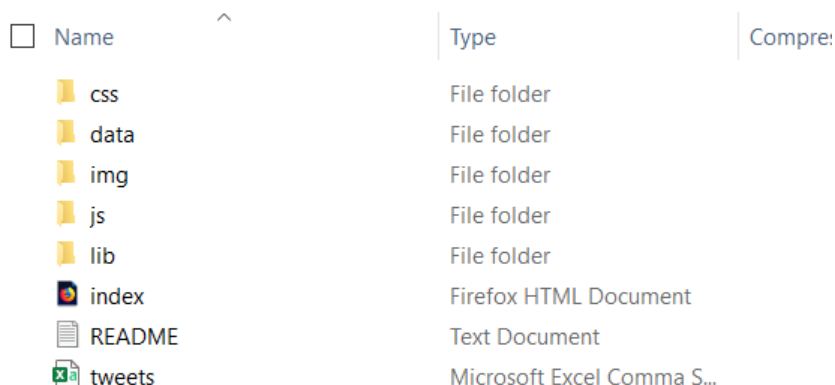
Twitter privacy policy inquiries

How can we help?

- I am requesting Twitter account information.
- I want to report an underage person's account.
- I want to request the deactivation of a deceased or incapacitated person's account.
- I want to ask a question regarding privacy on Twitter.

Figure 2 Making an additional data request through Twitter

A request to Twitter only took five minutes to be fulfilled. It provided an excel spreadsheet with all of the tweets associated with the account, a HTML document which functions as an interface that allows people to browse through their tweets from each month, and an industry standard JSON export of tweets that allows people to port their data to other platforms (see Figure 3).



Name	Type	Compre:
css	File folder	
data	File folder	
img	File folder	
js	File folder	
lib	File folder	
index	Firefox HTML Document	
README	Text Document	
tweets	Microsoft Excel Comma S...	

Figure 3 A sample of the data provided by Twitter

Platforms provide a lot of information once a request has been processed, to the extent that it would be tedious to list everything here. When responding to a full request, Facebook provides everything from data on 'Events' RSVPs and the 'Groups' you have joined and left, to associated data relating to accounts, such as information about your interactions with advertisers. While the provision of data varies on Instagram and Twitter, the scope of data provision is similar.

The amount of data that is provided points to one of the problems with how platforms facilitate data access. Facebook and Twitter try to provide some sort of structure to the data, by providing a HTML webpage for consumers to navigate. However, Instagram simply provides consumers with data in a series of folders, providing the consumer with little to no contextualisation. People are left to sort through their data with little guidance around what may or may not be important. As a result, consumers may not get a good sense of how their data is collected and processed, which challenges public statements from platforms, who promote the provision of data as a rebalancing of the power dynamics between platforms and the general public (see Tsotsis 2010). We have attempted to

address some of these literacy issues with a visualisation tool for Facebook data, which is available at visualisefacebookdata.com.

Similar issues emerge even when platforms are following best practice. One of the major reasons to provide consumers with access to their data is to give people the option to move their data to another service. All platforms provided this option and could provide data in JSON, the standard format to port data. However, this assumes that consumers have a high level of digital literacy, which is not always the case (Thomas et al. 2018). Industry has appeared to have recognised this and are at the very early stages of developing an intermediary service that will securely port data for consumers.⁴

There are also more systemic issues that the provision of data access cannot solve. The major problem is that **platforms do not provide all the data they hold on individuals**. Anna Weiner, one of the many journalists to download their data from Facebook following the Cambridge Analytica scandal, argues that the ‘information they provide is a slapdash, selective assortment of digital ephemera. It is by no means a complete record of the company’s data-collection practices’ (Weiner 2018). Companies did not provide granular data (i.e. tracking clicks), networked data (i.e. information about relationships between nodes in a social network such as the quality or level of interactions), and most only provided very limited information about how an account interacted with advertisers (although Twitter provided incredibly detailed data about advertiser interactions).

Platforms will rightly claim that some of this information is commercially sensitive. However, they could still provide some general information about data they might hold and assist consumers in developing greater literacy about data collection practices. At the moment, this **information is largely located in ‘long, complex, vague, and difficult to navigate’ privacy or data policies** (ACCC 2018, p. 182). While platforms have started to make consumers more aware about individual privacy settings, they have only started to produce tools to increase consumer understanding of the broader data practices associated with platform use. Facebook’s promised *News Feed* explainer (BBC News 2019) and Google’s and Twitter’s attempts at simplifying their privacy policies are steps in the right direction.

Indeed, privacy organisation noyb (none of your business) has filed a complaint against eight streaming companies for not providing sufficient access to requested data (noyb 2019). The director of noyb, privacy activist Max Schrems stated that:

Many services set up automated systems to respond to access requests, but they often don’t even remotely provide the data to which every user has a right. In most cases, users only got the raw data, but, for example, no information about who this data was shared with (noyb 2019).

While the question of who has a right to networked data is a complex one, we agree that most platforms provided partial data through automated systems. However, as stated above, our major concern is around *literacy*. We are particularly interested in ensuring that people do not just get access to data but are able to understand it.

The transnational nature of digital platforms also raises some interesting jurisdictional issues. While telecommunications companies were specifically oriented towards the legislative goals of the

⁴ You can find out more about the Data Transfer Project at: <<https://datatransferproject.dev/>>.

Privacy Act, social media platforms made no specific reference to ‘personal information’. While it was likely that the provision of data from each platform satisfied this requirement, most companies did not provide a clear way to make use of jurisdictionally-specific rights associated with privacy. This does not mean that these platforms are non-compliant with APP 12 but points to the problems that occur when attempting to make nationally-specific requests of transnational platforms.

Making further requests (or direct requests in relation to APP 12) was difficult. We found an email contact allowing consumers to contact Facebook and Instagram directly, hidden in a help page that could only be found after some determined searching.⁵ Facebook, for example, aims to direct the majority of people to their automated download service and only offers the email when someone wants data after their account has been suspended.⁶ However, as noted earlier, Twitter provides a specific form for data requests beyond what is provided through ‘Your Twitter Data’.

6.3 Google

It is relatively easy to access data from Google. The ‘Google Takeout’ service allows consumers to request data from a variety of Google services. Once you select the services you want, Google will prepare an archive as a ZIP file (see Figure 4). The file can be sent to you via email or directly added to a cloud storage provider (such as Google Drive or Dropbox).

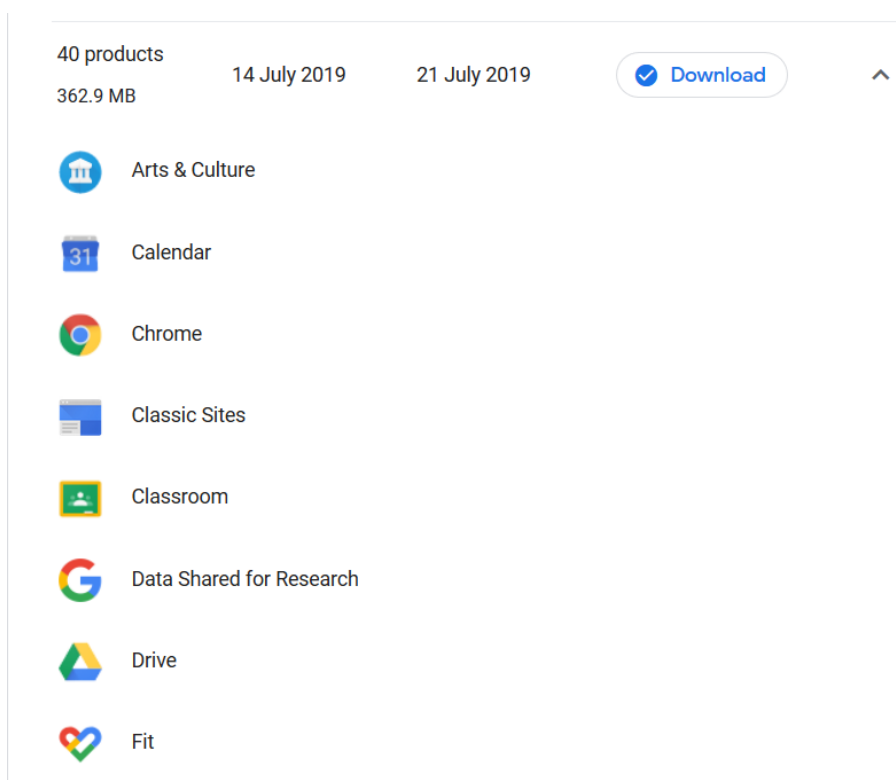


Figure 4 A sample of the data provided by Google

Google faces similar issues to other digital platforms, which we will quickly recap here. They do not provide information about all of their data collection practices; data portability is limited and there is little evidence of any sustained attempt to improve consumers’ data literacy.

⁵ These emails are: <datarequests@support.instagram.com> & <datarequests@support.facebook.com>.

⁶ This can be seen on the following help page: <<https://www.facebook.com/help/contact/180237885820953>>.

The main difference is that these issues are magnified due to the scope of Google’s services and its overarching privacy policy, which allows it to collect and then combine data from individuals across a range of services. Data access did not provide much clarity around how processes worked in practice, which was particularly worrying.

We requested all of the information we could from one team member’s account. Data comes in a variety of formats depending on the service. The scope of data that is provided is also immense with information on everything from YouTube playlists to contact lists from Google+ (plus, now defunct). Dylan Curran, an enterprising web developer, composed a Twitter thread where he explained that Google retained information about the events he attended in the past, due to his use of the Google Calendar, and all the emails he had ever sent through his Gmail account (Curran 2018). The research team made similar findings with respect to their own data.

We were unable to identify a direct contact that would allow us to make further specific requests. It is likely that the provision of information from Google Takeout would fulfil Google’s obligations under the Privacy Act.

6.4 Wearables

We took Fitbit and Apple Watch to be illustrative examples of the wearables sector. The research team used these devices for a number of months then attempted to access our data.

Despite some minor issues, Fitbit has one of the better data access processes. It is a relatively simple procedure, which is easy to enact from the main website. Once you have an account with Fitbit, you can log into your account and make a request to export your data (see Figure 5). You can download up to 31 days of data as a JSON file (although you can use the older process to download your data as an Excel file). This includes data about your activity, body, food, and sleep, depending on how you use the app.

17/10/2018	0									
18/10/2018	0									
19/10/2018	0									
Activities										
Date	Calories Bt	Steps	Distance	Floors	Minutes St	Minutes Li	Minutes F	Minutes V	Activity	Calories
14/10/2018	2,718	8,082	6	2	1,226	142	43	29		1,134
15/10/2018	2,076	2,663	1.98	2	1,362	78	0	0		353
16/10/2018	1,705	0	0	0	1,440	0	0	0		0
17/10/2018	1,705	0	0	0	1,440	0	0	0		0
18/10/2018	1,971	2,795	2.08	2	1,398	3	13	26		307
19/10/2018	876	3,164	2.35	2	682	12	0	0		53

Figure 5 A sample of the data provided by Fitbit

However, there are some problems with this relatively simple process. The major one is the restriction on the *amount* of data you can download. You cannot download all of your data at once. To gain a true picture of your activity, you need to make ongoing data requests. One consumer had to make 24 requests to obtain two years of data (randerson112358 2018). This is a strange

roadblock to introduce and means that regular users of wearable technology struggle to make productive use of this data.

Like other providers, Fitbit also does not return all of the data it collects from consumers. Fitbit collects location information as well some as usage and access information when you use certain online services connected to Fitbit, like their website. This information is not provided to consumers.

While Fitbit was much better than other international companies in facilitating direct requests, similar issues to other providers emerged when we attempted to make a further request. We were told our data was available through the data export tool and Fitbit asked us to make a specific request for any data that we felt was missing. As with other providers, it is likely that the provision of data would already fulfil APP 12. In addition, Fitbit appeared keen to facilitate further requests as opposed to other platforms who either could not support the request or were unable to even facilitate a request in the first place (Google).

We were not entirely successful when we tried to access Apple Watch data. Apple can provide health data but there are some limitations. To access Apple Watch data, we had to go to the Health app on our iPhone where there is an option to export your Health Data in an XML format. The format is not particularly consumer friendly. You can't look at your data and it is impossible to move this data to another device.

As a result, people have to turn to a range of third-party apps that allow you to transfer your Apple Health data from one phone to another (see Health Data Importer) or download your health data (see QS Access). There is even a website that transforms the XML data into a readable CSV file that can be opened in Excel (<http://ericwolter.com/projects/health-export.html>).

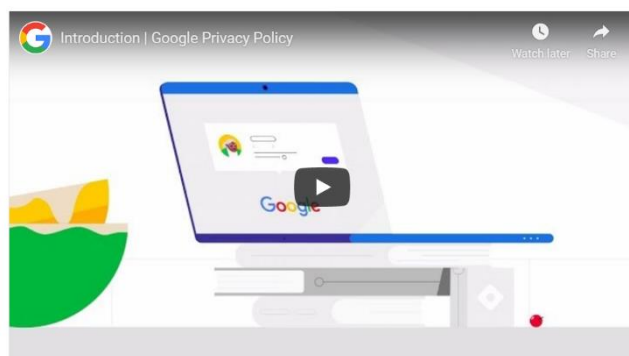
Apple offers guides on how and why it uses consumer data, including how to raise a concern or question, it does not let consumers access or transfer their wearable data easily. It is also hard to request additional data. There is no specific form or contact point where a consumer can make additional data requests (other than for correction of personal data). However, if the broader app ecosystem is taken into account, consumers are ultimately able to access and make use of their Apple Watch data.

7 Data access: Understanding the results

We will now return to our standards to interpret the results of our access attempts.

Transparency of data collection

None of the privacy policies met this standard of transparency. It was unlikely that consumers would be able to get a comprehensive understanding of what data was being collected by these services from the policies provided. We thought it was worth mentioning Google and Twitter, who made some effort to provide supplementary media and key takeaways respectively, to support consumer awareness. However, these efforts do not seem to be working, with the ACCC recently revealing that ‘only 0.03 per cent of devices with an Australian IP address spent more than ten minutes on the Google Privacy Policy web page’ (ACCC 2018, p. 182) – despite attempts to provide simplified policies (see Figure 6). It is worth noting, this is a sector-wide issue, for which there is no easy solution. We still do not know how much information Australian consumers need to provide informed consent before using data-intensive services.



We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads and embedded Google Maps



Twitter is public and Tweets are immediately viewable and searchable by anyone around the world. We give you non-public ways to communicate on Twitter too, through protected Tweets and Direct Messages. You can also use Twitter under a pseudonym if you prefer not to use your name.



When you use Twitter, even if you're just looking at Tweets, we receive some personal information from you like the type of device you're using and your IP address. You can choose to share additional information with us like your email address, phone number, address book contacts, and a public profile. We use this information for things like keeping your account secure and showing you more relevant Tweets, people to follow, events, and ads.



We give you control through your [settings](#) to limit the data we collect from you and how we use it, and to control things like account security, marketing preferences, apps that can access your account, and address book contacts you've uploaded to Twitter. You can also always [download](#) the information you have shared on Twitter.



In addition to information you share with us, we use your Tweets, content you've read, Liked, or Retweeted, and other information to determine what topics you're interested in, your age, the languages you speak, and other signals to show you more relevant content. We give you [transparency](#) into that information, and you can modify or correct it at any time.



If you have questions about this policy, how we collect or process your personal data, or anything else related to our privacy practices, we want

Figure 6 An attempt at providing simplified policies

Ease of data access

It was easy for us to access our data independently, or with customer support, across the vast majority of companies. Two companies did not meet this standard.

Vodafone needs to make minor improvements to its access process. Vodafone's data access processes were not easy to find, and it was unclear what data they could provide from the information displayed publicly. However, their standards improved dramatically once contact was made with their privacy team.

Optus needs to make major improvements. There is no simple process for consumers to access personal information, resulting in a confused and unclear facilitation of requests.

Scope of data provision

Telstra and Vodafone stood out with their willingness to provide a broader suite of data (beyond what they are legally required to do), for a fee. While we did not make use of this option, there were clear organisational procedures for us to follow if we decided to take this step.

However, the majority of companies did not provide all of the information they collected. As stated above, this was either due to poor processes making the original request difficult (Optus), or because companies only provided a limited amount of data (Facebook, Instagram, Fitbit, Apple Watch).

While it is likely that the above companies provided what they were legally required to under APP 12, we expected much more information to be returned from social media platforms, wearables and Google, considering their significant data collection processes. That being said, we want to recognise Google for providing an extensive (but not exhaustive) amount of data and Twitter, for providing information on advertising targeting, which is often not provided by social media platforms.

Further assistance and additional data requests

Vodafone, Telstra and Twitter stood out for having privacy requests handled by a privacy team that was easy to contact. They also allowed consumers to make additional data requests and established clear processes for doing so.

Fitbit gave support through a customer service team, which was relatively capable at guiding initial privacy requests and handling additional requests.

Every other company needed improvement. Facebook and Instagram have a privacy team, but their contact details were hidden away in an obscure public facing document. As noted earlier, Optus' systems were not set up to specifically facilitate data requests. There was no ability to contact someone at Google or Apple to specifically inquire about data access.

Data portability

Every service needed to improve in this area. While social media platforms, Fitbit and Google provided files in the (industry standard) JSON format (that helps people move data), this format would be meaningless to most consumers. Telecommunications companies did not even provide data in a machine-readable format. In the current climate, it would be impossible for an average consumer to move their data between services.

Summary of results

No organisation is currently adhering to what we have defined as 'best practice' data access across the communications sector. However, we do want to mention Telstra, Vodafone and Twitter who at various times, showed some consistency with respect to facilitating further requests, providing direct points of contact that were easy to find and in being able to provide a broad scope of data in

the context of their industry (Telstra and Vodafone) or some data that was not offered by other competitors (Twitter).

Considering these results, it is unsurprising that the Coalition government wants to introduce a CDR to facilitate better access and transfer. We will now turn to the specifics of the Bill and evaluate its effectiveness.

8 Assessing the Consumer Data Right

We have already outlined the basic function of the CDR in the background section from Chapter 3 of the report. The CDR allows Australian consumers (who can be either individuals or businesses), to direct companies to transfer specified data to a competitor or an accredited third-party service. Consumers can use the Right to meaningfully compare prices between companies based on their own consumption patterns or to maintain historical records while moving across services.

In the following section, we outline how the CDR will function and offer a critique of the Right as it currently stands, with reference to draft legislation, submissions from stakeholders, international examples, academic scholarship and findings from our own research. This analysis is based on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018*, which was introduced to Parliament in early February this year for consideration. A Senate Economics Legislation Committee recommended that the bill be passed unamended, which the Coalition government is likely to do.

There are still substantive issues with the CDR. As a result, we offer the following critique with the goal of contributing to possible amendments in the future.

We consider:

- Terminology used by the legislation.
- What sort of data will be captured by the legislation.
- How the CDR intersects with existing privacy and data protection frameworks.
- The benefits and risks of standardisation and accreditation.
- Levels of consumer engagement with data.

We close by providing an overall assessment of the CDR as a policy instrument and Australia's overall data policy framework.

8.1 CDR terminology

Before we assess the CDR in detail, we will briefly outline the specific terminology used by the CDR legislation, which is common throughout the draft.

A **consumer** is a person who is 'identifiable' or 'reasonably identifiable' from CDR data (Consumer Data Rights Bill 2019, 56AD(3b)). A consumer can be an individual or a business (Consumer Data Right Bill 2019, s. 56AD(1)).

A **data holder** is anyone (person or business) who holds data that the Treasurer has designated should be subject to the CDR (Consumer Data Right Bill 2019, s. 56AG).

An **accredited data recipient** is a person who has been accredited to receive data. At this stage, the ACCC is expected to provide accreditation in the initial period of the CDR's operation.

8.2 What is consumer data and should consumers pay for it?

The CDR provides access to more data than Australian privacy laws currently allow, which, as we have already noted, only allows individuals to access their personal information. Under the CDR, Australian consumers can access a range of data that relates to them, which may include data generated through the use of a particular service. The CDR may also apply to value-added data because the draft legislation allows the Treasurer to specify what data should be included from specific sectors (Consumer Data Right Bill 2018, s. 56AC(2)(a)), following a consultation period with stakeholders. A subsequent clause also places data that has been derived from that initial designation within the scope of the CDR, which implicates data that a company may have transformed in some way (Consumer Data Right Bill, s. 56A1(2)).

This initial framing is an issue because the legislation is vague about what is included in the CDR. While the Productivity Commission recommended that '[d]ata that is solely imputed by a data holder to be about a consumer may only be included with industry-negotiated agreement' (Productivity Commission 2017, p. 36), this certainty is not reflected in the legislation.

It is important to note that the Treasury is keen to ensure that 'there is no loophole to exclude CDR data from the protection of the CDR regime by transforming the data in an immaterial way' (Allens 2018). The ACCC is also tasked with creating specific rules for each sector, after the Treasurer decides to introduce the CDR to a sector. As a result, these sector-specific rules should provide some clarity. However, there is a risk that companies will not transform data sets, because 'they could be required to disclose this valuable data to their competitors' (Allens 2018).

This leads us to a fundamental problem: who owns data? In its current form, the CDR captures some value-added data – the scope of which is unclear. This suggests that the Australian Government wanted consumers to have access rights to at least some of this data. However, there is also a strong argument that value-added data is the result of significant business investment and should be treated as such, with companies able to withhold datasets in order to retain a competitive advantage. The outline of the rules for Open Banking show that the ACCC has taken a cautious approach and specified that customer data, account data, transaction data and product data should be included in the data set (Competition and Consumer (Consumer Data) Rules Exposure Draft 2019, 2.2, p. 87).

We believe that consumers should have a right to access some of this data, however the level of access should also be clarified. The Productivity Commission has already provided some guidance, suggesting that consumer data, which 'is not able to be re-identified to a consumer in the normal course of business within a data holder should not be considered consumer data' (Productivity Commission 2017, p. 36). This is a sound approach and would give consumers access to most of the relevant data produced about them by companies.

However, we suggest that companies should be encouraged to share more data if they choose to do so. We note that there is a bipartisan appetite across the Australian Parliament to invest in and develop a data economy. However, one of the challenges for business is that participation requires data to be a shared proposition and not just something that is taken from consumers. Venture capital firm Reinventure notes that 'joint ownership' is a viable approach in such an environment

(Gilligan 2018, p. 18). We agree with this approach and argue that industries should become **more comfortable with sharing their data with consumers**.

The existing bill proposes that companies should be able to charge for access to data, with the ACCC only intervening if fees become too high. We suggest that there should be a clear delineation of fees within the legislation, with basic consumer data provided for free. Companies should be able to charge for any value-added data they choose to provide but following the recommendation of CHOICE, '[c]onsumers should be able to gain access to non-essential data sets for free at least once a year' (CHOICE 2019, p. 7). We also follow CHOICE's suggestion that the ACCC should be able to 'set a price for data access' (CHOICE 2019, p. 7).

8.2.1 Recommendation 1

Companies should be required to provide basic consumer data. This should be defined as identifiable data or data that can be re-identified to a consumer in the normal course of business.

8.2.2 Recommendation 2

Basic consumer data should be provided for free.

8.2.3 Recommendation 3

Further data provision should be accessible for free once a year, with further requests available at a cost set by the ACCC.

8.3 Privacy and governance framework

As noted earlier, a series of 'Privacy Safeguards' are slated to be introduced to govern the CDR, superseding the APP. This comes with some benefits.

The safeguards are variously applied to entities that hold and receive data and largely align with existing APPs. However, the fact that these safeguards apply to a broader range of data significantly enhances existing protections, at least with respect to access and portability. There are also stricter consent requirements, with consent required to be part of an opt-in process, which is 'voluntary, express, informed, specific as to purpose, time limited and easily withdrawn' (Competition and Consumer (Consumer Data) Rules Exposure Draft 2019, 4.10, p. 32).

As noted earlier in this report, these safeguards may also improve privacy compliance more generally. Many small and medium businesses are not currently bound by the Privacy Act because they have a turnover of less than \$3 million. However, if any of these organisations want to be accredited recipients, they will have to adhere to these safeguards to receive data. Consumers are also able to bring an action against a party in the case of a data breach, which provides individuals with a rare cause of action around their privacy rights.

While these are positive steps, **we question the need to introduce new privacy safeguards**. The introduction of the safeguards would see two competing frameworks aim to regulate the privacy of Australians, alongside a range of other legislative instruments that relate to privacy (from trespass to anti-surveillance laws).

The introduction of privacy safeguards adds to this complicated legal framework. Businesses will now have to comply with APPs and new safeguards. They will also have to reform their data management practices, as CDR data will need to be handled differently from other data (Allens 2018). The CDR introduces a complex compliance framework that will be hard to operationalise.

For Australians, the safeguards are equally confusing. As some stakeholders have noted during consultations, the CDR is a misnomer (Consumer Policy Research Centre 2019). While there are a range of laudable protections for individuals, these only come into play when data is transferred. As a result, Australians will also be dealing with a multi-tier privacy framework, with personal information regulated by the APPs, a broader set of data regulated by the CDR safeguards and their privacy interests partially regulated by these instruments alongside a mixture of statutory and common law.

The proposed introduction of safeguards forms part of a broader bureaucratisation of privacy in Australia, with statutory bodies, regulatory instruments and bureaucratic processes favoured over substantial legislative reform. To briefly divert from the CDR, further evidence of this can be found in the recent ACCC *Digital Platforms Inquiry – Preliminary Report* (2018), where proposals to amend the Privacy Act have been floated. The ACCC is proposing to strengthen the definition of consent and introduce notification and erasure rights for consumers’ personal information. While these are laudable reforms, one of the authors of this report has noted concerns with this reform in a submission to the inquiry (Wilding, Fray, Molitorisz & Meese, 2019).

Firstly, “personal information” is too narrow a phrase to capture much of the data that is relevant for current purposes’ (Wilding et al. 2019, p. 11). As this study has shown, a significant portion of data that may be relevant to consumers does not fall under the legal definition of ‘personal information’. Secondly, the introduction of such a definition could lead to a confusing ‘two-tier system of data rights’ (Wilding et al. 2019, p. 11) with different data held to rules for access, erasure and notification.

The overall result is a series of overlapping and confusing processes and policies, which consumers and businesses will struggle to grapple with. We suggest that the Australian Government should instead introduce a substantive foundational rights framework for Australians in relation to their data rather than continuing to approach privacy through a narrow regulatory lens. This framework could introduce a new definition of data, replacing what promises to be an awkward divide between ‘personal information’ and ‘consumer data’ and establish new principles, drawing on the privacy safeguards and the existing APPs.

8.3.1 Recommendation 4

The CDR should form part of a broader suite of comprehensive data rights for consumers.

8.4 Standardisation

There are multiple benefits to **standardisation** and **this is one of the CDR’s central victories**. One of the major problems that emerged when we tried to access data was that data would be provided in a range of different ways. Although APP 12 specifies that access to personal information must be given ‘in the manner requested by the individual’, data was often provided through a standard process with no choices on offer. As noted earlier in our report, we received data in every format

from HTML files to PDFs and as a result, some of the data was not portable. It would have been difficult (if not impossible) to transfer relevant data to another provider. Subsequently, the promise of being able to access and transfer data easily across a sector remains one of the key benefits of the CDR. The ongoing issue is the need to agree on suitable data formats for each sector, leading to the issues discussed in the data section above.

8.5 Accreditation

Accredited data recipients will receive data from data holders and consumers, and the ACCC has provided the details of the initial accreditation process. There will be one initial level of accreditation, although there are likely to be more levels in the future to ‘accommodate business models that use third party intermediaries to collect and/or hold CDR data’ (Allens 2019). The first round of applicants will be required to:

- Be ‘fit and proper persons’.
- Have appropriate procedures in place to manage information security risks.
- Have internal dispute resolution processes.
- Adequate insurance in case the applicant needs to pay a fine after a breach (Competition and Consumer (Consumer Data) Rules Exposure Draft 2019, 5.11, p. 45).

They must also provide information about the services ‘they intend to offer consumers using CDR data as an accredited data recipient’, which may include things like ‘template consent screens and descriptions of security controls and mitigation measures, and procedures for the reporting of incidents and notification processes to consumers’ (Allens 2018). Once accredited, recipients would be required to be on a register and be willing to participate in an audit and compliance program. The ACCC will also be able to suspend or revoke accreditation for a range of reasons.

Foreign entities may also be accredited (Competition and Consumer (Consumer Data) Rules Exposure Draft 2019, 5.2, p. 40). In addition to going through the standard accreditation process, entities are required to hire a local agent who will be responsible for adhering to obligations, in a similar manner to the *Corporations Act 2001* (Cth) (Competition and Consumer (Consumer Data) Rules Exposure Draft 2019, 5.11, p. 45). Importantly, the legislation states that investigations can either be launched by the OAIC or with the support of the ACCC, and there must be an established internal system for consumer complaints as well as recourse to an external disputes resolution scheme (Competition and Consumer (Consumer Data) Rules Exposure Draft 2019, 5.11, p. 45). This suggests that companies that attempt to evade audits and other regulatory tools will not be looked upon kindly.

While the ACCC has released a detailed exposure draft of the rules relating to the use of the CDR in banking, some general issues around accreditation have emerged. One central concern is that the explanatory memorandum to the draft legislation suggests consumers will be able to move their data to entities without accreditation. There are no further details available to provide context around this provision but it suggests that there are tensions between the relatively rigorous accreditation process and the vision of continuous data flows between businesses and consumers envisaged by the Productivity Commission (2017) report.

Indeed, the banking sector has raised concerns about this mismatch between vision and reality in response to the government's draft Privacy Impact Assessment (PIA) into the CDR. The Australian Banking Association argued that the risk of a phishing attack or 'unauthorised access to consumer data' was higher than the 'unlikely' rating presented in the PIA (Hang 2019, p. 2). There is a whiff of incumbency to these complaints and indeed, banks have not wholly embraced the CDR, which will potentially support the rise of competing 'fintech' companies. However, banks also have a long record of managing sensitive data and their concerns point to the importance of ensuring data moves securely across multiple parties. **There should not be any possibility of data moving outside the relatively rigorous accreditation system.**

Furthermore, there is a broader sense that **government should pay greater attention to the risks** around ongoing data transfers between consumers and businesses. As we discuss later on, the government has developed a consistently positive narrative around the CDR, which veers on what privacy researcher Professor Helen Nissenbaum calls '**Big Data Exceptionalism**' (2017, p. 4). There is **a tendency to ascribe unclear benefits to big data**, which are unable to be tested prior to the introduction (or reform) of legislation. This is not to suggest that the CDR should be wholly abandoned, but rather to encourage a more critical and conservative approach to risk, in line with some of the already strong protections within the draft legislation and initial rules. Indeed, one suggestion made by multiple stakeholders is to formalise a review period for the rules and data sets (see Business Council of Australia 2019, p. 4; CHOICE 2019, p. 3). This is a sound proposal that embraces the necessary caution required for an economy wide reform.

8.5.1 Recommendation 6

Consumer data should not move outside of the accreditation system.

8.5.2 Recommendation 7

The regulatory frameworks around the CDR should be reviewed every three years.

8.6 Consumer and business attitudes

Another major factor in the CDR debate is the actual attitudes and behaviours of consumers and businesses. Stakeholders have focused around the minutiae of the Bill, but the public debate has largely glossed over whether the key actors will engage with the CDR. Indeed, the government bodies have been incredibly optimistic in their public announcements.

The initial outcomes of the United Kingdom's Open Banking reforms provide a good example of the significant cultural change that is involved with these reforms. The reforms effectively forced the United Kingdom's 'nine biggest banks [...] to release their data in a secure, standardised form, so that it can be shared more easily between authorised organisations online' (Manthorpe 2018). However, uptake in the United Kingdom has been slow with much of the public not aware of the potential benefits (Baclin 2018), organisations not actively using the APIs of major banks (Dinneen 2018; Manthorpe 2018) and the major banks failing to substantially embrace the reforms themselves (Withers 2018).

Some of the above issues can be attributed to the incumbency of the banks and the complexity of the reforms. However, there is evidence of limited consumer engagement in the United Kingdom

(Baclin 2018) and a similar situation may occur in Australia. Indeed, the limited use of existing rights points to potential problems with the CDR. As noted earlier, only around a third of Australians (37%) know they can access their information from government and businesses, and there is no data available that tells us how regularly the right is used (Van Souwe et al. 2017, p. 15). Obviously, the CDR will be of greater use to Australians than the existing APP 12, but the above data shows that most Australians do not actively engage with their existing access rights.

It will be up to businesses to solve the engagement problem. The OAIC will launch public education campaigns around the CDR, but it will be the tools and services that business provides that will contribute to the success or failure of the Right. Consumers will only use the Right if it assists in the ongoing administration of their lives in an easy and effortless manner. This is a relatively simple argument, but it is important to emphasise. In the same way that government needs to attend to risk, it also needs to refine its optimistic narrative and be prepared for the likelihood of a slow roll out phase. We are not offering a recommendation here, but rather just noting that there is a track record of limited engagement with existing rights and comparable reforms.

The policy debate has also ignored questions around inclusion. The value of the CDR will be realised in the exchange of digital data. However, this excludes those without internet access, and even those with internet access may find it difficult to use the CDR if they have limited digital literacy. One of the most important research projects in recent years has been the creation of an *Australian Digital Inclusion Index*, which aims to track how many people in Australia have access to technology, whether they can afford it and if they have the skills to use it. The 2018 report notes that there are currently 'more than 2.5 million Australians who are still not online' (Digital Inclusion in Australia n.d.), and most critically for our report, has found that 'Australians [...] struggle to keep up with new technologies, and relatively few users engage in more advanced activities' (Thomas et al. 2018, p. 15).

The CDR promises to help consumers navigate confusing and complicated markets, such as banking, telecommunications and energy. Some financial decisions may result in substantial savings. For example, consider the financial benefits that will accrue to a household that finds a cheaper mortgage thanks to the CDR. There has been little discussion about what will happen to individuals who either do not have internet access, or do not have the skills to engage with the Right effectively. While business should be responsible for ensuring broad consumer engagement with the Right, it is the responsibility of government to address these issues around inclusion. If the CDR is indeed a long-term project, there needs to be a greater recognition of the long-term inequalities that may emerge from the reform, if the broader issue of digital inclusion is not adequately addressed.

There is also a need to consider the potential inequalities that may emerge as businesses centralise their data handling and management procedures (Eyers 2018). Some banks have kept data in separate silos and the introduction of the CDR is forcing them to combine this customer data (Eyers 2018). This may cause banks (and in the future, other businesses) to develop a more accurate picture of their customers and potentially be able to discriminate accordingly. As a result, protections need to be put in place to protect consumers from 'the potential emergence of data discrimination' (Eyers 2018). We suggest that this important facet of the reform has not received much attention. One option would be to ensure that consumers can delete their own data, drawing on a similar recommendation from the ACCC *Digital Platforms Inquiry – Preliminary Report* (2018),

which suggests that this could occur when consumers 'have withdrawn their consent' and such data 'is no longer necessary to provide the consumer with a service' (ACCC 2018, p. 13).

The other side of this coin involves businesses keeping ethical considerations front of mind. Ultimately, the above issues are not just about data collection, but more about how and when to use data. Indeed, data misuse may not involve any breach of law, but may simply involve the use of data in invasive or harmful ways. The recent Banking Royal Commission stands as an important reminder for all sectors to keep the customer in mind rather than profits when working with data. We would encourage businesses to be mindful of their social obligations when using data and consider viewing ethical data handling as something that can give companies a competitive edge, considering the ongoing concerns of the Australian public.

8.6.1 Recommendation 8

The Australian Government needs to develop an inclusion plan to ensure that the CDR is accessible to all Australians.

8.6.2 Recommendation 9

The Australian Government should consider introducing data erasure, which will protect consumers against data discrimination.

8.7 Scope

The current bill also expands the scope of the right dramatically. The explanatory memorandum states that a consumer can be 'an identifiable or reasonably identifiable person, including a business enterprise' (Explanatory Memorandum, 2018, 1.100). Importantly, there is no limitation on the size of the business, which ignores the specific recommendation of the Productivity Commission, which only focused on individuals and small and medium sized businesses. Indeed, they stated that the right would apply to 'single persons, family groups or other groups resident at a single address in the data holder's dataset, and any entity with an Australian Business Number and turnover of \$3 million per annum or less' (Productivity Commission 2017, p. 198). There is little justification for providing large businesses with improved access to data through a bill designed largely for individual consumers.

8.7.1 Recommendation 10

The Right be restricted to individuals and small and medium businesses.

8.8 A new Australian data policy framework

In spite of the criticisms detailed above, we believe that the CDR is an innovative reform that will function as a useful access and transfer right for Australians. It will effectively streamline many of the issues that we encountered when trying to make use of the data access rights currently available to Australians. It is highly likely that new competitors will be able to make use of this framework to enter existing industry sectors.

However, we continue to be concerned around the excessively positive language surrounding the Right and suggest that a range of issues related to privacy, inclusion and prospective discrimination

have not been adequately addressed in the Bill's current state. We also note that consumer engagement may be difficult to achieve initially. Importantly, many of these issues affect businesses as well as consumers and so may ultimately limit the overall effectiveness of the rollout. But even reform will not solve the major problem with the bill: the disaggregated reform agenda around data.

As noted earlier, there are currently four different policy processes being undertaken, which to a greater or lesser extent focus on how to regulate the personal data of Australians. This report has focused on the CDR. However, it has noted that the Digital Platforms Inquiry (ACCC 2018) has tabled possible reforms to Australian privacy law in its preliminary report. In addition to these reforms, there are proposals to make it easier for public data to be shared (Data Sharing and Release, see Department of the Prime Minister and Cabinet 2018) and the Australian Human Rights Commission (AHRC) is reviewing how human rights and technology intersect (see <https://tech.humanrights.gov.au>).

These competing reviews and reforms are creating a confusing policy landscape. The CDR and ACCC are already proposing to amend different parts of the Competition and Consumer Act and Privacy Act. It is likely that the AHRC will recommend similar reforms. In addition to this, the proposed Data Sharing and Release legislation will dramatically change how Australian Government agencies handle data.

There is scope for Australia to establish a functioning data economy but there needs to be an appetite for a broader reform agenda that provides a strong legislative foundation for businesses and consumers. Only the CDR has been tabled in Parliament. The Data Sharing and Release draft Bill is still forthcoming, along with the Final Reports from the Digital Platforms Inquiry and the Human Rights and Technology project.

We suggest that the government should wait for the publication of these reports, rather than rushing towards reform. Drawing from these various reform processes will mean that consumer protection, consumer privacy, data access and transfer and fundamental rights can be addressed collectively. It will provide some coherence to these different (and often competing) agendas and give Australian consumers and businesses a much clearer understanding of their rights, obligations and opportunities with respect to their data.

This should result in substantial reform to key legislation like the aforementioned Competition and Consumer Act and Privacy Act and avoid a patchwork effort that results in confusing legislation and excessive red tape. Most importantly though, there is the potential to establish a comprehensive series of rights for Australians (including the right to access and move data), allowing them to participate with more confidence in a data-driven economy.

8.8.1 Recommendation 11

A range of issues related to privacy, inclusion and prospective discrimination must be adequately addressed in the proposed Bill.

8.8.2 Recommendation 12

A holistic approach must be taken rather than the introduction of a series of disconnected reforms.

9 Beyond data access: Conclusions and next steps

This project has assessed the state of data access in the communications sector, with a specific focus on data-intensive products and services. After trying to access data from across the communications sector, we found that those processes were convoluted and diverse with no clear standard across each product and/or service category. Following this, we analysed the CDR, which promises to solve this issue. We found that the reform was innovative at a broad level, but there were issues with the proposed legislation, and it did not solve many of the other problems associated with information asymmetry.

Our overarching recommendation is that data access should be simplified and standardised. By standardisation of data access, we mean multiple things. Firstly, we mean the manner in which data is accessed (either physical, electronic or both as appropriate). Secondly, we mean the format on which data can be accessed and downloaded. Thirdly, we mean the amount of data being captured and subsequently being made available for portability purposes.

This connects to our second major recommendation, which relates to the CDR. Australia is about to introduce the Right and our findings have shown that such a reform is needed. However, we suggest that the Right as it currently stands is poorly structured. We recommend that a revised Right form part of a broader comprehensive data policy framework equivalent to the European Union's GDPR.

This is because while data access has been the focus of our report, 'data protection' is the elephant in the room that also needs to be addressed. By data protection, we mean looking for the balance between data privacy and data exploitation in a data-driven economy. Data protection is a double-edged sword: on the one hand companies state that they are only seeking consumer data to provide services, while on the other hand, we know that this data is being used and shared by various parties (Federal Trade Commission 2014) and consumers have limited information about these processes.

Throughout our research process we have observed that post-GDPR and the Facebook-Cambridge Analytica scandal, both consumers and companies have turned their attention towards data protection. Consumers are not just accessing data because they want to move it somewhere else, they are also accessing data to have both a sense of agency and ownership, as well as to understand the manipulation of their data.

The focus of our work here has been to understand how organisations 'respect' one specific data right: the right to access data. However, we have also engaged with data protection issues through our studies of organisational privacy policies. So in closing, we present some general thoughts about data protection that have emerged from our research. In doing so, we refer to general trends we have identified and do not address specific companies.

We will begin with observations around consumers accessing their data. While most companies we researched did offer consumers their personal information (or other data), there was either very little or no information about what these companies did with consumer data. In short, the data

provided was not contextualised. A company may use a consumer's data as part of a dataset to understand broader consumer patterns, but this information was not readily available to consumers (apart from in convoluted privacy policies). One element of protection involves literacy, which requires companies to adequately inform consumers how their data is being used. A combination of access and literacy can form part of a broader strategy that supports consumer empowerment and engagement around data.

Another issue relates to the amount of data being captured by companies. Some companies seem to be operating with the twin logic of 'no data is bad' and 'all data is valuable'. This approach sets in motion the potential for data exploitation. While this sort of mindset is difficult to change, we believe that companies must focus only on capturing data that is necessary for their business model. Essentially, companies should only be collecting information closely related to the functioning of their services and not monitor or record consumer information beyond the purview of their services. Legislation can play a big part here, but there also needs to be a cultural change amongst data-driven organisations.

Our own report and other regulatory bodies have also noted that existing privacy policies need to change (ACCC 2018). We have outlined issues with privacy policies earlier in the report. However, we also want to highlight the need for ongoing engagement with consumers about data use. While companies sell or transfer data to third-parties, consumers generally do not know how or when this occurs. We suggest that more research needs to be done on how consumers could potentially be made aware of these transactions to ensure that they are providing their explicit consent to these transfers at a relevant point in the process (i.e. not just when they sign up for a service).

The final point we would make is data cannot only be seen as an economic resource. It also relates to people's fundamental rights. While we support the general aims of the proposed CDR, we do so with a recognition that much of our contemporary social and political lives occur online, not simply our economic interactions.

Subsequently, future policy frameworks must ensure that we have a sense of control over our lives – or in this case, 'our data'. There is still a heavy focus on the economic outcomes that will result from the CDR. Data regulation in Australia must do more to build a concept of data citizenship.

Voice is a fundamental aspect of citizenship. As citizens of a nation, our voice is empowered through various electoral and non-electoral processes including formal elections, petitions, protests and the ability to meet with our elected representatives. Individuals also need to feel that they have a voice with respect to how their data is used and managed. The risk is that if the data we manufacture in our online lives simply goes into a 'black box', we lose any sense of empowerment – something that ultimately undermines our sense of citizenship.

In summary, we started our research questioning the state of data access in the communications sector, with a specific focus on data-intensive products and services. While the question we asked, can consumers access their own data seemed simplistic, as we have shown, the answers and consequences are more wide-ranging.

Authors

James Meese

Dr James Meese is a Senior Lecturer at University of Technology Sydney. He holds an early career research fellowship from the Australian Research Council to study the algorithmic distribution of media content. His two books are *Authors, Users, Pirates: Subjectivity and Copyright Law* (MIT Press) and *Death and Digital Media* (Routledge, co-authored).

Punit Jagasia

Dr Punit Jagasia is a Research Associate at University of Technology Sydney and Casual Academic at University of Sydney. His research focuses on social media, mobile apps and data access. Punit has also worked in the marketing communications industry for over twelve years.

James Arvanitakis

Professor James Arvanitakis is a Researcher at the Institute for Culture and Society, Western Sydney University. He is also the Millard Simpson Chair of International Relations at the University of Wyoming – a position awarded as part of a Fulbright Fellowship. He is a regular media commentator on ABCNews24 and researches the areas of citizenship, future of universities and data ethics.

Abbreviations

AHRC	Australian Human Rights Commission
APP	Australian Privacy Principle
CDR	Consumer Data Right
GDPR	General Data Protection Right
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment

References

ACCC—see Australian Competition and Consumer Commission

Allens 2018, 'The devil in the detail – observations on the scope of CDR data and the new Privacy Safeguards', *Allens*, viewed 20 May 2019, <<https://www.allens.com.au/pubs/priv/cdr-18sep/article-04.htm>>.

—2019, 'Client Update: ACCC releases draft Consumer Data Right Rules for consultation', *Allens*, viewed 20 May 2019, <<https://www.allens.com.au/pubs/priv/cupriv15apr19.htm>>.

Arvanitakis, J. 2017, 'If Google and Facebook rely on opaque algorithms, what does that mean for democracy?', *ABC Online*, 11 August, viewed 20 May 2019, <<https://www.abc.net.au/news/2017-08-10/ai-democracy-google-facebook/8782970>>.

Australian Competition and Consumer Commission 2018, *Digital Platforms Inquiry – Preliminary Report*, Australian Competition and Consumer Commission, Canberra.

Australian Digital Inclusion Index n.d., *Digital Inclusion in Australia*, Australian Digital Inclusion Index, viewed 20 May 2019, <<https://digitalinclusionindex.org.au/about/about-digital-inclusion/>>.

Australian Privacy Foundation 2017, 'Submission to The Treasury', *Open Banking Review – Issues Paper*, 5 November, viewed 20 May 2019, <<https://treasury.gov.au/consultation/review-into-open-banking-in-australia>>.

Baclin, D. 2018, 'Open Banking – nine months on, does slow and steady win the race?', *UKTN*, 29 October, viewed 20 May 2019, <<https://www.uktech.news/news/industry-analysis/open-banking-nine-months-on-does-slow-and-steady-win-the-race-20181029>>.

BBC News 2019, 'Facebook to reveal News Feed algorithm secrets', 1 April, viewed 20 May 2019, <<https://www.bbc.com/news/technology-47771922>>.

Business Council of Australia 2019, 'Submission no. 9 to the Economics Legislation Committee', *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, 28 February, viewed 20 May 2019, <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABConsumerDataRight/Submissions>.

CHOICE 2019, 'Submission no. 23 to the Economics Legislation Committee', *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, 28 February, accessed 20 May 2019, <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABConsumerDataRight/Submissions>.

Consumer Policy Research Centre 2019, 'Submission no. 5 to the Economics Legislation Committee', *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, 28 February, viewed 20 May 2019, <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/TLABConsumerDataRight/Submissions>.

Curran, D. 2018, 'Are you ready? This is all the data Facebook and Google have on you', *The Guardian*, 30 March, viewed 20 May 2019, <<https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>>.

Department of the Prime Minister and Cabinet 2018, *New Australian Government Data Sharing and Release Legislation: issues paper for consultation*, Department of the Prime Minister and Cabinet, Canberra.

Dinneen, L. 2018, 'UK Open Banking six months later', Medium, 16 August, viewed 20 May 2019, <<https://medium.com/@lauradinneen/uk-open-banking-six-months-later-60cd522e66e8>>.

Esayas, S. & Daly, A 2018, 'The Proposed Australian Consumer Right to Access and Use Data: A European Comparison'. *European Competition & Regulatory Law Review*, vol. 2, no. 3, pp. 187-202.

Eyers, J. 2018. 'Open banking: Consumer data rights a double-edged sword for financial sector', *Australian Financial Review*, 20 December, viewed 20 May 2019, <<https://www.afr.com/business/banking-and-finance/open-banking-consumer-data-rights-a-doubleedged-sword-for-financial-sector-20181220-h19bgw>>.

Federal Trade Commission 2014, *Data Brokers: A Call for Transparency and Accountability*, Federal Trade Commission, Washington, viewed 20 May 2019, <<http://permanent.access.gpo.gov/gpo49352/140527databrokerreport.pdf>>.

Flyvbjerg, B. 2006, 'Five misunderstandings about case-study research', *Qualitative inquiry*, vol. 12, no. 2, pp. 219-245.

Forbrukerrådet 2018, *Deceived by Design*, Forbrukerrådet (Norwegian Consumer Council), 27 June, viewed 20 May 2019, <<https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>>.

Gilligan, D 2018, *Global Data Wars: Building a Thriving Data Economy for Australia*, Reinventure, viewed 20 May 2019, <<http://reinventure.com.au/wp-content/uploads/2016/10/GlobalDataWarsReportReinventure.pdf>>.

Goggin G, Vromen A, Weatherall K, Martin F, Webb A, Sunman L & Bailo, F 2017, *Digital Rights in Australia*, University of Sydney, Sydney.

Granvill, K 2018, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens', *The New York Times*, 19 March, 20 May 2019, <<https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>>.

Hang, D 2019, *Response to Treasury: Privacy Impact Assessment – Consumer Data Right*, Australian Banking Association, 18 January, viewed 20 May 2019, <https://www.ausbanking.org.au/wp-content/uploads/2019/01/PIA_CDR.pdf>.

Hoeren, T 2014, 'Big data and the ownership in data: recent developments in Europe', *European Intellectual Property Review*, vol. 36, no. 12, pp. 751-754.

- Johnston, A 2017, 'Mobiles, metadata and the meaning of 'personal information'', *Salinger Privacy*, 19 January, viewed 20 May 2019, <<https://www.salingerprivacy.com.au/2017/01/19/federalcourtdecision/>>
- Kemp, K & Vaile, D 2018, 'Soft terms like 'open' and 'sharing' don't tell the true story of your data', *The Mandarin*, 2 May, viewed 20 May 2019, <<https://www.themandarin.com.au/92040-soft-terms-like-open-and-sharing-dont-tell-the-true-story-of-your-data/>>.
- Larsson, S 2018, 'Algorithmic governance and the need for consumer empowerment in data-driven markets', *Internet Policy Review*, vol. 7, no. 2, DOI: 10.14763/2018.2.791.
- Langheinrich M, 2001, 'Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems', in Abowd GD, Brumitt B, Shafer S (eds), *UbiComp 2001: Ubiquitous Computing. UbiComp 2001. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 2201, pp. 273-291.
- Livingstone, S 2019, 'Audiences in an age of datafication: critical questions for media research', *Television & New Media*, vol. 20, no 2, pp. 170-183.
- Mahieu, RLP, Asghari, H, van Eeten, M 2018, 'Collectively exercising the right of access: individual effort, societal effect', *Internet Policy Review*, vol. 7, no. 3, DOI: 10.14763/2018.3.927.
- Manthorpe, R 2018, 'What is Open Banking and PSD2? WIRED explains', *Wired Magazine*, 17 April, viewed 20 May 2019, <<https://www.wired.co.uk/article/open-banking-cma-psd2-explained>>.
- Murphy, D 2018, 'What's In Your Instagram Data Dump And How To Get It', *Lifehacker Australia*, 12 May, viewed 20 May 2019, <<https://www.lifehacker.com.au/2018/05/whats-in-your-instagram-data-dump-and-how-to-get-it/>>.
- Nguyen, P & Solomon, L 2018, *Consumer Data and the digital Economy*, Consumer Policy Research Centre, Melbourne, viewed 20 May 2019, <https://cprc.org.au/wp-content/uploads/Full_Data_Report_A4_FIN.pdf>.
- Nissenbaum, HF 2017, 'Deregulating Collection: Must Privacy Give Way to Use Regulation?', *SSRN*, 1 May, viewed 20 May 2019, <<https://ssrn.com/abstract=3092282>>.
- noyb 2019, 'noyb files eight strategic complaints on 'right to access'', *European Digital Rights*, 28 January, viewed 20 May 2019, <<https://edri.org/noyb-files-eight-strategic-complaints-filed-on-right-to-access>>.
- OAIC——see Office of the Australian Information Commissioner.
- Office of the Australian Information Commissioner 2013, *Australian Privacy Principles and National Privacy Principles – Comparison Guide*, Office of the Australian Information Commissioner, Sydney, viewed 20 May 2019, <<https://www.OAIC.gov.au/agencies-and-organisations/guides/australian-privacy-principles-and-national-privacy-principles-comparison-guide>>.
- 2014, 'Chapter 12: Australian Privacy Principle 12 — Access to personal information', in *Australian Privacy Principles guidelines*, Sydney, viewed 20 May 2019,

<<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-12-app-12-access-to-personal-information>>.

Peyton, A 2018, 'Australian challenger banks: who's who (and what's their tech)', *FinTech Futures*, 7 August, viewed 20 May 2019, <<https://www.bankingtech.com/2018/08/australian-challenger-banks-whos-who-and-whats-their-tech/>>.

Productivity Commission 2017, *Data Availability and Use*, Report No. 82, Canberra.

randerson112358 2018, 'Analyzing FitBit Data', *Medium*, 3 September, viewed 20 May 2019, <<https://medium.com/@randerson112358/analyzing-my-fitbit-data-163d341a6cce>>.

Satariano, A 2018, 'G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog', *The New York Times*, 24 May, viewed 20 My 2019, <<https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html>>.

Schwartz, PM & Peifer, KN 2017, 'Transatlantic Data Privacy Law', *Georgetown Law Journal*, vol. 106, no. 1, pp. 115-180.

Solove, DJ 2013, 'Introduction: Privacy self-management and the consent dilemma', *Harvard Law Review*, vol. 126, no 7, pp. 1880-1903.

Treasury, The 2018, *Consumer Data Right*, The Australian Government the Treasury, Canberra, viewed 20 May 2019, <https://static.treasury.gov.au/uploads/sites/1/2018/05/t286983_consumer-data-right-booklet.pdf>.

Thomas, J, Barraket, J, Wilson, CK, Cook, K, Louie, Holcombe-James, I, Ewing, S, & MacDonald, T 2018, *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2018*, RMIT University, Melbourne, for Telstra.

Tsotsis, A 2010, 'Facebook Now Allows You To "Download Your Information"', *TechCrunch*, 6 October, viewed 20 May 2019, <<https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/>>.

Van Souwe, J, Gates, P, Bishop, B & Dunnin, C 2017, *Australian Community Attitudes to Privacy Survey 2017*, report to the Office of the Australian Information Commissioner, Sydney.

Vandor, M 2012, 'Your Twitter archive', *Official Twitter Blog*, 19 December, viewed 20 May 2019, <https://blog.twitter.com/official/en_us/a/2012/your-twitter-archive.html>.

Weiner, A 2018, 'What it's Like to Wallow in Your Own Facebook Data', *The Atlantic*, 15 September, viewed 20 May 2019, <<https://www.theatlantic.com/magazine/archive/2018/09/download-your-facebook-data/565736/>>

Wilding, D, Fray, P, Molitorisz S & Meese, J 2019, Submission to Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Preliminary Report*, 15 February, viewed 20 May 2019, <<https://www.ACCC.gov.au/system/files/Centre%20for%20Media%20Transition%20%28February%202019%29.PDF>>.

Withers, I 2018, 'Big six come under fire for slow take-up of Open Banking rules', *The Telegraph*, 19 August, viewed 20 May 2019, <<https://www.telegraph.co.uk/business/2018/08/19/big-six-come-fire-slow-take-up-open-banking-rules/>>.

Legislation and Cases Cited

Convention for the Protection of Human Rights and Fundamental Freedoms.

Competition and Consumer (Consumer Data) Rules Exposure Draft 2019 (Cth).

Explanatory Memorandum to the Treasury Laws Amendment (Consumer Data Right) Bill 2018.

General Data Protection Regulation 2016/679 (EU).

GDPR—see General Data Protection Regulation.

Mobile Number Portability Code (2009).

Privacy Commissioner v. Telstra Corporation Limited [2017] FCAFC 4.

Privacy Act 1988 (Cth).

Telecommunications Consumer Protections Code (2018).

Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth).



Consumer rights to personal data
Data access in the communications sector