(mis)Informed Consent in Australia (Report for iappANZ, 31 March 2021)

Author:
Manwaring, Kayleen; Kemp, Katharine; Nicholls, Rob

Publication details:
Commissioning Body: International Association of Privacy Professionals ANZ Chapter
SSRN Electronic Journal
pp. 1 - 139
978-0-7334-3978-0 (ISBN)
1556-5068 (ISSN)

Publication Date:
2021-06-08

Publisher DOI:
https://doi.org/10.26190/7sk3-0w49

DOI:
https://doi.org/10.26190/7sk3-0w49

UNSW SYDNEY

(mis)Informed Consent in Australia

A report funded by the International Association of Privacy Professionals – Australia/New Zealand Chapter Legacy Project

31 March 2021

http://doi.org/10.26190/7sk3-0w49

Authors

Chapters 1 and 2:
Dr Kayleen Manwaring, Senior Lecturer
School of Private and Commercial Law, UNSW Law & Justice

Chapters 3 and 5:
Dr Katharine Kemp, Senior Lecturer
School of Global and Public Law, UNSW Law & Justice

Chapters 4 and 6:
Dr Rob Nicholls, Associate Professor
School of Management and Governance, UNSW Business

Acknowledgements

This project was funded by the International Association of Privacy Professionals – Australia/New Zealand Chapter Inc (**iappANZ**) as part of its legacy grants scheme for research projects advancing professionals in the privacy and data industries. The views expressed in this document do not necessarily reflect the views of iappANZ.

In addition to the general membership of iappANZ, we would like to thank iappANZ members Katherine Sainty and Melanie Marks, who shepherded us through the grant process, and Professor of Practice Peter Leonard, who acted as proposer. We would also like to acknowledge the efforts of our research assistants, Dr Courtenay Atwell (Chapters 4 and 6), Roseanna Bricknell (Chapters 3 and 4, and general formatting of the entire document) and Jessica Liu (Chapters 1 and 2). However all opinions, errors and omissions for each chapter are those of the individual chapter author.

Suggested citation Manwaring, K, Kemp, K and Nicholls, R. *(mis)Informed Consent in Australia* (Report, March 2021)

http://doi.org/10.26190/7sk3-0w49

ISBN: 978-0-7334-3978-0

INTRODUCTION

> I'm not comfortable with them having any of my information, but if you want to be involved in whatever the site is about, you don't get options…
>
> I don't know how I can decipher where my data goes and how it's used. It concerns me, but it's not transparent to me
>
> I expect law to deal with that[1]

These consumer comments reflect some of the major issues facing consumers in Australia, New Zealand and worldwide. It is trite to say that digital platforms have become ubiquitous, with the likes of Google, Facebook, Microsoft and Apple attempting to influence many people's day-to-day activities, in both the personal and professional spheres. Such platforms offer several beneficial services, and many require no monetary payment on the condition that users consent to their data being collected, processed and used for the commercial purposes of third parties. However, this 'consent' usually involves a consumer accepting or agreeing to a set of take-it-or-leave it standard form terms, giving consumers essentially no choice but to submit to a wide range of data practices if they wish to access a product or service.

It is clear that consumers *expect* the law to protect them when it comes to how data is collected, shared and used. This report explores the notion of 'informed consent' in relation to commercial dealings with consumer data and its effectiveness to appropriately protect individuals under the law in Australia. It discusses aspects of informed consent in the context of the current legislative and regulatory framework regulating such dealings, and recommends changes to regulatory and legislative frameworks that deal with consumer data handling and standard form agreements.

This report sets out the research and critical analysis of three UNSW scholars, from the School of Global and Public Law, School of Management and Governance, and School of Private and Commercial Law in the Faculties of Business and Law & Justice. Each of these scholars provides their own unique insights relating to the interdependencies between the law, current business practices, consumer expectations, economic, social and behavioural considerations in the context of notions of informed consent and standard form agreements.

In exploring these issues, these scholars have explored the legislative frameworks created by the *Privacy Act 1988* (Cth) and the *Competition and Consumer Act 2010* (Cth), and also considered the impact of Australia's regulatory framework, including enforcement practices of the OAIC and the ACCC.

In **Chapter 1**, Dr Manwaring outlines the empirical evidence in Australia regarding consumer privacy expectations as to commercial dealings with their data, and introduces Australia's data protection legislative framework. In **Chapter 2** she proceeds to examine in detail issues with the legislative framework meeting consumer expectations in relation to informed consent, particularly in relation to the *Privacy Act* and the *Australian Consumer Law*. She also briefly examines the approach in other relevant jurisdictions for their utility in informing reform in the Australian context. However, Dr Manwaring concludes that none of those jurisdictions appears to have fully solved the problems posed by informed consent and standard form agreements.

---

[1] Responses from focus groups conducted by Roy Morgan Research in 2018, commissioned by the Consumer Policy Research Centre. Phuong Nguyen and Lauren Solomon, *Consumer data and the digital economy: emerging issues in data collection, use and sharing* (Report, Consumer Policy Research Centre, July 2018).

However, the legislative framework only poses part of the problem. In **Chapter 3**, Dr Kemp outlines issues with the *regulatory* framework supporting enforcement, including the operation of the enforcement and other powers of the main regulators of consumer data, the Office of the Australian Information Commissioner (OAIC) and the Australian Competition and Consumer Commission (ACCC). Dr Kemp concludes with proposals on necessary reforms.

In **Chapter 4**, Dr Nicholls examines economic, social and behavioural aspects of privacy and consumer protection policy approaches to standard form agreements and informed consent.

In **Chapter 5**, Dr Kemp provides a 'deep dive' into regulation of an area of growing concern, that of the data brokerage and adtech industries. These industries are characterised both by their growing influence and the obscurity of the data collection, processing and transfer practices employed in them, and the consequent near-invisibility of their practices to the consumers whose data drives their profits. Dr Kemp recommends a set of reforms to offset some of the harms posed by the practices of data brokers and adtech providers.

In **Chapter 6**, Dr Nicholls reviews the recent reform which introduced the Consumer Data Right, the proposals for reform contained in the Digital Platforms Inquiry, and the limitations of the current policy, regulatory and legislative regime. He examines the potential for general reform of these frameworks in relation to standard form agreements and the protection of consumers in relation to the collection and handling of their data by commercial entities and recommends both 'quick wins' and systemic long-term change.

The date of this report is 31 March 2021. However, on 16 April 2021, the Federal Court handed down a judgment which found that Google LLC and Google Australia Ltd had misled consumers about location data collected through mobile devices. Penalties are yet to be determined, but nevertheless this judgment is likely to prove an important development in how judges and businesses interpret privacy and consent requirements. Therefore, we have included a brief 'stop press' about this decision in **Appendix A** to this report (by Dr Kemp and Dr Manwaring).

The adequacy of the *Privacy Act* to protect data subjects has been vigorously and routinely contested. Commercial entities face few substantial barriers in dealing with consumer data (other than compliance costs, which are likely exacerbated by the nature of the legislation). In many cases consent of consumers is not required, and even where it is, the nominal consumer consent obtained is not informed, is non-negotiable, and is subject to unilateral interpretation and extension at the will of the commercial party.

While consumer protection law can potentially provide a more fertile area to protect consumers against the problems of a lack of true informed consent, there are significant gaps also in this framework.

With this report, we hope to draw greater attention to the problems with informed consent, the use of standard form agreements, the activities of data brokers and adtech providers, and to advocate for greater protection in respect of commercial dealings with consumer data.

Table of Contents

KAYLEEN MANWARING

1. Chapter 1 – Consumer expectations and Australia's data protection legislation

1.1 Introduction

The information age has seen a rapid growth in the number of online services and digital platforms with which consumers are interacting daily.[1] While many of these services are offered to consumers for no monetary cost, consumers are required to provide their data as a condition of using the services.[2] This data can be:

- actively provided *by* a consumer (for example, entering a name and email address upon account registration);
- passively collected *from* a consumer's activities (for example, background collection of metadata as a consumer uses the product or service or third-party apps or websites); and/or
- inferred from the combination of the above data and data from other sources (for example, by analysing combined datasets from various suppliers to make inferences about a consumer's income, family situation and habits).[3]

Personal data collection, use and disclosure in online environments ('digital data practices') is increasingly inescapable, leaving consumers concerned about the protection of their personal information (as shown in paragraph 1.2 below).

Consumers expect the law to protect them against the misuse of data,[4] and expect the government to regulate the way in which companies collect and use their data.[5] Currently, the two main areas of law in Australia which regulate the collection, sharing and use of consumer data are the *Privacy Act 1988* (Cth) ('*Privacy Act*') and the *Australian Consumer Law* (*ACL*), which forms Schedule 2 to the *Competition and Consumer Act 2010* (Cth) ('*CCA*').

This chapter is intended to set out the general framework under which digital data practices are currently regulated. First, it outlines the privacy experiences and expectations of consumers in Australia. In paragraph 1.3, it sets out relevant principles under the *Privacy Act*. Paragraph 1.4 discusses the link between consumer expectations and privacy complaints. Paragraph 1.5 concludes.

---

[1] Australian Competition and Consumer Commission ('ACCC'), *Digital Platforms Inquiry Final Report* (June 2019) https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf 1.
[2] Ibid 374.
[3] Ibid 378.
[4] Phuong Nguyen and Lauren Solomon, *Consumer data and the digital economy: emerging issues in data collection, use and sharing* (Report, Consumer Policy Research Centre, July 2018) 30 ('CPRC 2018 Survey').
[5] ACCC, *Digital Platforms Inquiry Final Report* (n 1) 36; Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020* (Report, OAIC, September 2020) 8 ('OAIC 2020 Survey').

1.2 'Privacy' expectations and consumer conduct

Several significant surveys on the privacy expectations of Australian consumers have been carried out since 2017. The most important of these include surveys carried out on behalf of the:

1. Consumer Policy Research Centre ('CPRC') in 2018 ('CPRC 2018 Survey')[6] and 2020 ('CPRC 2020 Survey');[7]
2. Australian Competition and Consumer Commission ('ACCC Survey');[8]
3. Office of the Australian Information Commissioner ('OAIC') in 2017 ('OAIC 2017 Survey')[9] and 2020 ('OAIC 2020 Survey');[10] and
4. accounting and consulting firm Deloitte ('Deloitte Survey').[11]

These surveys reveal consistent findings on consumer knowledge, behaviour and attitudes about data collection, use and sharing.[12]

Australian users of digital platforms use on average four different platforms daily. For example, the ACCC survey indicated that 95.9% of Australians used Google Search, 90.7% YouTube and 80.9% Facebook. The collection, use and sharing of information by these platforms are a growing concern amongst consumers.[13] The Deloitte Survey found that 98% of consumers believe privacy is at least somewhat important when deciding to use an app.[14] Additionally, the OAIC found 70% of Australians felt that privacy is a major concern in their lives,[15] and 83% believe there are greater privacy risks dealing with entities online compared to traditional settings.[16]

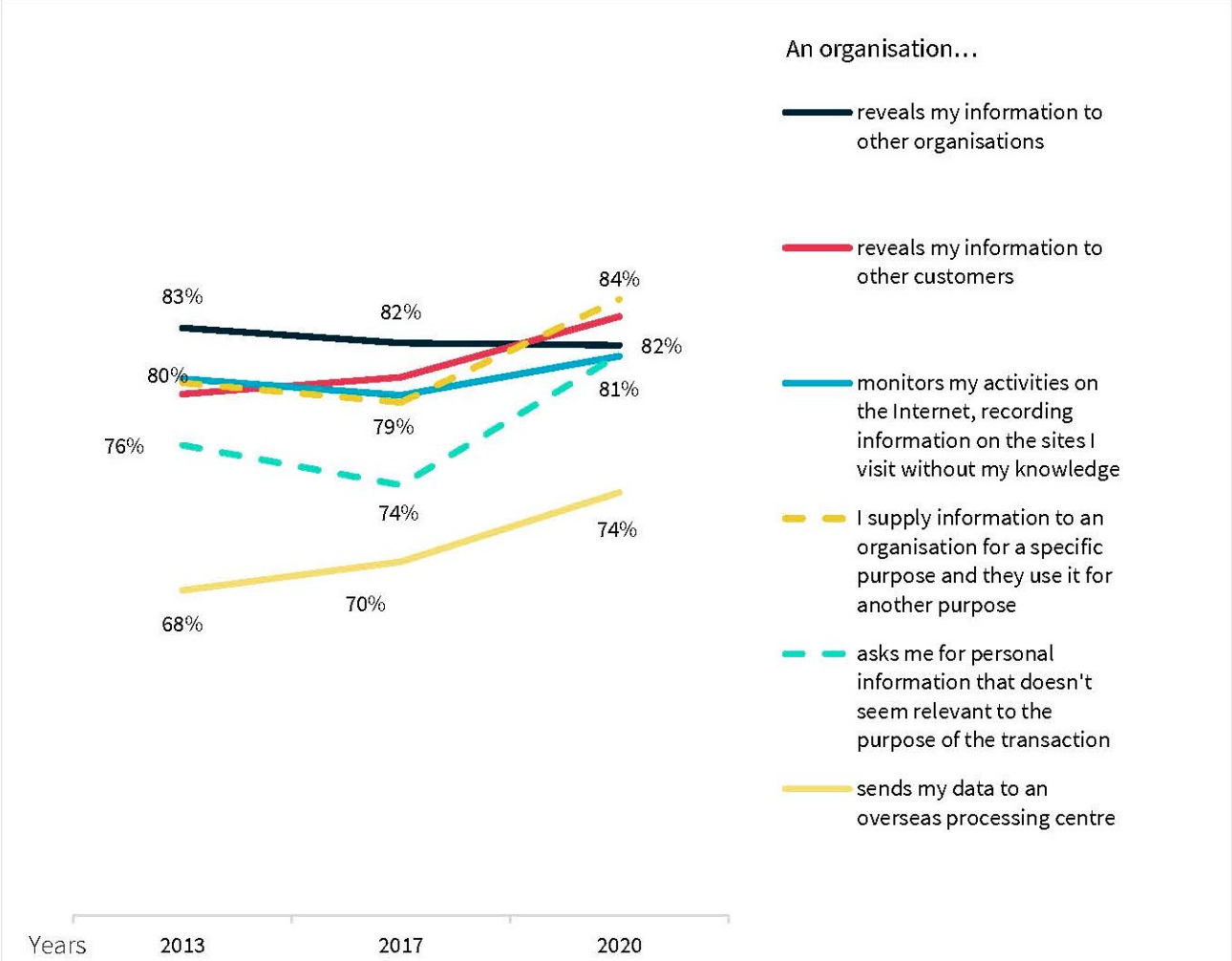
It is clear consumers want greater transparency and more control over how entities collect, use and share their data. The CPRC 2020 Survey revealed 92% of participants want companies to only collect data that is essential for the delivery of their service, and 94% want companies to be open about how they use their data to assess their eligibility or exclude them from services or products.[17] The ACCC Survey presented similar findings with a significant proportion of digital platform users agreeing or strongly agreeing that digital platforms should tell users to whom they are providing personal information (91%), allow users to opt out of collection of certain types of information (90%), be open about how they use data about users and assess eligibility for products and services (89%), and should only collect information necessary for the provision of their products or services (85%).[18]

---

[6] The results of this survey were reported in CPRC 2018 Survey (n 4).
[7] Consumer Policy Research Centre and Roy Morgan, *CPRC 2020 Data and Technology Consumer Survey* (Report, Consumer Policy Research Centre Dec 2020) ('CPRC 2020 Survey').
[8] Rebecca Varley and Nena Bagga, *Consumer Views and Behaviours on Digital Platforms* (Final Report, Roy Morgan, November 2018) ('ACCC Survey').
[9] Jayne van Souwe et al, *Australian Community Attitudes to Privacy Survey 2017* (Report, OAIC, May 2017) ('OAIC 2017 Survey').
[10] OAIC 2020 Survey (n 5).
[11] Rita Andraos et al, *Trust: Is there an app for that? Deloitte Australian Privacy Index 2019* (Report, Deloitte, 14 May 2019) (Deloitte Survey).
[12] See ACCC Survey (n 8); CPRC 2018 Survey (n 4); Deloitte Survey (n 11); OAIC 2017 Survey (n 9).
[13] ACCC Survey (n 8) 13.
[14] Deloitte Survey (n 11) 12.
[15] OAIC 2020 Survey (n 5) 17.
[16] OAIC 2017 Survey (n 9) 17.
[17] CPRC 2020 Survey (n 7) 22. These percentages have increased slightly since the same questions were asked in the CPRC 2018 Survey (n 4) 36.
[18] ACCC Survey (n 8) 17.

Consumers are particularly concerned about the misuse of personal information. The OAIC (over 2013-2020)[19] found that most Australians consider the following digital data practices to be a misuse of personal information:

Figure 20: Proportion of Australians who consider each data practice is a misuse 2013-2020



B9/B10/B11_2020. Thinking now about the way that your personal information is handled by private or public sector organisations, which of the following instances would you regard to be a misuse of your personal information? Base: Australians 18+ (n=950).
Q12_2017. Which of the following instances would you regard to be a misuse of your personal information? (n=632)

Note: "An organisation reveals my information to other organisations" label in the 2020 ACAPS was previously labelled "An organisation that you haven't dealt with gets hold of your personal information".

Despite these figures indicating high levels of consumer privacy concerns, numerous researchers have suggested there is a 'privacy paradox'. According to this view, a paradox is apparent when consumers repeatedly claim an increasing concern about how their data is handled, but do not actively read privacy policies and continue to 'consent' to data practices

[19] OAIC 2020 Survey (n 5) 38, Figure 20. This reflects similar findings around what is considered misuse of data in the ACCC Survey, although the terminology and questions differ.

that are not in their interests.[20] For example, the ACCC Survey found that only 18% of consumers read privacy policies for internet sites or applications most or every time,[21] the Deloitte Survey which found that only 12% of consumers 'always' or 'very often' read privacy policies,[22] and the CPRC 2020 Survey reported that only 6% of survey participants read the documents for **all** the products or services they signed up to in the past 12 months.[23]

The OAIC 2020 Survey reported that 31% of Australians read privacy policies *sometimes*, but not always due to length (41%) and lack of readability (26%) of those policies. Post-COVID, the numbers of people reporting that they attempted to read policies rose. However, 45% read less than half the policy, and 18% very little.[24]

However, there is little that is paradoxical about consumers expressing concern about their online privacy while failing to read inscrutable privacy policies that provide very limited or no privacy options.[25] Other than the length and complexity of policies, the focus groups conducted by the CPRC revealed several other reasons why consumers do not actively engage with policies and 'consent' to sharing their data with platform providers. These reasons include:

- an expectation that the law would protect consumers against the misuse of data;
- the belief that large and reputable companies will protect their information; or
- the feeling that individuals have no control over how their data is collected, used or shared.[26]

Even where consumers read a privacy policy or terms and conditions, two-thirds of consumers indicated they still signed up for the product or service even though they did not feel comfortable with the policies, with the most common reason being that it was the only way to access the product or service.[27]

These findings reveal the obstacles to consumers understanding the content and consequences of their decision when choosing whether to enter a transaction with a service provider. In its Digital Platforms Inquiry Final Report ('DPI Final Report'), the Australian Competition and Consumer Commission ('ACCC') listed several factors that may prevent a consumer from making informed decisions that align with their privacy and data collection preferences when engaging with digital platforms.[28] These factors include:

- the differences in bargaining power between the digital platform compared with the consumer;
- significant information asymmetries; and
- inherent difficulties for consumers in accurately determining the current and *future* costs of providing their data.[29]

Another possible reason why consumers do not read privacy policies is a lack of privacy awareness. Both the CPRC 2020 Survey and ACCC Survey revealed that a substantial

---

[20] See Patricia A Norberg, Daniel R Horne and David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours' (2007) 41(1) *Journal of Consumer Affairs* 100; Spyros Kokolakis, 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon' (2015) 64 *Computers & Security* 122.
[21] ACCC Survey (n 8) 6.
[22] Deloitte Survey (n 11) 13.
[23] CPRC 2020 Survey (n 7) 18. This percentage did not change from the CPRC 2018 Survey (n 4) 30.
[24] OAIC 2020 Survey (n 5) 117.
[25] See the discussion of the 'privacy paradox' and revealed preference theory in Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16(2-3) *European Competition Journal* 628.
[26] CPRC 2018 Survey (n 4) 30-31.
[27] Ibid 31.
[28] ACCC (n 1) 384.
[29] Ibid.

proportion of consumers mistakenly believe that if a company has a privacy policy, it means that they will not share information with third parties, and that the information which apps sought permission to access from a user is only necessary for the app to function.[30] Many Australians are also unaware of the scope of Australia's privacy legislation, with the mistaken belief that various organisations and types of data collection, use and disclosure are covered by the legislation when in fact there are many exceptions.[31] This indicates a general lack of privacy awareness amongst Australian consumers.

These consumer studies highlight that consumer privacy expectations are currently not met, and greater transparency is needed over how entities collect, use and share consumer information. They reveal not only that many consumers lack the knowledge and/or practical capacity to protect their own interests when choosing whether to engage a service provider, but that many justifiably feel they have no option but to 'consent' to the data practices of the provider even if they are uncomfortable with some or all of them.

1.3 Australia's data protection framework

In Australia, the collection, use and disclosure of personal information is primarily regulated under the *Privacy Act*. The stated objects of the *Privacy Act* are to promote the protection of the privacy of individuals, and to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities.[32]

1.3.1 Australian Privacy Principles

Under s 15 of the *Privacy Act*, an entity covered by the *Privacy Act* ('APP entity') must not do an act, or engage in a practice, that breaches an Australian Privacy Principle (APP). The APPs contain thirteen standards that APP entities must comply with when handling personal information of individuals.[33]

APP 1 – Open and transparent management of personal information

APP entities must manage personal information in an open and transparent way.[34] APP 1.3 requires an APP entity to have a clearly expressed and up-to-date privacy policy about the management of personal information by the entity. APP 1.4 contains a list of information that must be included in the privacy policy, such as the type of personal information that the entity collects and holds, purposes for collection, use and disclosure, and whether the entity is likely to disclose personal information to overseas recipients.

APP 2 – Anonymity and pseudonymity

APP entities must give individuals the choice of not identifying themselves, or of using a pseudonym (with some exceptions).[35]

APP 3 – Collection of solicited personal information

An APP entity must not collect personal information unless the information is reasonably necessary for one or more of the entity's functions or activities.[36] Higher standards apply to

---

[30] In the CPRC 2020 Survey (n 7) 20, 18% of participants had this view (1% less than in the CPRC 2018 Survey (n 4) 29). However, the ACCC Survey reported one in three people had this view (ACCC Survey (n 8) 6).
[31] OAIC 2017 Survey (n 9).
[32] *Privacy Act 1988 (Cth)* (*Privacy Act*) s 2A.
[33] Ibid sch 1.
[34] Ibid sch 1 cl 1.1.
[35] Ibid sch 1 cl 2.1. There has been little jurisprudence on this section under the *Privacy Act*. However, there is a case on a similar principle under the *Privacy and Personal Information Act 1998* (NSW), which applies to NSW public sector agencies, statutory bodies, universities and local councils. A NSW citizen was able to bring a successful case against Transport for NSW for requiring registration of those holding a Gold Seniors Opal travelcard: *Waters v Transport for NSW* [2018] NSWCATAD 40.
[36] Ibid sch 1 cl 3.1, 3.2.

the collection of 'sensitive information' where the collection of sensitive information can only occur with the *consent* of the individual and the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.[37]

APP 4 – Dealing with unsolicited personal information

Where an entity receives personal information that it did not solicit, the entity must, within a reasonable period after receiving the information, determine whether or not it could have collected the information under APP 3 if the entity had solicited the information.[38] If the entity determines that it could not have collected the personal information, and the information is not contained in a Commonwealth record, it must as soon as practicable, but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.[39]

APP 5 – Notification of the collection of personal information

At or before the time an APP entity collects personal information about an individual (or, if that is not practicable, as soon as practicable after), the entity must take reasonable steps to notify the individual of matters relevant to the collection.[40] APP 5.2 sets out a list of matters for which an entity must notify where reasonable, such as: the identity and contact details of the APP entity,[41] the purposes for which the APP entity collects the personal information,[42] and the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity.[43]

APP 6 – Use or disclosure of personal information

Where an entity holds information about an individual that was collected for a particular purpose (primary purpose), the entity must not use or disclose the information for another purpose (secondary purpose) unless the individual has consented to the secondary purpose.[44] This consent requirement does not apply where the individual would reasonably expect the entity to use or disclose the information for the secondary purpose, and the secondary purpose is directly related to the primary purpose if the information is sensitive information or related to the primary purpose if the information is not sensitive information.[45] The consent requirements also do not apply where use or disclosure is required for judicial proceedings or is reasonably necessary for law enforcement purposes.[46]

APP 7 – Direct marketing

An entity may only use or disclose personal information for direct marketing purposes if the individual consents or would reasonably expect the entity to use or disclose the information for direct marketing purposes.[47] The entity must provide a simple means for the individual to opt out of direct marketing communications from the organisation.[48]

---

[37] Ibid sch 1 cl 3.3; see 1.3.2.3 for discussion of 'sensitive information'.
[38] Ibid sch 1 cl 4.1.
[39] Ibid sch 1 cl 4.3.
[40] Ibid sch 1 cl 5.1.
[41] Ibid sch 1 cl 5.2(a).
[42] Ibid sch 1 cl 5.2(d).
[43] Ibid sch 1 cl 5.2(e).
[44] Ibid sch 1 cl 6.1.
[45] Ibid sch 1 cl 6.2(a).
[46] Ibid sch 1 cl 6.2(b), (e).
[47] Ibid sch 1 cl 7.1-7.6.
[48] Ibid.

APP 8 – Cross-border disclosure of personal information

Before an APP entity discloses personal information about an individual to a third-party outside of Australia or an external Territory, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[49]

APP 9 – Adoption, use or disclosure of government related identifiers

An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order.[50]

APP 10 – Quality of personal information

An APP entity must take reasonable steps to ensure that the personal information that the entity collects is accurate, up-to-date and complete.[51] It must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose of use or disclosure.[52]

APP 11 – Security of personal information

An APP entity holding personal information must take reasonable steps to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.[53] Where an entity no longer needs personal information it holds for any purpose for which the information may be used or disclosed under the Schedule, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified.[54]

APP 12 – Access to personal information

An APP entity that holds personal information about an individual must, on request by the individual, give the individual access to the information unless an exception applies.[55]

APP 13 – Correction of personal information

If an individual requests the entity to correct information it holds, and the entity is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, it must take reasonable steps to correct the information.[56]

1.3.2 Thresholds for application of the *Privacy Act*

1.3.2.1 APP entities

The *Privacy Act* only applies to 'APP entities', which are predominantly federal government agencies and private sector organisations with an annual turnover of more than $3 million.[57] However, consumer surveys show that many Australians erroneously believe many

[49] Ibid sch 1 cl 8.1.
[50] Ibid sch 1 cl 9.1-9.3.
[51] Ibid sch 1 cl 10.1.
[52] Ibid sch 1 cl 10.2.
[53] Ibid sch 1 cl 11.1.
[54] Ibid sch 1 cl 11.2.
[55] Ibid sch 1 cl 12.1.
[56] Ibid sch 1 cl 13.1.
[57] Section 6 of the *Privacy Act* defines an 'APP entity' as an agency or organisation. Section 6C defines an organisation as (a) an individual; (b) a body corporate; (c) a partnership; (d) any other unincorporated association; or (e) that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory. Section 6D defines a 'small business' as a business with an annual turnover of $3 million or less in the previous year.

organisations that are *not* APP entities are covered by the *Privacy Act*.[58] The *Privacy Act* exempts small businesses with an annual turnover of $3 million or less (but see below),[59] public schools and universities, media organisations acting in the course of journalism,[60] and registered political parties and political representatives.[61] These exceptions exclude many businesses from the operation of the *Privacy Act,* presenting a major gap in Australia's data protection framework. State and territory government agencies are excluded from the *Privacy Act*, but tend to be subject to separate Acts. For example, NSW public sector agencies, statutory bodies, universities and local councils are subject to 12 Information Protection Principles (IPPs) under the *Privacy and Personal Information Protection Act 1998* (NSW).

Whilst small business operators (with annual turnover less than $3 million) are generally exempt from the *Privacy Act*, the following entities are specifically made subject to the *Privacy Act*, whatever their turnover:

- they provide a health service to another individual and holds any health information except in an employee record;[62]
- they disclose personal information about another individual to anyone else for a benefit, service or advantage;[63]
- they provide a benefit, service or advantage to collect personal information about another individual from anyone else;[64]
- are contracted service providers for a Commonwealth contract;[65] or
- are credit reporting bodies.[66]

This means that entities that collect, aggregate and analyse datasets for benefit, service or advantage, or engage in other data trading transactions, are considered APP entities, and must adhere to the APPs contained in the *Privacy Act*. This would include data brokers such as Veda and Acxiom, but also those who sell information to third parties as a mere adjunct to their main business. However, the wording of the *Privacy Act* does not require direct financial benefit, but leaves open the possibility of non-monetary 'benefit, service or advantage', such as bartering of data or advantageous contractual conditions.

1.3.2.2 '*Personal* Information'

The APPs regulate the activities of APP entities in relation to the collection, use and disclosure of *personal information.* 'Personal information' is now defined in that Act as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable'.[67] This means that data that does not fall within this definition of 'personal information' is not covered by the *Privacy Act.* In particular, the *Privacy Act* does not apply to de-identified or

[58] See the OAIC 2017 Survey which found that 77% of Australians surveyed believed that 'public schools and universities' are covered by the *Privacy Act*, 69% believed 'media organisations' are covered, and 55% believed 'small Australian businesses' are covered when in fact, these fall within the exceptions contained in the *Privacy Act.* OAIC 2017 Survey (n 9).
[59] *Privacy Act* s 6D(1).
[60] Ibid s 7B(4).
[61] Ibid s 6C(1).
[62] Ibid s 6D(4)(b).
[63] Ibid s 6D(4)(c).
[64] Ibid s 6D(4)(d).
[65] Ibid s 6D(4)(e).
[66] Ibid s 6D(4)(f).
[67] Ibid s 6.

anonymous data, and it is unclear whether the scope of 'personal information' includes metadata such as IP addresses and location data.[68]

In *Privacy Commissioner v Telstra Corporation Ltd* both the Administrative Appeals Tribunal (AAT) and the Full Federal Court on appeal proposed a narrow construction of the meaning of personal information 'about an individual'. Whilst the Federal Court did not decide on the broader question of whether network related data is 'personal information', they stated that it was an evaluative process that should be determined on a case by case basis directed 'to the need for the individual to be a subject matter of the information'.[69] However, the Full Federal Court considered that the colour of the complainant's mobile phone and his network type was not information about the complainant, and therefore not personal information. Similarly, the AAT gave an example of car service records, and stated that these would not constitute information 'about' the car's owner, even if the records contained the owner's name and the car's registration number. The definition of 'personal information' in the *Privacy Act* has been amended since this case, but without clarifying the scope of information being 'about an individual'. Significant uncertainty remains as to its meaning.

In *Freelancer International Pty Ltd and Australian Information Commissioner,*[70] the Australian Administrative Tribunal (AAT) was tasked with determining whether the IP address of the complainant was considered 'personal information' for the purposes of the *Privacy Act.*[71] The AAT considered the nature of IP addresses, including the fact that they are assigned by a user's internet service provider to facilitate communication, and is likely to change over time.[72] As such, the AAT was of the view that an IP address does not merit characterisation as being 'about an individual' nor as being information from which an individual's identity can be reasonably ascertained.[73]

However, the current interpretation of the meaning of 'personal information' under the *Privacy Act* does not appear to adequately reflect the expectations of consumers. For example, the ACCC Survey found a significant majority of consumers consider 'personal information' to include information such as name, date of birth, telephone or device information, credit card details, photos, location information, emails, health information and browsing history.[74] However, it is likely that at least some of this information - such as location information, browsing history, device information – will not, without being linked to other information, be personal information under the *Privacy Act*.

In comparison, other jurisdictions provide clearer and broader definitions of the types of consumer information protected by their statutes. The General Data Protection Regulation (GDPR)[75] contains a set of data protection requirements that apply across the EU and are intended to harmonise data protection laws across the EU and enhance consumer trust in online services.[76] For the purposes of the GDPR, 'personal data' means any information *relating to* an identified or identifiable natural personal ('data subject'),[77] which is broader than the Australian requirement that the information be 'about' an individual. An identifiable

---

[68] ACCC (n 1) 435.
[69] *Privacy Commissioner v Telstra Corporation Ltd* (2017) [2017] FCAFC 4 [63].
[70] *Freelancer International Pty Ltd v Australian Information Commissioner* [2016] AATA 349.
[71] Ibid [39].
[72] Ibid.
[73] Ibid [63].
[74] ACCC Survey (n 8) 19.
[75] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1 ('GDPR').
[76] European Commission, 'Joint Statement on the final adoption of the new EU rules for personal data protection' (Press Statement, 14 April 2016).
[77] GDPR art 4(1) (n 75).

person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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.[78] The GDPR definition of 'personal data' explicitly mentions 'location data' and 'an online identifier', indicating greater clarity and a wider scope of protection for EU consumers compared with Australian consumers under the *Privacy Act*. (See section 2.10 below for a detailed discussion of other jurisdictions.)

An 'employee record', defined as 'a record of personal information relating to the employment of the employee' under s 6(1) of the *Privacy Act*, is specifically excluded from the application of APPs.

1.3.2.3 '*Sensitive* Information'

The standards set out in the APPs are higher for personal information that is considered 'sensitive information'. Section 6 of the *Privacy Act* defines 'sensitive information' as:

(a) information or an opinion about an individual's:
  i. racial or ethnic origin; or
  ii. political opinions; or
  iii. membership of a political association; or
  iv. religious beliefs or affiliations; or
  v. philosophical beliefs; or
  vi. membership of a professional or trade association; or
  vii. membership of a trade union; or
  viii. sexual orientation or practices; or
  ix. criminal record;

that is also personal information; or
(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information; or
(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) biometric templates.[79]

APP 3.3. states than an APP entity must not collect sensitive information about an individual unless the individual ***consents*** to the collection of the information and the information is reasonably necessary for one or more of the entity's functions or activities.[80]

The Fair Work Commission Full Bench's decision in *Lee v Superior Wood Pty Ltd* examined the application of APP 3 to sensitive information (in this case, biometric information used for identification) in the context of an employment dispute.[81] The complainant, Mr Lee, was informed by his employer, Superior Wood, that it was introducing fingerprint scanners to record employees' hours of work and employees were required to register their fingerprints and use the scanners as directed.[82] Mr Lee declined to use the scanners and informed Superior Wood of his concerns regarding the control of his biometric data.[83] Superior Wood issued several warnings to Mr Lee and terminated his employment for refusing to comply with the direction to use the scanners.[84]

Mr Lee submitted an unfair dismissal application to the Fair Work Commission which was unsuccessful at first instance. On appeal, the Full Bench quashed the initial decision,

---

[78] Ibid.
[79] *Privacy Act* s 6.
[80] Ibid sch 1 cl 3.3.
[81] *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946.
[82] Ibid [5].
[83] Ibid [7]-[8].
[84] Ibid [10],[12].

concluding that Mr Lee was unfairly dismissed.[85] The Full Bench decided that the employee records exemption did not apply to employee records that were not yet 'held' by an APP entity. It went on to discuss the application of APP 3 and found that the use of biometric scanners and the collection of the employee's fingerprints were not 'reasonably necessary' for the recording of start and finish times, and the introduction of the biometric scanners was mainly for administrative convenience.[86] On the issue of consent, the Full Bench found the direction issued to Mr Lee, despite his lack of consent, was 'directly inconsistent' with APP3 which requires consent for the collection of sensitive information.[87] Given these circumstances, the Full Bench found that the direction issued to Mr Lee to submit his biometric data when he did not consent to the collection of his sensitive information was not a lawful direction.

Although the decision in *Lee v Superior Wood Pty Ltd* dealt with an employment dispute, it is nonetheless relevant to the discussion of consumer consent in respect of the commercial dealing of consumer data. However, the double requirement of consent and reasonable necessity for collection of sensitive information does not apply to 'personal information' that is not 'sensitive information'. APP3 not does require consent for collection of personal information that is not sensitive information.

1.4 Privacy complaints

It is also worth commenting on the growing number of privacy complaints made to the OAIC since 2015. The annual reports released by the OAIC reveal that there were 2,128 privacy complaints made to the Commissioner in 2015-16,[88] 2,495 complaints in 2016-17,[89] 2,947 complaints in 2017-18,[90] and 3,306 complaints in 2018-19.[91] These statistics indicate a 55% growth in the number of privacy complaints since 2015, with no information on the breakdown of these complaints or the types of matters surrounding these complaints. (The 2019-2020 annual report indicated a 19% decline in complaints, but the OAIC attributed this anomalous outcome to the effects of the COVID-19 pandemic.) Little jurisprudential insight can therefore be drawn from these complaints, save to note that only a tiny proportion are ever taken to the determination stage. However, the growth in complaints supports the results of the consumer surveys that individuals are becoming more concerned about their privacy.

1.5 Conclusion

This chapter has outlined the significant empirical evidence demonstrating:

1. consumers have real concerns about privacy of their information;
2. these concerns cannot easily be addressed by individuals; and
3. consumers expect the law to have a role in protecting them against misuse of their information.

However, the analysis above indicates that there is a significant disconnection between actual digital data practices by businesses and the expectations of consumers.

It has also outlined the nature of Australia's current data protection framework.

---

[85] Ibid [102].
[86] Ibid [85].
[87] Ibid [48].
[88] OAIC, *Annual Report 2015-16* (Report, 27 September 2016) 14.
[89] OAIC, *Annual Report 2016-17* (Report, 14 September 2017) 18.
[90] OAIC, *Annual Report 2017-18* (Report, 17 September 2018) 12.
[91] OAIC, *Annual Report 2018-19* (Report, 12 September 2019) 11.

The next chapter examines the current Australian legislative framework regarding approaches to ‘consent’ for data protection. It also examines an alternative legislative framework, that of consumer protection law.

2. Chapter 2 – Law and practice in relation to informed consent

2.1 Introduction and the importance of 'informed consent'

This chapter will discuss the Australian approach to 'consent' for data protection and identify the gaps in existing primary and secondary material when dealing with the notion of 'informed consent'.

First, it sets out the relevant principles under the *Privacy Act 1988* (Cth) ('*Privacy Act*') relating to the requirement of consent. Second, it details the available OAIC guidance material and cases, and critically analyses their utility in informing notions of consent. In paragraph 2.7, some normative views of informed consent are outlined. Paragraph 2.8 provides details barriers to informed consent, particularly those common in industry practice. Paragraph 2.10 provides an outline of the relevant parts of the *ACL* that may apply to digital data practices. Paragraph 2.11 concludes.

The introduction of the *Privacy Act* and other privacy legislation in Australia was in response to Australia's international obligations under the International Covenant on Civil and Political Rights (ICCPR). The ICCPR recognises a basic human right to privacy based on the autonomy and dignity of the individual.[1] The ability to give 'informed consent' is regarded as an important part of maintaining dignity and autonomy. As was stated in the Australian Privacy Charter in 1994, 'consent is meaningless if people are not given full information, or have no option but to consent in order to obtain a benefit or service'.[2] The requirement of 'informed consent' is based on the idea that a consumer should have knowledge of the consequences of giving or not giving consent and have the freedom to choose whether or not to allow an entity to collect, use and disclose their data.[3]

2.2 The requirement for 'consent' under the *Privacy Act*

Under the *Privacy Act,* there is no strict requirement for an APP entity to obtain any form of consent before collecting personal information, save for 'sensitive information'.[4] An organisation can solicit and collect personal information (other than sensitive information) that is reasonably necessary for one or more of its functions or activities (APP 3.2).[5] When it does so, it must take steps to provide notice of the collection of personal information, as are reasonable in the circumstances (APP 5).[6]

However, consent is needed where an entity seeks to use or disclose personal information that was collected for a particular purpose for a *secondary* purpose (although this is subject to many exceptions).[7] Consent is also required for an entity to use personal information it holds about an individual for the purpose of direct marketing,[8] unless the individual would

---

[1] *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.
[2] Australian Privacy Charter Council, 'Australian Privacy Charter' (December 1994), https://privacy.org.au/about/privacycharter/.
[3] Jeremy Riddle, 'Informing Consent Online and Empowering Consumers through Better Communication of Privacy Information' (2017) 25 *Australian Journal of Competition and Consumer Law* 149, 151.
[4] See 1.3.2.3 for a discussion on 'sensitive information'.
[5] *Privacy Act* sch 1 cl 3.2.
[6] Ibid sch 1 cl 5.
[7] Ibid sch 1 cl 6.2.
[8] Ibid sch 1 cl 7.1.

reasonably expect their personal information to be used for the purpose of direct marketing.[9]

2.3 The meaning of 'consent' under the *Privacy Act*

Given the relevance of 'consent' to numerous APPs, its meaning is important in determining the obligations of entities with respect to the handling of consumer data.

The *Privacy Act* defines 'consent' to mean 'express consent or implied consent', but the text of the legislation does not make any mention of 'informed consent', nor does it expressly require any factors to be considered when obtaining an individual's consent.[10] This definition has remained unchanged since the introduction of the original Act in 1988. The Explanatory Memorandum to the original 1988 Act did not include any discussion of 'informed consent' nor any other explanation of what 'consent' is intended to mean, despite introducing the consent requirements contained in the current Act.[11]

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) ('*PAEPPA*') amended the *Privacy Act* in 2012, including the introduction of the APPs. None of the statutory amendments contained in PAEPPA amended the original definition of 'consent'. However, the Explanatory Memorandum to PAEPPA did discuss the concept, as follows (emphasis added):

Consent is a defined concept within the current *Privacy Act* which will be retained in the amended Act. Consent is defined to mean 'express consent or implied consent'. Express consent exists where a person makes an *informed decision* to give their *voluntary agreement* to collection, use or disclosure taking place.

Whether consent can be said to be implied depends entirely on the circumstances. Consent may be implied when, in the circumstances, the individual and the relevant entity have each engaged in conduct that means that it can be inferred the individual has consented, even though the individual may not have specifically stated that he or she gives consent.

Consent, in many circumstances, can be withdrawn at any time. In such circumstances, the consent no longer exists, and an entity would no longer be able to rely on consent having been given when dealing with the individual's personal information.

Consistent with the Government's response to ALRC Recommendation 19-1, the Government encourages the development and publication of appropriate guidance by the OAIC about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*.[12]

It is noticeable that the terms 'informed decision' and 'voluntary agreement' arose in the Explanatory Memorandum of a Bill that did not make any changes to the original consent definition, when the Explanatory Memorandum of the original Bill made no mention of these terms. It is highly unlikely that the PAEPPA Explanatory Memorandum could be used to assist in interpreting the meaning of consent. While section 15AB(2) of the *Commonwealth Acts Interpretation Act 1901* (Cth) allows for Explanatory Memoranda to be used as approved extrinsic material in ascertaining the meaning of a provision, this is understandably confined to Explanatory Memoranda 'that was laid before, or furnished to the members of, either

[9] Ibid sch 1 cl 7.2.
[10] Ibid s 6.
[11] Australian Government, Explanatory Memorandum, Privacy Bill 1988 (Cth).
[12] Australian Government, Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).

House of the Parliament by a Minister *before* the time when the provision was enacted' (emphasis added).[13]

PAEPPA was intended to implement a number of recommendations put forward by the Australian Law Reform Commission (ALRC) in a report published in 2008, following an inquiry into the *Privacy Act*.[14] Chapter 19 of the ALRC Report discussed consent, including the meaning and elements of consent.[15] Relevantly, the ALRC Report mentioned a number of options for reform to clarify the meaning of consent as it applies to the privacy principles.[16]

These included:

- amending the *Privacy Act* to set out in detail what is required to obtain the requisite consent in the many contexts in which it may be sought under the *Privacy Act*, and with greater precision, the factors that should be taken into account in obtaining an individual's consent;
- requiring the Office of the Privacy Commissioner (OPC) (replaced by OAIC in 2010) to provide more guidance on what constitutes consent for the purposes of the privacy principles in various contexts; or
- combining elements of the above approaches.[17]

During the inquiry, the ALRC consulted with numerous stakeholders, with most stakeholders supporting the option of OPC guidance over amending the statutory definition of 'consent'.[18] In particular, the OPC submitted that it would not support approaches to amend the current definition of consent or to set out consent requirements for a given sector in legislative provisions, stating that such legislative change would introduce greater complexity into privacy regulation.[19] A small number of stakeholders, however, submitted that further OPC guidance was not enough, and that the *Privacy Act* should be amended to include a more detailed definition of consent.[20]

In considering these views, the ALRC concluded that:

> The most appropriate way to clarify the meaning of consent, as it applies to the privacy principles, is for the OPC to provide further guidance in this regard. The guidance should address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained…[21]

Amending the *Privacy Act* to set out in detail what is required to obtain the requisite consent in the many contexts in which it may be sought is problematic. This approach would require a very large number of prescriptive rules that attempt to cover the wide variety of situations in which an agency or organisation may seek consent to deal with an individual's personal information. Such an approach would be inconsistent with the ALRC's view that a principles-based approach should continue to be at the heart of the *Privacy Act*. Moreover, such an approach would be doomed to fail because it would be very difficult, if not impossible, to cover every relevant context.[22]

---

[13] S 15AB(2)(e) *Commonwealth Acts Interpretation Act 1901* (Cth).
[14] Ibid.
[15] Australian Law Reform Commission ('ALRC'), *For Your Information: Australian Privacy Law and Practice* (Report, May 2008) vol 108.
[16] Ibid [19.29].
[17] Ibid [16.26]–[16.35].
[18] Ibid [19.31].
[19] Ibid [19.32].
[20] Ibid [19.39].
[21] Ibid [19.58].
[22] Ibid [19.61].

The common law has an important role to play in determining the elements of consent. A statutory definition is unable to capture nuances in the evolution of the common law and may have unintended consequences. The definition may be interpreted too restrictively, creating an undesirable restriction on the flow of information.[23]

As such, the ALRC Report recommended that the OPC should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*.[24] The ALRC's recommendation was specifically referenced in the Explanatory Memorandum to the Amendment Bill 2012, with the Government encouraging the 'development and publication of appropriate guidance by the OAIC about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*'.[25]

A review of the *Privacy Act,* the 1988 and 2012 explanatory memoranda, and the ALRC Report suggests that the vague definition of 'consent' contained in the *Privacy Act* is intended to encapsulate many contexts involving the collection, disclosure and use of personal information, and that the OAIC Guidelines (discussed below) should be the point of reference used for clarifying the meaning of consent as it applies in a given context.[26] However, as the following sections will explore, the non-binding OAIC Guidelines appear to have little effect in influencing the data practices of many firms,[27] and the current approach to regulating 'consent' has not provided adequate protections for consumers in light of extensive empirical evidence regarding consumer privacy preferences and attitudes regarding data practices.

2.4 The OAIC Guidelines

The OAIC introduced the Australian Privacy Principles Guidelines ('OAIC Guidelines') in 2014, replacing older guidelines on the National Privacy Principles.[28] The OAIC Guidelines outline the regulator's interpretation of the *Privacy Act* and matters taken into account when exercising its powers and functions.[29] It is important to emphasise that the OAIC Guidelines are non-binding on APP entities, but may useful in providing insight into the regulator's interpretation of 'consent' under the *Privacy Act*.

The OAIC Guidelines provide a framework for interpreting 'express or implied consent' under the *Privacy Act*. Express consent is given explicitly, either orally or in writing,[30] whereas implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.[31] The OAIC Guidelines discuss some common business practices that entities engage in when seeking consent from consumers for digital data practices.

---

[23] Ibid [19.62].
[24] Ibid 686.
[25] Australian Government, Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).
[26] *Privacy Act* (Cth); Australian Government, Explanatory Memorandum, Privacy Bill 1988 (Cth); Australian Government, Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth); ALRC (n 15).
[27] See additionally chapter 5 of this report.
[28] OAIC, 'Read the Australian Privacy Principles', https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/.
[29] OAIC, 'Australian Privacy Principles Guidelines: *Privacy Act* 1988' ((July 2019) https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf ('OAIC Guidelines').
[30] Ibid [B.36].
[31] Ibid [B.37].

For example, it is a common practice for an entity to provide a notice of its data handling practices to a consumer before enabling access to their services.[32] This practice is insufficient for obtaining consent according to the OAIC Guidelines that state:

> [g]enerally, it should not be assumed that an individual has given consent on the basis alone [sic] that they did not object to a proposal to handle personal information in a particular way. An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. It will be difficult for an entity to establish that an individual's silence can be taken as consent. Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individuals intention.[33]

The OAIC Guidelines also mention the use of opt-out mechanisms by businesses, stating that the 'use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous'.[34]. The discussion of common business practices strongly indicates the regulator's recognition that many such practices inhibit a consumer's ability to give informed consent.

The OAIC Guidelines also provides four key elements of consent, including that:

- the individual is adequately *informed* before giving consent;
- the individual gives consent *voluntarily*;
- the consent is *current* and *specific*; and
- the individual has the capacity to *understand* and communicate their consent.[35]

2.5 Informed

The OAIC states that entities 'should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent'.[36] This includes information about the implications of providing or withholding consent, with information 'written in plain English, without legal or industry jargon'.[37]

2.5.1 Voluntariness

This element requires that an individual be given a genuine opportunity to provide or withhold consent.[38] The practice of 'bundled consents' was identified by the ALRC, consumer bodies (such as ACCAN) and the ACCC as having the potential to undermine the voluntary nature of consent. 'Bundled consent' is common amongst service providers, and occurs when an entity combines numerous requests for a consumer's consent to a wide range of data handling practices, without giving the consumer the opportunity to choose which practices they agree to and which they do not.[39]

---

[32] See, for example, Facebook's sign-up page https://www.facebook.com/ which states 'By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy, You may receive SMS notifications from us and can opt out at any time.' See also, Apple's sign-up page https://appleid.apple.com/account#!&page=create which states 'Your Apple ID information is used to allow you to sign in securely and access your data. Apple records certain usage data for security, support, and reporting purposes. See how your data is managed'.
[33] OAIC (n 29) [B.39].
[34] Ibid [B.40]
[35] Ibid.
[36] Ibid [B.47].
[37] Ibid.
[38] Ibid [B.43].
[39] Ibid [B.45]-[B.46]. See also **chapter 5**.

2.5.2 Current and specific

The OAIC believes that consent should be current and specific where consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely.[40] Further, the OAIC states that an 'APP entity should not seek a broader consent than is necessary for its purpose, for example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures''.[41]

2.5.3 Capacity

An individual must have the capacity to consent, meaning that they are capable of understanding the nature of a consent decision, including the effect of giving or withholding consent. A key concern with respect to consent is the age of the individual as the *Privacy Act* does not specify an age after which individuals can make their own privacy decisions.[42] This is concerning given that children and young people can easily create an account on platforms such as Facebook and YouTube at the click of a button, with the providers having no legal obligation to ensure that the user has the capacity to consent.

2.6 Existing Australian authorities on consent

Under section 52 of the *Privacy Act*, the Commissioner can make 'determinations' on privacy complaints where conciliation has not resolved the matter, or where the complaint is not able to be finalised on some other basis.[43] The Commissioner may also make a determination following an investigation on the Commissioner's own initiative under section 40(1A).[44]

However, interpretation of the *Privacy Act* suffers significantly from a lack of jurisprudence. Over the last 10 years (1 Nov 2010 – 30 Nov 2020), there have been a total of 42 published privacy determinations, with seven of these determinations reviewed by the Australian Administrative Tribunal and two by the Federal Court of Australia.[45] In 26 of these 42 determinations, the Commissioner referred to the OAIC Guidelines, or their predecessors, the National Privacy Principles (NPP) Guidelines, when interpreting the meaning of certain terms contained in the *Privacy Act.*[46] None of the decisions by the AAT and Federal Court discuss the meaning of consent in any substantial way, and only two of the determinations by the Commissioner contain significant discussions of the issue of consent. These two cases are discussed below.

Financial Rights Legal Centre Inc & Others v Veda Advantage Information Services and Solutions Ltd [2016] AICmr 88 (*FRLC v Veda*)[47]

In *FRLC v Veda* three representative complaints (or 'class actions') were made jointly by consumer advocacy groups on behalf of a class of individuals. These actions were filed against Veda Advantage Information Services and Solutions Ltd (Veda) who operated a credit reporting business.[48] The case dealt with a number of issues related to credit reporting provisions under the *Privacy Act* irrelevant to this discussion. The relevant matter

---

[40] Ibid [B.49].
[41] Ibid [B.50].
[42] Ibid [B.56].
[43] 'Chapter 4: Determinations', *OAIC* (Web Page, Updated 28 August 2019) [4.4] https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-4-determinations/.
[44] Ibid [4.7].
[45] OAIC 'Privacy Determinations' (Web Page) https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations/.
[46] Ibid.
[47] *Financial Rights Legal Centre Inc. & Others and Veda Advantage Information Services and Solutions Ltd* [2016] AICmr 88 ('*FRLC v Veda*').
[48] Ibid.

for this discussion surrounded an online application form contained on Veda's website that allowed class members to obtain a free credit report.[49] The application included two tick boxes.

> Tick box 1 stated: 'Veda can contact me on the details supplied above regarding my application for a copy of my credit report'.[50]
>
> Tick box 2 stated: 'I would like to be contacted by telephone/email with finance, insurance and other offers relating to finance. I consent to Veda providing my personal information including my contact details to relevant corporate partners for this purpose'.[51]

The complainants contended that the wording of the statements associated with the tick boxes was misleading and in breach of APP 7, which prohibits an organisation from using or disclosing personal information for the purposes of direct marketing unless an exception applies.[52] The relevant exceptions to the case are contained in APP 7.2 and 7.3 which respectively provide that an organisation may use or disclose information about an individual for the purpose of direct marketing if the organisation collected the information from the individual and the individual would reasonably expect the organisation to use or disclose the information for that purpose,[53] or where the individual consents to such purposes.[54]

In relation to tick box 1, Veda claimed that express consent for Veda to contact the access seeker for direct marketing purposes had been given by virtue of several clauses contained in the user agreement which the access seeker must have read and agreed to in order to request a free report.[55] On the other hand, the complainants contended that the consent given in this situation was not effective because the access seeker was not adequately informed before giving consent, and the consent was involuntary.[56] They further claimed that the statement at tick box 1 was misleading and the user agreement terms and conditions were lengthy and not readily accessible.[57]

In determining the issue of consent, the Commissioner referred to the OAIC Guidelines which provide four elements of consent (informed consent, voluntariness, current and specific consent, and the capacity to consent), and the definitions of 'informed consent' and 'voluntary'.[58] The Commissioner rejected the complainants' contention that the consent was not voluntary, finding that:

> there is nothing to suggest that not ticking the box has serious or adverse consequences for the access seeker attempting to obtain their credit report free of charge… Given this, I cannot accept that consent is involuntarily given.[59]

---

[49] Ibid [153].
[50] Ibid.
[51] Ibid.
[52] Ibid [154]. See section 1.3.1 for a discussion of APP 7.
[53] Ibid [157].
[54] Ibid [158].
[55] Ibid [168].
[56] Ibid [170].
[57] Ibid [170].
[58] The Commissioner referred to B.29, B.30, B.37 and B.38 of the OAIC Guidelines (n 29). See earlier discussion of the OAIC Guidelines at 2.4.
[59] *FRLC v Veda* (n 47) [174]-[175].

On the issue of whether there was informed consent, the Commissioner stated that:

> [t]hough I agree the user agreement is lengthy, I accept that an ordinary and reasonable member of the class could have been expected to read the terms and conditions in the user agreement, and be aware that…if they provided 'express consent' when they ordered their [free credit] report, Veda and its related companies could use their personal information to send them information about Veda and its related companies' products and services'.[60]

In the Commissioner's opinion, that express consent was given when selecting tick box 2 (but not tick box 1, as discussed below).

An important point made by the Commissioner is that the *Privacy Act* aims to protect the privacy of individuals, and promotes the principle of freedom from interference with privacy as contained in article 17 of the *International Covenant on Civil and Political Rights,* to which Australia is a party.[61] As such, the Commissioner formed the view that 'any express consent obtained must…be sufficiently precise with regard to the kind of information to which the consent relates'.[62] The Commissioner concluded that the purpose for use and disclosure contained in the statement at tick box 1 was limited to the purpose of contacting an individual in relation to their 'application'.[63] Despite reading the terms and conditions of the user agreement, an ordinary and reasonable person would not have reasonably expected that by selecting tick box 1, they were providing express consent for direct marketing purposes.[64] As such, the Commissioner concluded that access seekers were not adequately informed about the consent they were providing when selecting tick box 1, and that those who ticked the box were not giving consent to the use or disclosure of their information for the purpose of direct marketing, nor was it reasonable for the individual to expect that their information would be used or disclosed for that purpose.[65] Accordingly, Veda was held to be in breach of APP 7.

In relation to tick box 2, the Commissioner found that Veda had sufficiently described the purpose of the use or disclosure of personal information for the purpose of securing informed consent.[66] The Commissioner highlighted that there is no specific requirement under the *Privacy Act* to specify the third parties to whom the information is proposed to be disclosed. However, the question was raised as to whether Veda's related entities could rely on consent obtained by Veda without being identified.[67] This was a separate issue that did not need to be determined for the purposes of the case, but nevertheless highlights a gap that remains unaddressed by both the Australian statutory framework and body of privacy cases.

Flight Centre Travel Group (Privacy) [2020] AICmr 57 (*Flight Centre Determination*)

Some more guidance was received on the nature of consent in November 2020. The Commissioner determined that Flight Centre Travel Group Ltd (Flight Centre) interfered with the privacy of almost 7000 individuals.[68] Flight Centre had organised a 'design jam' for travel agents, to promote the development of sales support technology. A supposedly *deidentified* customer dataset was provided to the travel agents, but due to a mistake in the deidentification process, some customers' credit card details, passport numbers, and dates of birth were left in the dataset that was accessed by the travel agents.

---

[60] Ibid [176].
[61] Ibid [178].
[62] Ibid.
[63] Ibid [179].
[64] Ibid [180].
[65] Ibid [181].
[66] Ibid [191].
[67] Ibid [191].
[68] *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 (25 November 2020) ('*Flight Centre Determination*')

Use or disclosure of personal information by an APP entity for a *secondary purpose* (ie the disclosure to the travel agents and its use for the design jam) is prohibited under the APPs unless *consent* is obtained.[69] Flight Centre attempted to argue that the required consent was obtained via its Privacy Policy 'as all customers consented to this in the course of transacting with the respondent'.[70]

The relevant parts of the Privacy Policy stated:

> [para 2] By providing personal information to us … you agree that this Policy will apply to how we handle your personal information and you consent to us collecting, using and disclosing your personal information as detailed in this Policy. If you do not agree with any part of this Policy, you must not provide your personal information to us and this may affect the services we can provide to you…
>
> [para 12] By providing us, or otherwise allowing us to collect, your personal information, you consent to us using and disclosing your personal information for the purposes for which it was collected, and for related or ancillary purposes, such as any one or more of the following purposes:
>
> ...
>
> - developing, improving and marketing our products and services and those of our related entities.

However, the Commissioner held that this was **not** consent as required by the APPs. In arriving at this conclusion, the Commissioner engaged in a detailed discussion of consent.

The Commissioner acknowledged that under section 6(1) of the *Privacy Act*, consent is express or implied. However, the Commissioner referred to the OAIC Guidelines to flesh out her interpretation of the meaning of consent:

> … Express consent is given explicitly, either orally or in writing... Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity… Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individuals intention…
>
> The four key elements of consent are:
>
> - the individual is adequately informed before giving consent
> - the individual gives consent voluntarily
> - the consent is current and specific
> - the individual has the capacity to understand and communicate their consent…[71]

No evidence was presented arguing for express consent. In relation to implied consent, the Commissioner stated:

> An APP entity cannot infer consent simply because it provided an individual with a policy or notice of a proposed collection, use or disclosure of personal information… I am therefore not satisfied that consent can be implied merely by making the respondents Privacy Policy available to customers and relying on the statement in paragraph 2 of that Policy.
>
> In any event, even if individuals had indicated their agreement to the uses and disclosures set out in the Policy (whether explicitly or, after reading the policy, through their continued engagement with the respondent), consent could not be obtained through the Privacy Policy as it was not sufficiently specific, and bundled together different uses and disclosures of personal information.
>
> A privacy policy is a transparency mechanism .... It is not generally a way of providing notice and obtaining consent … If the respondent had intended to disclose credit card details and passport

---

[69] *Privacy Act* APP6.1(a)
[70] *Flight Centre Determination* (n 68) [44].
[71] *Flight Centre Determination* (n 68) [47-48].

> information to third parties for this purpose… I would expect a request for consent to clearly identify the kind of information to be disclosed, the recipient entities, the purpose of the disclosure, and for consent to be sought separately, not as part of a Privacy Policy
>
> The respondents Privacy Policy also bundled together information about a wide range of possible collections, uses and disclosures of personal information, without giving customers the opportunity to choose which collections, uses and disclosures they agreed to and which they did not. Any purported consent was not voluntary, as the Privacy Policy did not provide individuals with a genuine opportunity to choose which collections, uses and disclosures they agreed to, and which they did not.[72]

2.7 Implications for 'Informed Consent'

There are several points to be made regarding the decisions in *FRLC v Veda* and the *Flight Centre Determination* relating to concepts of 'informed consent'.

2.7.1 Voluntariness

Firstly, whilst the Commissioner did not find any problems with voluntariness in *FRLC v Veda*, there could be a problem with voluntariness in a situation where an individual suffers consequences if they fail to provide their 'consent' to the provider's data practices. For example, many consumers feel pressured to 'consent' to the policies of service providers because they are otherwise unable to access the services.[73]

The OAIC's determination demonstrated the importance of the explicit choice of words contained in a request for consent, and the clauses contained in the terms and conditions or privacy policy, in determining whether 'informed consent' is provided. In this case, the request was restricted to the individual's 'application' for a credit report. However, the Commission stated that, 'If Veda wished to ensure that access seekers consented to being contacted by Veda for direct marketing purposes, then it should have expressed this plainly'.[74] It is unclear from this decision whether a broad or vague consent request for data collection, use and disclosure, coupled with an agreement or data policy that details use and disclosure for direct marketing purposes, would satisfy the requirements under APP 7. It should be noted that the general collection and use of personal information (except sensitive information) does not require express consent, only a notice of collection where reasonable.[75] It is therefore unclear whether the OAIC or a court would apply a similar interpretation of consent in a situation involving the use and disclosure for purposes other than direct marketing.

2.7.2 Intelligibility

Another problem with the OAIC's discussion of consent in *FLRC v Veda* is that there was no assessment as to whether the relevant class of consumer could reasonably understand the content contained within the user agreement. Rather, the OAIC was quick to state that an ordinary and reasonable person is expected to read the agreement and notices of the provider, and by checking the box, they provide express consent to those clauses (assuming that the words of the consent request are adequate, which was not the case in *FLRC v Veda*).[76] This is problematic because it suggests that as long as a provider gives the consumer all the information to read, it can be assumed that they have understood and consented to it by accepting the consent request. In practice, consumers are burdened with

---

[72] *Flight Centre Determination* (n 68) [53-56].
[73] See section 1.2 of this chapter for discussion of consumer expectations.
[74] *FRLC v Veda* (n 47) [181].
[75] See discussion in section 2.3 of this chapter.
[76] *FRLC v Veda* (n 47) [176].

lengthy and complex agreements and data policies that are difficult to understand, which prevent consumers from making informed decisions.[77]

2.7.3 The OAIC Guidelines and the meaning of consent

The Commissioner in both determinations discussed above applied the expanded meaning of consent set out in the OAIC Guidelines, that is, that the consent is informed, voluntary, current and specific, and given by an individual with the capacity to understand and communicate their understanding. However, as pointed out in section 2.3, there is no legislative basis for the applicability of the OAIC Guidelines. There has been no review – by either the AAT or the Federal Court – as to whether the OAIC Guidelines equate with the actual legislative drafting on the topic, which is considerably less detailed than the OAIC Guidelines, particularly in the discussion on consent.

Apart from these two OAIC determinations, there are no other relevant cases dealing with the issue of informed consent. The lack of primary material in Australia makes it difficult to provide a rich discussion on how the *Privacy Act* is applied and how 'consent' is viewed within the Australian privacy landscape.

The results of consumer surveys outlined in **chapter 1** indicate that the lack of case law is not due to lack of interest by consumers in their privacy. It is more likely to arise from a combination of factors: the barriers to enforcement by the regulator and individuals, the difficulty of gaining realistic compensation and the non-binding nature of the OAIC guidelines.

For example, no direct right of action is available to consumers: their only recourse is to make a 'complaint' to the OAIC under section 36 of the *Privacy Act*. Regulator decisions relating to complaints are only subject to appeal where the OAIC decides to make a 'determination' under s 52 of the *Privacy Act*. The small number of determinations made under this provision has resulted in a paucity of appellate jurisprudential development. Additionally, the sanctions that have been applied have been insubstantial (for example, enforceable undertakings). Where compensation has been awarded,[78] the amounts have been too small to have any meaningful deterrent effect. No civil penalties (which are potentially up to AUD 2.1 million) have been awarded since their introduction in 2014, standing in stark contrast to some other jurisdictions such as the UK.[79]

Additionally, insufficient funding and resourcing of the OAIC restricting its enforcement capacity (discussed in more detail in paragraph 3.2.6 in **Chapter 3**) has been publicly criticised.[80] And despite government representations around the importance of privacy

---

[77] See section 2.9.2 of this chapter which discusses the problems associated with privacy policies.
[78] Office of the Australian Information Commissioner, 'Determinations' www.oaic.gov.au/privacy-law/determinations/. The compensation awarded can be found in the 'Remedies' part of the summary of the determination decision. The compensation decision in the representative action of *'WP' and Secretary to the Department of Home Affairs (Privacy)* [2021] AICmr 2 (11 January 2021) is likely to be the largest compensation order to date in Australia, as a schedule of awards has been set for 1297 complainants.
[79] Information Commissioner's Office, 'Actions We've Taken' https://ico.org.uk/action-weve-taken/enforcement/. The first substantive pursuit of civil penalties by the OAIC was taken in 2020 against Facebook for serious interference with privacy. See Katharine Kemp and Kayleen Manwaring 'Australia's privacy watchdog is taking Facebook to court. It's a good start' (*The Conversation*, 11 March 2020), https://theconversation.com/australias-privacy-watchdog-is-taking-facebook-to-court-its-a-good-start-133345.
[80] For example, Allie Coyne, 'Starved of Funding, Resources, OAIC is Left to Shrivel' (*IT News*, 17 July 2015) www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273; Denham Sadler, 'Privacy Office at Breaking Point' (*InnovationAus,* 26 March 2018) www.innovationaus.com/2018/03/Privacy-office-at-breaking-point; Ben Grubb, 'Australia's Privacy Watchdog is 'Woefully' and 'Criminally' Underfunded' (*Crikey*, 16 July 2018) www.crikey.com.au/2018/07/16/australias-privacy-watchdog-is-woefully-and-criminally-underfunded/?ft=SGxCKzkvcXRVNWk0eU1tcjdPcGlNQT09.

following the ACCC DPI Final Report, the OAIC's funding was decreased in the 2020 Federal budget, and significant contingency funding remains without guarantee.[81]

2.8 Normative views of informed consent

There is a consensus amongst privacy scholars that Australian law provides weak privacy protections, with calls for increased consumer protections, particularly given the growth of digital platforms,[82] digital wallets,[83] big data,[84] and the Internet of Things and related technologies.[85]

One key gap in the existing Australian literature on privacy is the paucity of discussion on the notion of 'informed consent' and the problems associated with the current 'consent' requirements under the Australian *Privacy Act.* Rather, scholars have used numerous terms in discussing consent. Examples of such terms include, 'formal consent',[86] 'true consent',[87] 'genuine consent',[88] 'quality of consent',[89] 'adequate consent',[90] 'meaningful consent',[91] and 'proper consent'.[92] The diversity of terms indicates a lack of clarity in what 'consent' really means under Australian data protection law. In many instances, these terms are used without any analysis of what such consent means, but instead there is a tendency for privacy scholars to focus on themes such as the need for more 'transparency' over data handling practices or greater 'privacy safeguards' to protect consumers.[93] The underlying notion of 'informed consent' has often been overlooked in the academic discussion of Australian privacy and data protection laws.

However, some insights can be drawn from the few papers that do explore 'informed consent'.[94] Mathews-Hunt's research into privacy and consumer protection in the context of consumer internet of things (CIOT) considers the type of consumer data that may be generated by the CIOT, who owns it, and whether consumers provide informed consent as to its collection and use.[95] Whilst primarily focused on consumer law implications of CIOT, Mathews-Hunt points out numerous consent issues found in online contracts, including

---

[81] Denham Sadler, 'Privacy office faces 'remarkable' drop in funding' (*InnovationAus*, 26 October 2020) https://www.innovationaus.com/privacy-office-faces-remarkable-drop-in-funding/.
[82] Samson Esayas and Dan Svantesson, 'Digital platforms under fire: What Australia can learn from recent developments in Europe' (2018) 43(4) *Alternative Law Journal* 275; Kemp (n 25).
[83] Kanchana Kariyawasam and Matthew Tsai, 'Digital Wallets and Consumer Protection' (2017) 25 *Australian Journal of Competition and Consumer Law* 183.
[84] Suzana Livaja, 'Unlocking the Potential of Data in Australia's Financial System' (2018) 29 *Journal of Banking and Finance Law and Practice* 332; Jarrod Bayliss-McCulloch, 'Risks and opportunities in big data – how well adapted are Australia's privacy laws?' (2015) 20 *Media and Arts Law Review* 57.
[85] Kayleen Manwaring, 'Will emerging information technologies outpace consumer protection law? The case of digital consumer manipulation' (2018) 26(2) *Competition and Consumer Law Journal* 141, 175-177.
[86] Mark Briedis, Jane Webb and Michael Fraser, *Improving the Communication of Privacy Information for Consumers* (Report, UTS/Australian Communications Consumer Action Network, February 2016) 51.
[87] Ibid 52.
[88] Ibid.
[89] Ibid 56-60.
[90] Esayas and Svantesson (n 82) 281.
[91] Riddle (n 3) 149.
[92] Bayliss-McCulloch (n 84) 61.
[93] See, for example, Eli Fisher, 'Toward a proprietary interest in personal information' (2018) 22 *Media and Arts Law Review* 274, who suggests that the failure of Australia's privacy law to protect personal information can be attributed to a lack of transparency, the impracticability of monitoring for compliance, and the inability to enforce breaches of privacy.
[94] See Briedis, Webb and Fraser (n 86); Kate Mathews-Hunt, *consumeR-IOT: where every thing collides. Promoting consumer internet of things protection in Australia* (SJD minor thesis, Bond University, 2017) http://epublications.bond.edu.au/theses/179/; Dana McKay et al, *State of the Art in Data Tracking Technology* (Report, University of Melbourne, November 2019) 10-11.
[95] Mathews-Hunt (n 94) xii.

capacity, voluntariness and informed consent.[96] She highlights that whilst the OAIC Guidelines provide some guidance on what 'consent' means in the privacy context, in practice, privacy consents are merely based on disclosure, and courts are unlikely to interfere provided that entities give notice and consumers assent or are taken to do so implicitly.[97] She considers that any other view of consent 'opens millions of online contracts to review, which would be impracticable'.[98]

A similar view is formed by Lowden and Booth who believe that 'informed consent' is hard to achieve in the context of big data because of the inherent difficulty for an entity to predict and disclose all the possible ways they may in future seek to use data collected about an individual at the time of collection.[99] In contrast, Briedis et al contend that 'adequately informed consent does not require the consumer to understand the full complexity of information handling processes, but rather to have an awareness of how those processes are likely to have an impact on the consumer's interests'.[100] The variance in views across Australian scholars suggests that there is uncertainty about what 'informed consent' means in the context of privacy, and whether it can be achieved in practice.

In its DPI Final Report,[101] the ACCC explored the impact of digital platforms' data practices on consumers, including the gaps in Australia's existing privacy framework. The ACCC found that the 'existing Australian regulatory framework for the collection, use and disclosure of user data and personal information does not effectively deter certain data practices that exploit the information asymmetries and bargaining power imbalances between digital platforms and consumers'.[102] Despite the existence of the OAIC Guidelines and the decision in *Veda*, the ACCC recommended legislative changes to 'strengthen… consent requirements to require that consents are freely given, specific, unambiguous and informed'.[103]

2.9 Practical barriers to informed consent

Informed consent requires an individual to genuinely assent to something based upon a proper understanding of the relevant practices and their consequences.[104] Service providers hold extensive power as they determine what data their systems collect, what services are accessible to their customers, and the design of their ICT architecture.[105] Many digital data practices of service providers are not visible to consumers, with the only visibility available in the form of user agreements and privacy notices, and, in many cases, limited control over privacy settings.[106]

Given the hidden nature of a provider's activities, a consumer must engage in several steps before they can give informed consent to an entity's commercial data handling practices. Firstly, a consumer must locate or be made aware of information describing how the entity will collect, use or disclose consumer data. This is usually presented in the form of a user agreement and privacy policy that can be found on the service provider's website, but may consist of numerous different webpages and/or agreements, often connected by various hyperlinks. The consumer must then read the information, and having read the information, the consumer must understand what it means. Finally, once a consumer has read and fully

---

[96] Ibid 197.
[97] Ibid 199.
[98] Ibid.
[99] Livaja (n 84) 338.
[100] Briedis, Webb and Fraser (n 86) iv.
[101] ACCC (n 1).
[102] Ibid 434.
[103] Ibid 24.
[104] Briedis, Webb and Fraser (n 86) 52.
[105] Marcin Betkier, 'Individual Privacy Management' (2016) 21 *Media and Arts Law Review* 315, 317.
[106] Ibid 320. See further Kemp (n 26).

understood the information about a service provider's data handling practices, they must be able to determine the impact of these practices on them, and compare this with the information of other providers in order to make a free and informed decision as to whether to consent to each of the commercial data handling practices.[107]

There are myriad business practices that service providers engage in throughout these steps that prevent a consumer from providing informed consent. These practices create information asymmetries and power imbalances between service providers and consumers which make it difficult for consumers to assess the quality of data protection offered by different providers, and to make an informed decision on whether to allow a provider to collect, use and disclose their personal information.[108]

2.9.1 Browsewrap and Clickwrap Agreements

It is typical for a consumer to be faced with a user agreement and privacy policy to which they signal acceptance using the services ('browsewrap agreement'), or by clicking a button to indicate the acceptance of such terms ('clickwrap agreement').[109] The problem with these agreements is that they often involve a request for bundled consents. Bundled consents are likely to pressure consumers into providing overall consent to numerous collections despite actually being concerned about one or more particular practices.[110] When a consumer is presented with a browsewrap or clickwrap agreement, they have no opportunity to negotiate terms but are instead forced to agree to all consents on a take-it-or-leave it basis.[111]

Researchers have identified a distinction between such contractual acceptance and informed consent.[112] In their view, acceptance of browsewrap or clickwrap agreements should not be regarded as indicating that the consumer provides genuine, informed consent for the commercial handling of personal information.[113] This is consistent with the ACCC's finding that 'take-it-or-leave-it' terms creates a significant bargaining power imbalance between service providers and consumers, such that providers can unilaterally set the terms of use and privacy policies, which often include the right to amend their terms.[114] Consumers are unable to provide informed consent at the time of accepting such terms because they are unable to reasonably foresee the consequences of such acceptance.[115] Consumers often do not realise they are entering into a continuous, long-term agreement relating to the collection, use and disclosure of their personal data.[116]

Under Australia's existing legislative and regulatory framework, there is no strict regulation on the use of these standard form agreements and the law views acceptance of such agreements as valid consent. Whilst the OAIC states in its OAIC Guidelines that bundled consent has the potential to undermine the voluntary nature of consent,[117] its determination in *FRLC v Veda* (discussed in section 2.6 above) indicates that bundled consents are valid under the existing law.[118] In this case, consumers were presented with two tick boxes upon signing up to the relevant service, with one of the tick boxes seeking a broad consent to

---

[107] Briedis, Webb and Fraser (n 86) iv-vi.
[108] ACCC (n 1) 403.
[109] Briedis, Webb and Fraser (n 86) 41.
[110] Briedis, Webb and Fraser (n 86) 56.
[111] McKay et al (n 94).
[112] See Briedis, Webb and Fraser (n 86) 52; Brigid Richmond, *A Day in the Life of Data: Removing the opacity surrounding the data collection, sharing and use environment in Australia* (Report, Consumer Policy Research Centre, 29 May 2019).
[113] Briedis, Webb and Fraser (n 86) 52.
[114] ACCC (n 1) 394, 397.
[115] Betkier (n 105), 320.
[116] Ibid.
[117] OAIC, 'Australian Privacy Principles Guidelines: *Privacy Act* 1988' (n 29) B.46.
[118] *FRLC v Veda* (n 47).

direct marketing for 'offers relating to finance', and providing personal information to 'relevant corporate partners'.[119] The OAIC deemed the acceptance of the agreement through that tick box as valid consent.[120] This decision highlights the need for enforceable guidelines over standard form agreements to ensure consumers have greater autonomy in deciding how platforms handle consumer information, and therefore, are able to provide informed consent.

2.9.2 Intelligibility of Privacy Policies

Consumers require adequate information about a platform's practices in order to make an informed decision as to whether to engage a service provider.[121] In principle, privacy policies should fill the information gap between the consumer and the service provider by giving the consumer a complete understanding of the provider's commercial data handling practices.[122] In practice, lengthy, complex and vague privacy policies have proven ineffective disclosure tools that do not adequately assist consumers in making informed choices.[123]

Under the *Privacy Act,* APP 1.3 requires an APP entity to have a clearly expressed and up to date policy about the management of personal information about the entity.[124] The current legislative and regulatory framework in Australia, however, does not adequately regulate the use of standard form agreements in providing the necessary information required for consumers to make informed decisions about the commercial handling of their data. User agreements and privacy policies are often lengthy, complex and vague, and commercial entities engage in concealed data practices that are not appropriately disclosed in their policies.[125] Consumers are faced with the burden of having to read and decipher such agreements, only to be faced with little choice but to accept such terms in order to access the product or service.

2.9.2.1 Length

An early study conducted by US researchers in 2008 estimated that consumers are likely to encounter an average of 1,462 privacy policies a year for all the various online services they use and different websites that they visit.[126] The study estimated that it would take an individual 244 hours per year to read, or 154 hours per year to skim, all these privacy policies.[127] More recent figures from an A*CCA*N project found that the privacy policies in their study contained an average of 3232 words and would take an average reader 13 minutes to read a privacy policy of average length.[128] Similarly, the ACCC found it would take an average reader between 10 and 20 minutes to read the privacy policies of the major digital platforms.[129] This figure can be expected to increase given the growing number of online services and digital applications.

Consumers face an enormous time cost for reading all privacy policies, particularly given they often do not fully understand the information presented to them (discussed below), nor do they feel they have any other choice but to accept to the terms in order to access the

---

[119] Ibid 153.
[120] Ibid 191.
[121] Lauren Solomon, *Submission to the Consultation on the ACCC Digital Platforms Inquiry Preliminary Report December 2018* (Consumer Policy Research Centre, 15 February 2019) 4.
[122] Janice Y Tsai et al, 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study' (2011) 22(2) *Information Systems Research* 254, 256.
[123] Ibid.
[124] *Privacy Act 1988* (Cth) APP 1.3.
[125] Kemp (n 25).
[126] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) *I/S: A Journal of Law and Policy for the Information Society* 543, 561.
[127] Ibid 563.
[128] Briedis, Webb and Fraser (n 86).
[129] ACCC (n 1) 598.

product or services (discussed above).[130] The cost of reading online policies is a significant barrier to consumers providing informed consent, and consumer surveys indicate that a thorough reading of these documents is not perceived to contribute to consumer welfare.

2.9.2.2 Complexity

Even where consumers read data policies, the documents are often littered with legal jargon and technical terminology, making it difficult for consumers to understand the information presented to them. The data handling practices of online platforms and digital applications often involve technical processes that are unknown to, or difficult to understand by an average consumer.[131] For example, algorithms may be used to collect information about an individual consumer and select which products and services are promoted or displayed to the consumer, however, an average consumer may not understand what these algorithms are or how they affect their purchasing options.[132] Similarly, many consumers would not understand the consequences of suppliers collecting their location data; how 'beacons', 'tags' and 'pixels' are used to track online behaviour; or how to effectively prevent tracking of their online activities.

The complex nature of data handling practices and the existence of lengthy and complex data policies make it difficult for consumers to reasonably comprehend or manage how their data is collected, used, and disclosed across all the platforms they use. As such, consumers are vulnerable to entering unfair or misunderstood contractual agreements.[133] Some researchers have proposed regulatory measures focused on shortening and simplifying user agreements and privacy policies and standardising their terms to increase consumer engagement and understanding of such documents.[134]

2.9.2.3 Broad, vague and incomplete language

Consumers require precise and meaningful information about a platform's practices in order to make an informed decision as to whether to engage a service provider.[135] Whilst the inherent purpose of a privacy policy is to inform a reader about the nature of the entity's data practices, it is not uncommon for terms to be expressed in broad, vague or incomplete language that do not reveal the actual practices of the entity.[136]

The OAIC Guidelines state that 'an APP entity should not seek a broader consent than is necessary for its purpose, for example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures'.[137] In practice, vague terms and examples of what information 'may' be collected are used in many policies in an attempt to give service providers a wider scope to collect and use information, and reduce the risk of liability for potentially unlawful data practices.[138] This is particularly the case when it comes to informing consumers about the disclosure of data to third-parties. Many service providers indicate in their privacy policies that they may pass on information to third parties, however, these third parties are usually described in vague terms such as 'affiliates' or 'trusted partners'.[139] Privacy policies often do not specify the type of information that will be

---

[130] Briedis, Webb and Fraser (n 86).
[131] McKay et al (n 94).
[132] Ibid.
[133] Ibid 7.
[134] Yannis Bakos, Florencia Marotta-Wurgler and David R Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts' (2009) *CELS 2009 4th Annual Conference on Empirical Legal Studies Paper* NYU Law and Economics Research Paper No. 09-40. 31.
[135] Solomon, (n 121) 4.
[136] Kemp (n 25).
[137] OAIC, 'Australian Privacy Principles Guidelines: *Privacy Act* 1988' (n 29) B.50.
[138] Richmond (n 112).
[139] Ibid.

disclosed, to whom information will be disclosed, and how these third parties will use this information.[140]

Numerous researchers highlight the need for increased transparency over the collection, use and sharing practices of online platforms, in order to increase consumer understanding and choice.[141] This should not be misinterpreted as 'more information' equals 'better information',[142] but requires certainty and specificity as to the factual elements and duration of the request.[143] The factual elements relate to the specific data collected, the purposes for which the data will be used, and specific parties to which disclosures will be made.[144] In relation to the duration of a request, researchers argue that indefinite consent creates a distance between the original permission granted and the purpose to which personal information is used or disclosed.[145] Without limitations on future use of personal information, it is not possible for individuals to accurately weigh the costs and benefits of providing their data because it is difficult to predict how their data will be used over time and the privacy harms that may occur.[146]

2.9.3 Design features

Design features of platforms and user interfaces are another barrier preventing consumers from giving informed consent. Firstly, consumers may find it difficult to navigate some online platforms to find relevant information about the provider's data handling practices.[147] Some providers have numerous interlinked policies that require consumers to click between multiple documents. For example, Google has a separate privacy policy for each of its services, including Chrome, Play, Payments, G Suite, YouTube etc, as well as a central privacy policy and terms of use that apply to all these services.[148] The problems with navigation, combined with lengthy and complex privacy policies, can make it difficult for consumers to decide whether or not to give consent to the collection, use and disclosure of their personal information.[149]

Numerous researchers have discussed the practice of 'nudging'.[150] While 'nudging' can be beneficial, for example in public health settings, in this chapter I use it in the sense of 'dark patterns', where interface design is crafted in a way that manipulates users into providing more personal information than necessary for the interaction.[151] In particular, the use of default settings or hidden pre-selections can cause potential confusion or may nudge consumers towards more privacy intrusive options.[152] When service providers use such

---

[140] See, for example, Facebook's Data Policy https://www.facebook.com/policy.php which provides a general list of third parties such as 'partners who use our analytics services', 'advertisers', vendors and service providers' etc., however, does not specifically provide the names of these third parties nor detail the purposes for which the third parties will use the consumer information.
[141] See CPRC 2018 Survey (n 4); Richmond (n 112).
[142] CPRC 2018 Survey (n 4).
[143] Briedis, Webb and Fraser (n 86).
[144] Ibid.
[145] Ibid.
[146] CPRC 2018 Survey (n 4) 43; Kemp (n 25).
[147] Ibid 406.
[148] Ibid.
[149] Ibid 404-406.
[150] Eg Richard H. Thaler and Cass R. Sunstein, *Nudge: improving decisions about health, wealth, and happiness* (Yale University Press, 2008); Ryan Calo, 'Code, nudge, or notice? (regulatory methods of influencing citizen behavior)' (2014) 99(2) *Iowa Law Review* 773;, Karen Yeung, '"Hypernudge"': Big Data as a mode of regulation by design' (2017) 20(1) *Information, Communication & Society* 118-136
[151] McKay et al (n 94); Joel R Reidenberg et al, 'Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding' (2015) 30(1) *Berkeley Technology Law Journal*, 46; Norwegian Consumer Council, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (Report, 27 June 2018) 7.
[152] ACCC (n 1) 589.

design tactics to nudge consumers toward giving their consent to share personal information, the notion of 'informed consent' is severely undermined.[153]

The Norwegian Consumer Council (NCC) report 'Deceived by Design' revealed that major platforms such as Facebook and Google have privacy intrusive default settings, misleading wording that give users an illusion of control, and platform architectures that make it difficult for consumers to choose the privacy friendly option.[154] All of these features are arguably unfair data practices. The report highlights that most consumers will never look at, let alone change, the default settings.[155] Default selection of consent (eg a tick box that is displayed already filled in) has been found to be an efficient way of manipulating consumers towards actions that benefit the service provider, but may not be in the consumer's interest.[156] EU regulators have recognised the negative impact of default settings and pre-selections on consumers, and as such the GDPR requires 'data protection by design and default'.[157] Organisations are required to implement appropriate technical and organisational measures that ensure that default settings should not allow for more collection or use of personal data than is necessary for the provision of the service.[158]

In contrast, the current Australian legislative and regulatory framework does not provide any guidance on design features and the use of default settings. The ACCC Digital Platforms Inquiry found that some digital platforms have user interfaces, such as default settings or pre-selections, that lead consumers to make privacy-intrusive selections.[159] The ACCC revealed that none of the digital platforms reviewed (Google, Facebook, Twitter and Apple) required a consumer to review and change their default settings before the creation of a new account.[160] Rather, an individual is opted into the default settings at the outset and has to navigate to, and change, their privacy settings themselves.[161] Despite the significant consumer demand for greater control over their personal information, the ACCC found that user interface design features of digital platforms tend not to provide consumers with effective opt-outs or meaningful controls over how their personal information is collected, used and disclosed.[162]

2.10 'Informed Consent' in other Jurisdictions

2.10.1 European Union (EU)

The EU's GDPR provides six lawful bases on which an entity can process personal data. One of these bases is where an individual gives free, specific, informed and unambiguous consent to an entity to process their personal data.[163] The consent requirements under the GDPR are much stronger than those under Australian law. Article 7 requires entities to seek consent before processing personal data, with the request for consent presented in a manner which is 'clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language'.[164] Under the definitions clause, 'consent' of

---

[153] Norwegian Consumer Council (n 151).
[154] Ibid 3.
[155] Ibid 13.
[156] Ibid; George J Stigler Center for the Study of the Economy and the State and The University of Chicago Booth School of Business, *Stigler Committee on Digital Platforms Final Report* (September 2019) ('Stigler Report') available at https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf 8, 30, 59.
[157] GDPR (n 75) art 35.
[158] Ibid.
[159] ACCC (n 1) 374.
[160] Ibid 431.
[161] Ibid.
[162] Ibid 433.
[163] GDPR (n 75).
[164] Ibid art 7.

the data subject is defined as 'any freely given, specific, informed and unambiguous indication of data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[165]

Several recitals contained in the GDPR further emphasise the need for 'informed consent', including Recital 32 which states that:

> consent should be given by a clear and affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.[166]

Further, for consent to be informed:

> the data subject should be aware of at least the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[167]

Compared with the Australian 'consent' requirements, the GDPR provides much stronger and clearer protections for consumers with respect to the handling of their data.

Since the introduction of the GDPR, several European data protection regulators have issued fines against organisations for failing to comply with the GDPR. For example, CNIL, the French data protection authority, issued a fine of €50 million to Google for its 'lack of transparency, inadequate information and lack of valid consent regarding ads personalisation'.[168] The CNIL found that Google had engaged in several practices that were in violation of the obligations of transparency and consent, including consent bundling, pre-selected consents, and vague wording of its data processing notices.[169] As such, the CNIL concluded that the users' consent was not sufficiently informed, and therefore Google had breached its obligation to obtain freely given, specific and unambiguous consent from consumers.[170]

2.10.2 United Kingdom

The data protection framework in the UK is currently governed by the EU GDPR and the *Data Protection Act 2018* (UK) (DPA). From 31 December 2020, due to the exit of the UK from the European Union, the *Data Protection, Privacy and Electronic Communications (Amendments) etc (EU Exit) Regulations 2019* created a new UK GDPR regime, but quite similar to the previous regime. A report published by the UK Human Rights Committee on privacy online discussed the consent requirements under the current UK data protection framework. The report found that many users do not have a meaningful choice to consent to the use of their personal data.[171] The Committee highlights that informed consent requires individuals to have the necessary expertise to understand the risks that may be involved in what they are

---

[165] Ibid art 4.
[166] Ibid recital 32.1.
[167] Ibid recital 32.
[168] 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC', *CNIL* (Web Page, 21 January 2019) https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.
[169] Ibid.
[170] Romain Dillet, 'French data protection watchdog fines Google $57 million under GDPR', *TechCrunch* (Online Article, 22 January 2019) https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/.
[171] United Kingdom Joint Committee on Human Rights, *The Right to Privacy (Article 8) and the Digital Revolution* (HC 1222 | HL Paper 14, 3 November 2019) 12, discusses a submission made by the think tank Doteveryone which found that 47% of survey participants felt they had no choice but to sign up to the terms and conditions, even if they have concerns about them.

consenting to, however, in practice the vast majority of individuals would find it impossible to understand what they are consenting to due to the complexity and length of agreements.[172] The Committee's view is that the 'consent model is broken' and places too much onus on the consumer to educate themselves on an entities' policies and practices.[173] Instead, the report urges the UK Government to improve the regulation of data practices by setting a higher standard of protection by default, so that individuals are protected without the burden of having to understand and monitor the activities of entities.[174]

2.10.3 Canada

The *Personal Information Protection and Electronic Documents Act (PIPEDA)* is the data protection legislation governing private-sector organisations across Canada that collect, use or disclose personal information in the course of a commercial activity.[175] Similar to the APPs contained in the Australian *Privacy Act,* PIPEDA contains 10 fair information principles aimed at protecting personal information. Principle 3 requires entities to obtain consent for the collection of personal information and the subsequent use or disclosure of this information.[176] PIPEDA does not specifically refer to 'informed consent', but states that 'to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed'.[177]

The Office of the Privacy Commissioner of Canada (OPCC) held a consultation and released a discussion paper in 2016 that examined the consent requirements under PIPEDA. Whilst the paper does not specifically discuss the notion of 'informed consent', it states that 'consent is only valid if it is reasonable to expect that an individual whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting'.[178] This statement is consistent with the view that 'informed consent' should be the legal standard required for the collection, use and disclosure of personal information. As a result of the consultation, the OPCC released new guidelines on 'meaningful' consent.[179]

2.10.4 United States

The United States does not have omnibus federal legislation that deals with data protection and privacy.[180] Rather, the US approach to data protection involves state-based legislation and federal regulation of certain sectors and contexts, such as healthcare, education or financial services.[181] The Federal Trade Commission (FTC) has become the leading privacy enforcement agency in the US, with its authority arising out of section 5 of the *Federal Trade Commission Act* which prohibits unfair or deceptive practices in the marketplace.[182] The FTC

---

[172] Ibid 25.
[173] Ibid 26.
[174] Ibid 4.
[175] 'PIPEDA in brief', *Office of the Privacy Commissioner of Canada* (Revised May 2019) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.
[176] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, Schedule 1, cl 4.3.1.
[177] Ibid cl 4.3.2.
[178] Policy and Research Group of the Office of the Privacy Commissioner of Canada, Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act (*Discussion Paper* 2016) 2 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.
[179] Office of the Privacy Commissioner of Canada, 'Guidelines for obtaining meaningful consent' (2018) https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.
[180] Shawn Marie Boyne, 'Data Protection in the United States' (2018) 66 *The American Journal of Comparative Law* 299, 299.
[181] Ibid.
[182] Ibid 305-306.

has the jurisdiction to pursue business conduct that amounts to unfair or deceptive acts or practices,[183] and has authority to enforce a variety of sector-specific laws.[184]

Children's Online Privacy Protection Act 1998

One relevant piece of federal legislation is the *Children's Online Privacy Protection Act 1998* (*COPPA*) that regulates the online collection and use of information collected from children under the age of thirteen.[185] The *Children's Online Privacy Protection Rule* (*COPPA Rule*) (in effect April 2000) aims to give parents control over what information is collected from their children online.[186] Under the *COPPA Rule*, operators of websites or online services directed at children have the obligation to obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.[187] 'Obtaining verifiable consent' means making a reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child receives notice of the operator's data handling practices, and authorizes any collection, use, and/or disclosure of personal information.[188] *COPPA* also gives parents the ability to review personal information collected about their children and request that it be deleted.[189] In comparison, Australia's *Privacy Act* does not provide any regulation of the collection, use or disclosure of the personal information of children. The OAIC Guidelines recognise that the *Privacy Act* does not specify an age of consent after which individuals can make their own privacy decisions, but state that an individual aged under 15 is presumed not to have capacity to consent.[190] As previously emphasised, the OAIC Guidelines are non-binding, and overall, Australia's privacy and data protection law framework provides weak protections for children with respect to the handling of their personal information.[191]

California Consumer *Privacy Act* 2018

The most notable state regulation is the *California Consumer Privacy Act* (CCPA), which was passed in June 2018.[192] The CCPA applies to for-profit businesses that have annual gross revenue in in excess of $25 million; receive, sell or share for commercial purposes the personal information of 50,000 or more California residents; or derive more than 50% of their annual revenue from selling California residents' personal information.[193] Whilst CCPA does not specially mention the notion of informed consent, it grants California consumers numerous rights relating to the access to, deletion of, and sharing of personal information collected by businesses about them.[194]

Under CCPA, a California consumer has the right to request that a business that collects their personal information disclose the categories and specific pieces of personal information the business has collected,[195] or request the business to delete any personal information the business has collected about them.[196] Consumers have the right to request

---

[183] *Federal Trade Commission Act* of 1914, 15 USC § 45.
[184] Boyne (n 180) 306.
[185] Children's Online Privacy Protection Act of 1998, 15 USC §§ 6501-6506 (1998) ('COPPA').
[186] Boyne (n 180) 310.
[187] Children's Online Privacy Protection Rule 16 CRF Part 312, § 312.5(a).
[188] Ibid § 312.2.
[189] Ibid § 312.6.
[190] OAIC Guidelines (n 29) [B.56] – [B.58].
[191] See paragraph 2.4 for a discussion of the OAIC Guidelines (n 29).
[192] California Consumer *Privacy Act* of 2018 (CCPA), Cal Civil Code s 1798.100-1798.199.
[193] Ibid s 1798.140(c).
[194] Stigler Report (n 156) 224.
[195] CCPA (n 192) s 1798.100.
[196] Ibid s 1798.105.

information about the categories of data being shared with third parties, the categories of third parties to whom the data is shared with,[197] and at any time, to direct a business not to sell their information to a third party. [198] A third party that has been sold information about a consumer by a business cannot sell that personal information unless the consumer is provided explicit notice and an opportunity to exercise the right to opt-out.[199] These rights allow customers greater access to and control over their personal information, particularly in relation to third-party sharing.

2.10.5 The utility of other jurisdictions' approaches

This examination of the approaches of other jurisdictions does yield some useful material, but none without their own problems. For example, the GDPR's much stronger consent requirements requires much more specific disclosures, but does little to address the practical problem of how consumers can realistically deal with the volume of material with which they are being presented. The UK Human Rights Committee recommendations are more attractive: that is, a better basic standard of data protection, below which businesses should not be allowed to operate, shifting some of the onus on good data practice to businesses rather than consumers. The strong rights to deletion, 'no-sell' directions and opting out of third-party dealings offered by the CCPA are also worth examining in the Australian context. In relation to children's rights, the COPPA requirements of parental consent are useful, but suffer the same problems as consent to processing adults' data, in addition to the likelihood that parents will be put under pressure by their children to give their consent.

2.11 *Australian Consumer Law* Framework

Service providers are in a position to know more about their data handling practices than consumers,[200] and the provision of information through agreements or notices can affect an individual's decision as to whether to consent to the provider's practices. As discussed in the previous section, the use of browsewrap or clickwrap agreements and long, complex and vague privacy policies can create information asymmetries and power imbalances between the service provider and consumer. These problems are not addressed by the *Privacy Act*, with its underinclusive and vague definitions, limited enforcement, lack of hard law and jurisprudence resulting in a failure to protect consumers from these business practices. However, the *ACL* framework has been mooted as a potential source of more effective protection for consumers.[201]

The objective of the *Competition and Consumer Act 2010* (Cth), which contains the *ACL*, is to enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection.[202] There are a number of reasons why consumer law remains a more fertile area than current privacy legislation for examining the existence of effective mechanisms to protect individuals from unwanted collection, use and disclosure of data.[203] First, the drafters of the *ACL* and its predecessors recognised that 'consent' is insufficient to absolve sellers of responsibility for their marketing activities, and that consumers need to be protected against seller misconduct even when they have said 'yes' to a transaction.[204] This normative outlook is demonstrated by the nature of the marketing and

---

[197] Ibid s 1798.115(a).
[198] Ibid s 1798.120.
[199] Ibid s 1798.115(d).
[200] Manwaring (n 85) 155.
[201] Damian Clifford and Jeannie Paterson, 'Consumer Privacy and Consent: Reform in The Light of Contract and Consumer Protection Law' (Pt 10) (2020) 94 *Australian Law Journal* 741.
[202] Competition and Consumer Act 2010 (Cth) sch 2 ('*Australian Consumer Law*') s 2.
[203] Manwaring (n 85) 177.
[204] Ibid.

selling protections contained in the *ACL*: for example, the prohibitions against misleading or deceptive conduct and false or misleading representations (ss 18 and Part 3-1 Div 1), unconscionable conduct (ss 20–22), and unfair contract terms (ss 23–27). All these provisions presume that the conduct regulated detrimentally affects the quality of a consumer's consent to entering a transaction, or to the terms which are offered. They also assume that this effect on consent is unacceptable, and should be prohibited or mitigated in some way.

This fundamental acknowledgment that 'consent' is not sufficient to protect consumers in a broad range of circumstances provides a more reasonable, and consumer-friendly, framework than the *Privacy Act*. The comparative strength and activity of the *ACL* regulators (namely the ACCC and state and territory fair trading agencies) as compared to the OAIC,[205] also displays an advantage for consumer protection law over Australia's current data protection legislation.

2.11.1 Misleading and deceptive conduct

Privacy policies, and other representations concerning the use of personal information, can be contained in standard form contracts or as stand-alone representations. Where these policies or representations are provided in the course of trade or commerce, they are subject to the misleading or deceptive conduct provisions of the *ACL*,[206] and in some cases the false or misleading representations provisions (discussed below).

Section 18 of the *ACL* prohibits a person in trade or commerce engaging in conduct which is misleading or deceptive, or is likely to mislead or deceive. Any person may bring an action for a wide range of civil remedies, including the regulator, an individual or a competitor. Additionally, Part 3-1 Div 1 of the *ACL* further regulates false or misleading representations, and misleading or deceptive conduct, in relation to the supply and/or (in the circumstances of section 29) promotion of goods or services. The relevant provisions of Part 3-1 Div 1 (sections 29, 33 and 34) not only attract civil pecuniary penalties for proceedings brought by the regulator,[207] but are mirrored in sections 151, 155 and 156 of the *ACL* which provide for strict criminal liability.

While section 18 applies generally, sections 29, 33 and 34 prohibit a set of specific false and misleading representations and misleading and deceptive conduct from a closed list, reflecting the harsher penalties applicable to those sections. This list applies to representations in the supply and promotion of goods and services, including misrepresentations relating to:

- standard, quality, value or grade (section 29(1)(a)–(b));
- performance characteristics or uses (section 29(1)(g));
- necessity (section 29(1)(l)); and
- existence, exclusion of effect of any condition, warranty, guarantee, right or remedy (section 29(1)(g)–(h)).

Sections 33 and 34 prohibit misleading conduct as to the nature, characteristics and suitability for purpose of goods and services.

So, if for example a provider collected a user's email address through a mobile phone app and then sold it to a third party despite its privacy policy saying it would not share any information provided to the app, then this would likely constitute misleading and deceptive

---

[205] Ibid, 176.
[206] Gordon Hughes and Lisa di Marco, 'Online privacy policies — it's not just about the *Privacy Act*' (2015) 18(2) *Internet Law Bulletin* 38.
[207] Mirror provisions relating to financial services are found in sections 12DA and 12DB of the *Australian Securities and Investments Commission Act 2001* (Cth) ('*ASIC Act*').

conduct under section 18, and also a false and misleading representation under section 29(1)(g).

Despite their popularity in almost every other aspect of commercial and consumer transactions, little use was made of these provisions in Australia in relation to protection of consumer data until late 2019. In October 2019, the ACCC instituted proceedings against Google LLC and Google Australia Pty Ltd (together, Google) alleging breaches of sections 18, 29(1)(g), 33 and/or 34. These proceedings were filed in response to on-screen representations Google made concerning user control over location data and Google's use of that data collected from Android mobile phones and tablets.[208] The hearing for this case scheduled for November 2020 was vacated and mediation scheduled, but as of late 2020 the case appears to be continuing in the Federal Court.[209] Less than a year after the first filing, the ACCC followed up with new proceedings against Google LLC claiming breaches of sections 18, 29, and 34. These proceedings concern an alleged failure by Google LLC to obtain explicit and informed consent (contrary to clauses in Google LLC's earlier privacy policy) when Google LLC decided to change the way data was used by the company, as well as additional conduct contrary to its privacy policy.[210]

However, to determine the likelihood of these *ACL* provisions applying to conduct of businesses in collecting, processing and communicating personal information, it is important to understand certain concepts. These concepts concern the nature of 'conduct' and the extent to which consumers must take 'reasonable care of their own interests' in assessing the effect or likely effect of conduct.

2.11.1.1 Conduct and leading into error

Under section 29, a 'misrepresentation' is required. However, this is not the case for section 18 (nor likely in terms of sections 33 and 34, both of which use the language of 'conduct' rather than 'representation'). In 2010, the High Court confirmed that '[f]or conduct to be misleading or deceptive it is not necessary that it convey express or implied representations ... It suffices that it leads or is likely to lead into error'.[211] Therefore, section 18 of the *ACL* covers a broader range of conduct than section 29, due to its open-ended definition and the absence of a misrepresentation requirement. However, even absent a misrepresentation, someone must be led (or likely to be led) into error.

It is also important to note that misleading or deceptive *omissions*, *opinions* and *statements* of law are caught under s 18.[212] In relation to opinions around future events, s 4 of the *ACL* states that any representation as to a future matter must be based on 'reasonable grounds'; otherwise it is misleading. Case law has established that statements of opinion must be genuinely held; if they are not, they can be misleading.[213] As most privacy policies include

---

[208] Concise statement, NSD1760/2019, *ACCC v Google LLC & Anor*, 29/10/2019, available at https://www.accc.gov.au/system/files/Concise%20Statement_ACCC%20v%20Google%20Australia%20Pty%20Ltd%20%26%20Anor_%2029.10.19.pdf

[209] According to a search carried out on 22 December 2020 on the Commonwealth Courts Portal (File No NSD1760/2019) https://www.fedcourt.gov.au/services/check-progress-of-a-case

[210] Concise statement, NSD816/2020, *ACCC v Google LLC*, available at https://www.accc.gov.au/system/files/ACCC%20v%20Google%20LLC%20-%20Concise%20Statement.pdf. Some additional actions are discussed in Part 3.3.3.4.2 of Chapter 3.

[211] *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Ltd* [2010] HCA 31 [15].

[212] Colin Lockhart, *The Law of Misleading or Deceptive Conduct* (4th edn, LexisNexis Butterworths 2015) [2.5]–[2.6]; Heydon, *Trade Practices Law: Competition and Consumer Law* (Thomson Legal & Regulatory) [160.430] (online version, accessed 16 January 2018).

[213] *Tobacco Institute of Australia Ltd v Australian Federation of Consumer Organisations Inc* [1992] FCA 630 [47]; *Global Sportsman Pty Ltd v Mirror Newspapers Ltd* [1984] FCA 180 (*Global Sportsman v Mirror Newspapers*) [17]; *Commonwealth Bank of Australia v Smith* [1991] FCA 375 [71]–[72]; *Stoker v Pomcol Pty Ltd* [1987] FCA 90 [15]; *Adour Holdings Pty Ltd v Commonwealth Bank of Australia* [1991] FCA 502 [21].

representations as to future matters - that is, what businesses are planning to do with information collected from consumers – these principles are important. Additionally, some privacy policies contain statements about compliance by the business with the *Privacy Act,* arguably a statement of law. Although it is common to make a distinction between statements of fact and statements of law, a misleading statement of the law still contains a factual error, subsisting in the mistaken belief that a particular principle can be enforced by legal means when in fact it cannot (and vice versa).[214]

2.11.1.2 Reasonable care

As stated by the Full Federal Court in *Global Sportsman v Mirror Newspapers*, the court must be 'concerned with the effect or likely effect of conduct upon the minds of those by reference to whom the question of whether the conduct is or is likely to be misleading or deceptive falls to be tested'.[215] The test as to whether such conduct was misleading or deceptive is objective rather than subjective.[216] Gibbs CJ in *Parkdale v Puxu* stated that courts must consider:

> the effect of the conduct on reasonable members of the class. The heavy burdens which the section creates cannot have been intended to be imposed for the benefit of persons who fail to take reasonable care of their own interest.[217]

The 'reasonable care' standard has been supported in several subsequent cases.[218] The High Court in *Campomar v Nike*[219] held the relevant question to ask is whether:

> the 'ordinary' or 'reasonable' members of the class of prospective purchasers of a mass marketed product for general use' would be misled, and the court would exclude the effect of those 'whose reactions are extreme or fanciful.[220]

However, the difference between an 'ordinary' consumer and a 'reasonable' one is still unclear, and is relevant to the discussion below concerning consumers subject to cognitive biases and other vulnerabilities. More recently, the High Court in *ACCC v TPG*[221] also adopted the *Parkdale v Puxu* formulation of 'reasonable care', subject to the existence of a causal link between the defendant's conduct and the error of the alleged victim.[222]

However, Lockhart casts some doubt on the existing authority that this requirement of a 'reasonable person' applies in all cases.[223] He proposes instead that the requirement was only intended to apply to relatively sophisticated purchasers and high-value property, as in *Parkdale v Puxu*, where a greater standard of care should be expected. His assessment of the interpretation of the 'reasonable care' standard in the High Court and lower courts is that 'extreme, fanciful or unusually foolish interpretations of widely disseminated conduct' will not mean that the relevant sections are breached, but 'uncertainty remains' as the extent to which a 'reasonable care' standard can be applied.[224]

---

[214] *Public Trustee v Taylor* [1978] VR 289.
[215] *Global Sportsman v Mirror Newspapers* (n 213)[14].
[216] Ibid.
[217] *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* [1982] HCA 44 [9].
[218] *Commercial Dynamics Pty Ltd v M Hawke Nominees Pty Ltd* [1996] FCA 1394 [8]; *WEA International Inc v Hanimex Corp Ltd* [1987] FCA 379 [22]; *Tec & Tomas (Australia) Pty Ltd v Matsumiya Computer Co Pty Ltd* [1984] FCA 14 [25]; *Decor Corp Pty Ltd v BoWater Scott Ltd* [1985] FCA 218 [15], [17]; *National Exchange Pty Ltd v Australian Securities & Investments Commission* [2004] FCAFC 90 (*National Exchange v ASIC*) [18].
[219] *Campomar Sociedad Limitada v Nike International Ltd* [2000] HCA 12.
[220] Ibid [105].
[221] *Australian Competition and Consumer Commission v TPG Internet Pty Ltd* [2013] HCA 54.
[222] Ibid [39].
[223] Lockhart, *The Law of Misleading or Deceptive Conduct* (n 212) [3.29].
[224] Ibid.

If a criterion of 'reasonable care' *is* applied, this is problematic for at least some cases of questionable data practices. Many of the provider practices in designing websites and other consumer interfaces outlined in paragraph 2.9.3 (design features) are designed to undermine the consumer's capacity to take reasonable care. These practices do not in themselves lead a consumer into *error*, but into conduct against their interests, by taking advantage of common and individual cognitive biases and/or vulnerabilities.[225] The conduct may prey on their need for the product or service, their feeling that they cannot get a better deal, or learned helplessness. However, this is *manipulative conduct* as opposed to *misleading and deceptive* conduct. Where there is a misrepresentation, s 18 (and possibly ss 29, 33 and 34) of the *ACL* will apply to such conduct. However, conduct that is merely unfair does not constitute a breach of s 18 unless it leads the 'victim' into error.

Therefore, the misleading and deceptive conduct provisions may not provide a full remedy for problematic digital data practices. In some cases, consumers may nevertheless find a remedy under other provisions of the *ACL* such as those governing unconscionable conduct or unfair terms.

2.11.2 Unconscionable conduct

2.11.2.1 Elements of unconscionable conduct

Conduct that is 'unconscionable' is prohibited under sections 20 and 21 of the *ACL* (and in mirror provisions relating to financial products and services in the *Australian Securities and Investment Commission Act 2001* (Cth) ('*ASIC Act*')).[226] No definition of unconscionability is provided in the sections, and Australian appellate courts have shown a marked reluctance to attempt a precise definition.

Section 21 prohibits unconscionable conduct in connection with the actual or possible supply of goods or services. Section 22 sets out a non-exhaustive list of matters to which a court may have regard when assessing whether conduct is unconscionable under section 21. The matters most relevant to unfair data practices include:

- relative bargaining power (section 22(1)(a));
- undue influence or pressure, or unfair tactics (section 22(1)(d));
- consistency of supplier's conduct towards others (section 22(1)(f));
- unreasonable failure to disclose conduct affecting consumer interests or unforeseeable risks to the customer (sections 22(1)(i) and (ii)); and
- the extent to which both parties acted in good faith (section 22(1)(k)).

Additionally, section 21(4)(a)–(c) states as 'interpretative principles' that the doctrine:

(a) is not limited by the 'unwritten law' (that is, case law) of unconscionable conduct;
(b) applies to 'a system of conduct or pattern of behaviour, whether or not a particular individual is identified as having been disadvantaged by the conduct or behaviour'; and
(c) includes terms and performance, not just formation, of a contract.

Remedies for breach of the unconscionable conduct provisions are significant, and include civil pecuniary penalties.[227] However, breach of the unconscionable conduct provisions does *not* attract a criminal remedy.

---

[225] Manwaring (n 85).
[226] Ss 12CA, 12CB and 12CC *ASIC Act*. The NSW Court of Appeal in *Tonto Home Loans Australia Pty Ltd v Tavares* [2011] NSWCA 389 (*Tonto v Tavares*) [290] confirmed that the meaning of unconscionability under the *ASIC Act* was not 'distinct or different' from the equivalent *ACL* provisions. However, some remedies may differ: see Gail Pearson, 'The Ambit of Unconscionable Conduct in Relation to Financial Services' (2005) 23 *Company and Securities Law Journal* 105, 107–09.
[227] *ACL* s 224.

Section 20 of the *ACL* also prohibits unconscionable conduct 'within the meaning of the unwritten law', which is a reference to the law of equity in respect of unconscionable dealing. However, it is unlikely that this provision will directly apply to digital data practices, due to the operation of section 20(2) of the *ACL*, which excludes conduct prohibited by section 21. The effect of the two provisions is that section 20 will only apply in the very rare case where conduct is in trade or commerce, but is not in relation to the supply or potential supply, or acquisition or potential acquisition, of goods or services. Almost all data practices considered in this chapter would relate to the supply or possible supply of goods or services, even if that supply is for a zero-monetary price. Further, while it is still possible to bring an equitable claim under the general law where conduct is not in trade or commerce, there are no commercial data practices which would fall outside the broad scope of 'trade or commerce'.

2.11.2.2 Meaning of unconscionable conduct

It is difficult to extract from the statute and the cases the precise meaning of 'unconscionable conduct' under section 21. One definition adopted in several decisions is 'showing no regard for conscience; irreconcilable with what is right or reasonable'.[228] However, there is still no widely-accepted standard in the case law.[229] In contrast, the definition of section 20 or 'unwritten law' unconscionability is somewhat clearer due to the seminal High Court decision in *Commercial Bank of Australia Ltd v Amadio*.[230] Here, the court required an 'unfair or unconscientious advantage' to have been taken of a party who was at a 'special disadvantage'.[231] The existence of an *Amadio* 'special disadvantage' may be relevant to the assessment of unconscionable conduct under sections 21–22, but it is not *required*.[232] It also sets a higher standard than that which is required for section-21 unconscionability.

The technological neutrality of section 21 does, on its face, leave room for statutory unconscionability to capture problematic digital data practices. However, its meaning and effectiveness remain contentious.[233] Repeated criticism by consumers, small business, downstream suppliers and scholars has included concern about:

- the high threshold for contravention,[234] in that conduct which is merely unfair[235] is unlikely to be considered unconscionable without additional factors;
- failure of the provisions to provide any real guidance to assess whether particular forms of conduct would be considered unconscionable;[236] and

---

[228] *Qantas Airways Ltd v Cameron* (1996) 66 FCR 246, 262; *Hurley v McDonald's Australia Ltd* [1999] FCA 1728 [21]; *Tonto v Tavares* (n 226) [291].
[229] Jeannie Paterson and Gerard Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) 38 *Journal of Consumer Policy* 331, 343.
[230] *Commercial Bank of Australia Ltd v Amadio* [1983] HCA 14.
[231] Ibid [5].
[232] Explanatory Memorandum, Competition and Consumer Legislation Amendment Bill 2010 (Cth) [2.23].
[233] See summary of contentious elements in Manwaring (n 85).
[234] Gerard Brody and Katherine Temple, 'Unfair But Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (2016) 41 *Alternative Law Journal* 169, 170. See in particular the formulation in *ACCC v Allphones Retail Pty Ltd (No 2)* [2009] FCA 17 (*ACCC v Allphones*) [113] which requires that 'the privacy actions of the alleged contravenor show no regard for conscience, and be irreconcilable with what is right or reasonable' (although note that this was an interlocutory application).
[235] *Australian Competition and Consumer Commission v ACN 117 372 915 Pty Ltd (in liq) (formerly Advanced Medical Institute Pty Ltd)* [2015] FCA 368 [39].
[236] Manwaring (n 85).

- practical enforcement difficulties due to difficulties of proof[237] and vulnerable victims lacking practical capacity to bring actions themselves or providing poor testimony for regulator actions.[238]

The contention surrounding the doctrine has led to multiple government and parliamentary inquiries since the introduction of statutory unconscionability in 1986.[239] There have been repeated requests amend the *ACL* to include a specific definition or list of examples of unconscionable conduct (as was done for the unfair contract terms provisions).[240] The government and parliamentary inquiries have led to some restructuring of the sections and amendments to supporting wording, such as the introduction of section 21(4). But overall, successive governments have refused requests for more specificity.

An additional concern has arisen due to the 2019 High Court decision in *Australian Securities and Investments Commission v Kobelt*[241] (*ASIC v Kobelt*), where the judges were split 4-3, with strong dissenting judgments by Edelman, Nettle and Gordon JJ. In the opinion of some commentators, the majority judgment 'failed to provide adequate guidance on the scope of the prohibition in responding to a business system alleged to be unconscionable'.[242] Additionally, and particularly important in the context of corporate defendants (who comprise the vast majority of the potential defendants to claims made on the basis of unfair digital data practices), *ASIC v Kobelt* arguably imposes an unacceptably high evidentiary burden to plaintiffs in proving some form of unconscientious intent or knowledge by a defendant.[243]

Many cases of unfair digital data practices could be considered as cases of 'undue influence or pressure', or 'unfair tactics', which are factors under section 22(1)(d) to which the court may have regard in making a decision about unconscionable conduct. There are several cases where inappropriate pressure or unfair tactics have been considered unconscionable.[244] However, these generally involve face-to-face or telephone contact

---

[237] Submissions to the Australian Government's Competition Policy Review held over 2014–15 (also known as the 'Harper Review'), in particular submissions of AgForce Queensland, 2; Australian Chicken Growers' Council Limited, 7-8; Australian Dairy Farmers Limited, 9-10; Australian Newsagents' Federation, 11; and National Farmers' Federation, 7. See Australia, 'Issues Paper Submissions' (*Competition Policy Review*, 2014) http://competitionpolicyreview.gov.au/issues-paper/submissions/.

[238] Brody and Temple (n 234) 171.

[239] Michelle Sharpe and Christine Parker, 'A Bang or a Whimper? The Impact of ACCC Unconscionable Conduct Enforcement' (2007) 15 *Trade Practices Law Journal* 139, 142 provides a list of *eleven* 'government reports recommending for or against unconscionable conduct provisions'. There have also been many others since 2007, for example: Australia, Senate Standing Committee on Economics, *The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974* (December 2008); Australia, Treasury, *The Nature and Application of Unconscionable Conduct Regulation: Can Statutory Unconscionable Conduct be Further Clarified in Practice?* (Issues Paper, November 2009); Australia, *Commonwealth Government Response to the Senate Standing Committee on Economics Report on The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974* (November 2009); Bryan Horrigan, David Lieberman and Ray Steinwall, *Strengthening Statutory Unconscionable Conduct and the Franchising Code of Conduct* (Expert Panel Report to the Treasury and the Department of Innovation, Science and Research, February 2010); Ian Harper and others, *Competition Policy Review: Final Report* (Harper Review) (March 2015); Consumer Affairs Australia and New Zealand, *Australian Consumer Law Review: Final Report* (March 2017).

[240] *ACL* s 25.

[241] [2019] HCA 18 (*ASIC v Kobelt*)

[242] Jeannie Paterson, et al. (2019). 'Doctrine, policy, culture and choice in assessing unconscionable conduct under statute: ASIC v Kobelt' 13 *Journal of Equity* 81, 112. See also Chris Maxwell (2019). 'Equity and good conscience: the judge as moral arbiter and the regulation of modern commerce' *Victoria Law Foundation Oration given by Justice Chris Maxwell, President, Victorian Court of Appeal* (14 August 2019).

[243] Paterson et al (n 242) 109.

[244] *Australian Competition and Consumer Commission v Lux Distributors Pty Ltd* [2013] FCAFC 90 (*ACCC v Lux*); *ACCC v AMI* (n 235); *ACCC v Origin Energy Electricity Ltd* [2015] FCA 55 (*ACCC v Origin*).

between the seller representatives and the consumers.[245] Commonly (although not exclusively),[246] some aspect of the conduct breached, or was likely to breach, other sections of the *ACL*, such as the door-to-door selling provisions,[247] unsolicited consumer agreement provisions,[248] and/or the prohibitions on misleading or deceptive conduct, and false and misleading representations.[249]

2.11.2.3 Conclusion

Consumers, regulators and advocacy organisations may find some protection from the most serious forms of unfair data practices under the statutory doctrine of unconscionable conduct, as the concept is, at least as law on the page, quite broad. However, the operation of the unconscionability provisions in the face of problematic data practices is *uncertain*. The lack of a useful definition of unconscionability, as well as the high threshold for unconscionable conduct set by *ASIC v Kobelt*, makes it difficult to assess when and where problematic data practices (and other new commercial practices) would constitute unconscionable conduct. This uncertainty may also deter proceedings by consumers and regulators.

2.11.3 Unfair contract terms

2.11.3.1 Summary of the law

Part 2-3 of the *ACL* sets out the law on unfair contract terms (UCTL). Section 23(1) currently deems unfair contract terms **void** if they are contained in a standard form consumer contract. A *consumer contract* in the UCTL is one for a supply of goods or services 'to an individual whose acquisition of the goods [or] services is wholly or predominantly for person, domestic or household use or consumption' (section 23(3)). A *standard form contract* is not defined in the *ACL*, but the ACCC's guidance provides, uncontroversially, that 'a standard form contract will typically be one that has been prepared by one party to the contract and is not subject to negotiation between the parties – that is, offered on a 'take it or leave it' basis'.[250] Section 27 of the *ACL* puts the onus of proof on the person alleging that the contract is *not* a standard form contract, and courts may take any factors into account it thinks relevant, but section 27(2) states that courts:

> must take into account the following:
>
> (a) whether one of the parties has all or most of the bargaining power relating to the transaction;
>
> (b) whether the contract was prepared by one party before any discussion relating to the transaction occurred between the parties;

---

[245] For example, *Australian Securities and Investments Commission v Malouf Group Enterprises Pty Ltd* [2018] FCA 808 (*ASIC v Malouf*); *Ibrahim v SCE Solar City Enterprises Pty Ltd* [2017] NSWCATCD 96 (*Ibrahim v SCE*); *ACCC v Get Qualified Australia Pty Ltd (in liq) (No 2)* [2017] FCA 709 (*ACCC v Get Qualified*); *ACCC v Acquire Learning & Careers Pty Ltd* [2017] FCA 602 (*ACCC v Acquire*); *ACCC v Clinica Internationale Pty Ltd (No 2)* [2016] FCA 62 (*ACCC v Clinica*); *ACCC v Lux* (n 244); *ACCC v Origin* (n 244); *ACCC v Titan Marketing Pty Ltd* [2014] FCA 913 (*ACCC v Titan*).

[246] See for example, *National Exchange v ASIC* (n 218), where unconscionability was found but NOT misleading and deceptive conduct.

[247] For example, *ACCC v Get Qualified* (n 245); *ACCC v Acquire* (n 245); *ACCC v Origin* (n 244); *ACCC v Titan* (n 245); *ACCC v Lux* (n 244).

[248] For example, *ACCC v Nuera Health Pty Ltd (in liq)* [2007] FCA 695; *ACCC v Titan* (n 245); *ACCC v Origin* (n 244); *ACCC v Clinica* (n 245); *ACCC v Acquire* (n 245); *ACCC v Get Qualified* (n 245); *Ibrahim v SCE* (n 245); *ASIC v Malouf* (n 245).

[249] *ACCC v Lux* (n 244).

[250] ACCC, 'Unfair contract terms', *Business Rights and Protections* (Web Page) https://www.accc.gov.au/business/business-rights-protections/unfair-contract-terms.

(c) whether another party was, in effect, required either to accept or reject the terms of the contract (other than the terms referred to in section 26(1)) in the form in which they were presented;

(d) whether another party was given an effective opportunity to negotiate the terms of the contract that were not the terms referred to in section 26(1);

(e) whether the terms of the contract (other than the terms referred to in section 26(1)) take into account the specific characteristics of another party or the particular transaction;

(f) any other matter prescribed by the regulations.

Under section 24, a term in a standard form contract is considered *unfair* (and therefore void) if:

(1) …

(a) it would cause a significant imbalance in the parties' rights and obligations arising under the contract; and

(b) it is not reasonably necessary in order to protect the legitimate interests of the party who would be advantaged by the term; and

(c) it would cause detriment (whether financial or otherwise) to a party if it were to be applied or relied on.

(2) In determining whether a term of a contract is unfair under subsection (1), a court may take into account such matters as it thinks relevant, but must take into account the following:

(a) the extent to which the term is transparent;

(b) the contract as a whole.

(3) A term is ***transparent*** if it is:

(a) expressed in reasonably plain language; and
(b) legible; and
(c) presented clearly; and
(d) readily available to any party affected by the term.

Section 26 exempts some terms from the prohibition, namely: those defining the main subject matter of the contract; setting upfront price; or terms required or expressly permitted by law. The same provisions apply to small business contracts, which may be particularly relevant to data practices in respect of sole traders.

2.11.3.2 Applicability of the UCTL to privacy policies and privacy representations: a difficult problem

The ACCC stated in the DPI Final Report that '[d]igital platforms' consumer-facing terms of use and privacy policies would likely be considered standard form contracts, which would mean that they must comply with the unfair contract term provisions in the *ACL*'.[251] Although this statement is probably correct for the *major* digital platforms such as Google and Facebook, it is not so for all of those engaging in digital data practices.

It will usually be uncontroversial that terms of use and privacy policies will be *standard form* as no negotiation is possible. However, their status as *contracts* will vary from platform to platform, for two reasons. First, not all terms of use will fulfil the requirements for formation of a legally binding contract, or incorporation as terms in such a contract. This is a particular risk in the case of 'browsewrap'-style terms,[252] where the supplier does not take reasonable

[251] ACCC (n 1), 437.
[252] These are terms that are provided by hyperlink only but no active assent (such as clicking an 'I agree' button) is required. See Kayleen Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the U.S. and the U.K' (2011) 5(1) *Studies in Ethics, Law, and Technology* Article 4.

steps to give the consumer notice of those terms.[253] Second, even where terms of use were proffered in a way that would constitute a contract, stand-alone privacy policies or separate privacy representations may not (by accident or design), be legally *incorporated*[254] into those terms or any other contract entered into between the supplier and the consumer.[255]

If the privacy policy does *not* form part of a contract, then the UCTL will not apply to the terms of the policy. Of course, the consumer will also not be *contractually* bound by other terms in the policy. This could be problematic for the provider, if the data practices they are engaging in require consent. For example, if the business wishes to use or disclose the information for a secondary purpose, this use or disclosure generally requires consent under APP 6. If a consumer can successfully argue that the consumer did not contractually accept the privacy policy, then the business must prove some other means of consent.

2.11.3.3 Consequences of the inclusion of unfair terms

Even in cases where privacy policies or representations are contractual in nature, other issues arise. Unfair contract terms are not *currently* illegal, merely void, which means they cannot be enforced. The rest of the terms of the contract can be enforced unless the omitted term makes the whole contract uncertain.[256]

The consequence that an unfair term is **void** may aid consumers where the term in question imposes some obligation on the consumer, that is, when it requires the consumer to do something. In such cases, the fact that the term is void means that the consumer has grounds for declining to fulfil that obligation. However, rarely do privacy policies impose significant obligations on consumers that would require enforcement by the service provider. Also, it is of little use where there is a zero monetary price, like many digital platforms' terms of use and privacy policies. Here, the impact of declaring a term void is unlikely to have immediate impacts on the parties' financial rights and obligations.[257]

The consequence that the unfair term is void may be less useful when that term provides a firm with permission to do something. In the case of privacy terms, an unfair 'term may permit overbroad collection or use of the consumer's personal information secured under the original privacy terms, or under terms which have been unilaterally varied by the firm'.[258] In this case, the consumer would most likely need to bring proceedings to obtain a declaration that the term is unfair and seek an injunction to restrain the firm from relying on that term in future. However, there is no realistic prospect of reversing the data practices of the firm in unfairly collecting, using and disclosing the consumer's information up to that point. In these circumstances, the current remedies are likely to supply negligible recourse for a consumer affected by unfair privacy terms.

2.12 Conclusion

Significant empirical evidence demonstrates that consumers have real concerns about privacy of their information that cannot easily be addressed by individuals, and expect the

---

[253] Ibid.
[254] See ibid for a discussion of incorporation of online terms.
[255] Norton, Thomas B., 'The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model' (2016) 27(1) *Fordham Intellectual Property, Media and Entertainment Law Journal* 181, 189-195. This sets out the US position. However, the Australian contractual position is likely to be the same in this context. Norton also usefully outlines the practice of websites where they deliberately design their policies not to have contractual effect.
[256] *ACL* s 23(2).
[257] ACCC (n 1), 497-8.
[258]Katharine Kemp and Rob Nicholls, *Submission on the Digital Platforms Inquiry: Preliminary Report* (The Allens Hub for Technology, Law & Innovation, 1 March 2019) https://www.accc.gov.au/system/files/Katharine%20Kemp%20%26%20Rob%20Nicholls%20%28March%202019%29.pdf, 8.

law to have a role in protecting them against misuse of their information. However, the analysis above indicates that:

(1) there is a significant disconnection between actual digital data practices by businesses and the expectations of consumers; and
(2) the existing Australian legislative framework for the collection, sharing and use of consumer data is currently ill-equipped to deal with this disconnection.

In particular, there are problems with the existing 'consent' requirements contained in the *Privacy Act* which override several safeguards for consumers in relation to the use of consumer data, and its transfer to third parties.

In our view, the notion of consent in the *Privacy Act* is inadequate to protect consumers from the potential misuse of their information. Commercial entities can and often do deal with consumer data in a wide-ranging and ultimately non-transparent way even though in most cases the consumer consent obtained is not informed, is non-negotiable, and is subject to unilateral interpretation and extension at the will of the commercial party.[259] In particular, the use of standard form contracts increases information asymmetries and power imbalances between the consumer and service provider, preventing consumers from providing informed consent. Consumer privacy expectations are not met by existing legislation. Therefore, proper regulation of data collection, use and disclosure terms is needed to protect consumers from the mishandling of their data.

Given the inadequacies of the *Privacy Act*, the *ACL* has the potential to provide a more fertile area to protect consumers against the problems of a lack of true informed consent. However, there are also serious uncertainties and limitations in this area that need to be addressed to allow appropriate consumer expectations to be addressed in ways that do not unduly hamper businesses in their legitimate activities.

[259] Ibid; ACCC (n 1) 177.

KATHARINE KEMP

3. Chapter 3 – Regulatory Landscape

3.1 Introduction

The extent to which individuals' privacy is protected under Australian law is not only a function of the obligations imposed on entities dealing with personal information, but of the regulatory framework within which those laws are applied and enforced. What powers and resources have been provided to the Office of the Australian Information Commissioner (OAIC) and the Australian Competition & Consumer Commission (ACCC) to enforce the relevant laws? What are the consequences if an entity does not provide adequate notice or obtain adequate consent for its personal data practices, or otherwise interferes with an individual's privacy? What rights does an individual have to seek a remedy from a regulator or court, and are those remedies adequate to compensate injured parties and deter wrongdoing?

The regulatory regime provided by the *Privacy Act 1988* (Cth) ('*Privacy Act*') has long been criticised for its relative ineffectuality in providing both remedies for individuals and guidance and deterrence for entities obliged to comply with the statute.[1] There is substantial consensus that the funding currently allocated to the OAIC is insufficient to permit the regulator to actively and effectively enforce the *Privacy Act*.[2] The OAIC's actual enforcement activities have been relatively limited, at times negligible,[3] although it has been more active in its advice and advocacy roles in recent times, and last year brought proceedings seeking a civil penalty for the first time.[4]

The ACCC is a regulator that enjoys the benefits of greater resources and a reputation as an active regulator.[5] In the last two years, the ACCC has begun to take on an important role in advocating for reform of Australia's privacy law and in litigating privacy-related matters under the *Australian Consumer Law*.[6] However, as explained in this chapter, substantial law reform, and changes to the resourcing and activity of the OAIC, will be required before Australians have appropriate access to justice in redressing privacy wrongs.

3.2 Office of the Australian Information Commissioner

The Australian Information Commissioner (Commissioner) is responsible for monitoring and enforcing compliance with the *Privacy Act*. The enforcement regime under the *Privacy Act* has been described as adopting an 'escalation model', or an 'enforcement pyramid approach', to regulation, in which the regulator initially uses less interventionist measures to encourage compliance in any given case, 'with more severe sanctions generally held in reserve as a threat'.[7] Under the *Privacy Act*, preference is clearly given to conciliation of complaints by the Commissioner, with formal determinations by the Commissioner and proceedings in the Federal Court as (rare) exceptions to the general rule. As will be explained in the following sections, significant discretion is reserved to the Commissioner essentially as the 'gatekeeper' who determines whether a case will be heard, whether any

---

[1] See, eg, Australian Privacy Foundation, *Bringing Australian's Privacy Act up to international standards: Submission in response to Privacy Act Review – Issues Paper* (18 December 2020).
[2] See 3.2.6 below.
[3] See 3.2.2 and 3.2.4 below.
[4] See 3.2.4 below.
[5] See 3.3 below.
[6] See 3.3 below.
[7] Attorney-General's Department, Australian Government, *Privacy Act Review: Issues Paper* (October 2020) 65; OAIC Submission 120; Angelene Falk, *Submission by the Office of the Australian Information Commissioner: Privacy Act Review Issues Paper* (11 December 2020).

remedy will be provided and/or whether there will be an award of compensation enforceable in a court of law. While this framework has the advantage of reducing the potential burden of privacy complaints on the court system, there is a growing consensus that it creates excessive obstacles to justice and deterrence.

In February 2018, the Commissioner's role was expanded to include responsibility for the mandatory data breach notification scheme. This scheme imposes an obligation upon government agencies and businesses covered by the *Privacy Act* to notify individuals whose personal information is involved in a data breach that is likely to result in 'serious harm' to the individual to whom the information relates, as well as report to the OAIC.[8] One of the key underlying rationales of the scheme was to 'reinforc[e] organisations' accountability for personal information protection and encourage[e] a higher standard of personal information security across the public and private sectors'.[9]

3.2.1 OAIC complaints and investigations

The recourse available to an individual affected by a contravention of the *Privacy Act* is currently very limited. Under the *Privacy Act*, an individual has no right to apply directly to any court or tribunal for compensation for an interference with their privacy. This has not only limited individuals' access to justice, and placed pressure on the OAIC's limited resources,[10] but ensured that there is no substantial body of case law to provide guidance on the interpretation of the *Privacy Act*.

Rather than applying to a court to seek compensation, the individual must first approach the entity it suspects of a contravention and allow the entity an adequate opportunity to resolve the matter.[11] If the matter remains unresolved, the individual may only make a complaint to the Commissioner.[12] The Office of the Australian Information Commissioner (OAIC) received 2,673 such complaints in 2019-2020.[13]

At the outset, the Commissioner is required to make a reasonable attempt to conciliate the complaint if the Commissioner considers it is reasonably possible that the complaint may be conciliated successfully.[14] Even before the Commissioner attempts any conciliation, the OAIC has an 'early resolution' approach to complaints received, with the majority of complaints resolved at this stage, largely it seems on the basis that the Commissioner lacks jurisdiction.[15] At the conciliation stage, the main remedies agreed in 2019-2020 included:

- compensation;
- record amended;
- apology;
- access provided;
- changed procedures; and
- staff training or counselling.[16]

---

[8] See the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth); *Privacy Act* 1988 (Cth) ss 26WE, 26WG, 26WK, 26WL.
[9] Office of the Australian Information Commissioner, 'Mandatory data breach notification comes into force this Thursday' (Media Release, 19 February 2018).
[10] See section 3.2.6 below.
[11] *Privacy Act*, ss 40(1A), 41 (2)(b).
[12] *Privacy Act*, s 36.
[13] OAIC, *Annual Report 2019-2020* (Report, 21 September 2020) 13 ('Annual Report').
[14] *Privacy Act*, s 40A(1).
[15] OAIC, Annual Report 36.
[16] Ibid 135.

Compensation amounts have not been substantial. Most of the compensation amounts in closed privacy complaints in that year were under AUD 10,000, with the median compensation amount between AUD 1,000 and AUD 5,000.[17]

If the complaint cannot be conciliated, the Commissioner will decide whether to investigate the complaint. The OAIC can conduct preliminary enquiries to make this decision.[18] The Commissioner may refuse to investigate the complaint on numerous grounds, including where the complaint is not brought within 12 months, no interference with privacy is found, or an investigation is not warranted in the circumstances.[19]

The Commissioner may also investigate potential contraventions of the *Privacy Act* on his or her own initiative, in the absence of any complaint by an individual or group of individuals.[20] The OAIC has indicated that such investigations are initiated 'to examine serious or systemic issues and evaluate compliance with the requirements of the scheme and the *Privacy Act*'.[21]

In the course of an investigation, the Commissioner has certain ancillary powers to obtain information and documents, and to examine witnesses.[22] However, the *Privacy Act* does not expressly provide the Commissioner with the power to make copies of relevant documents (as opposed to merely inspecting them) where it is authorised to enter premises. Nor does it expressly empower the Commissioner to seek a warrant to preserve or secure relevant documents or make it an offence to destroy documents reasonably required by the Commissioner.[23] The lack of such powers may seriously hinder the OAIC's enforcement of the *Privacy Act*. The OAIC cites the example of an investigation which was impeded when the relevant data was held by a small business sub-contractor of the relevant entity, and in the course of the investigation, the sub-contractor began deleting the relevant information.[24]

3.2.2 OAIC section 52 determinations

If the Commissioner proceeds to investigate a complaint where conciliation is not reasonably possible, the Commissioner may ultimately make a determination under section 52 of the *Privacy Act*, dismissing the complaint or finding the complaint substantiated.[25] Importantly, however, the Commissioner is not obliged to make any formal determination where a complaint cannot be resolved by conciliation.[26] This has several negative consequences.

First, in the absence of such an obligation, the Commissioner has made **very few determinations** under section 52, vastly reducing the potential for such determinations to provide entities with guidance as to how the Commissioner interprets the *Privacy Act*, limiting the deterrent effect of the Commissioner's power to make determinations, and raising serious doubt about the extent to which individuals have been able to access justice under the *Privacy Act*. The Commissioner has only published 48 determinations under

[17] Ibid.
[18] *Privacy Act*, s 42.
[19] *Privacy Act*, s 41.
[20] *Privacy Act*, s 40(2).
[21] OAIC Annual Report (n 13) 9.
[22] *Privacy Act*, s 44, 45, 66.
[23] Falk (n 7) 128.
[24] Ibid 128-129.
[25] An interested party may request that the Commissioner hold a hearing before making any determination under section 52 in respect of the investigation: *Privacy Act*, s 43A.
[26] Attorney-General's Department, Australian Government, '*Privacy Act* Review: Issues Paper' (October 2020) 65.

section 52 in approximately 10 years.[27] This represents only a fraction of one percent of the complaints made to the OAIC in this period.[28]

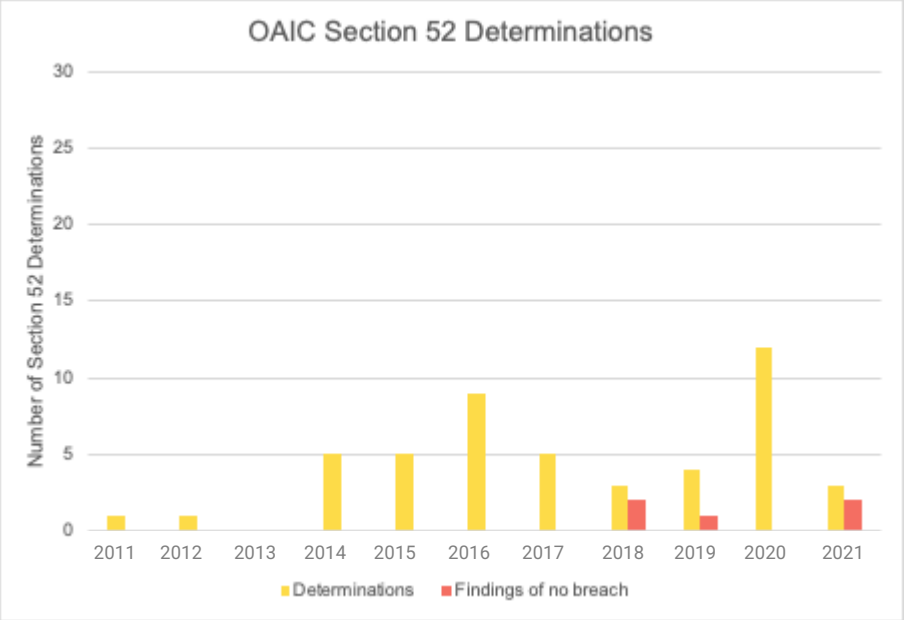
Second, the Commissioner appears to have adopted a **practice of informally dismissing complaints** rather than dismissing complaints via a formal determination under section 52. This too reduces individuals' recourse under the *Privacy Act*. While an individual can seek review of the Commissioner's decision to formally dismiss a complaint under section 52,[29] he or she has no recourse when the Commissioner declines to make any formal determination. Practitioners have complained that the OAIC has taken this course with complaints that practitioners believed to have merit (and wider significance).[30] Of the 48 determinations published in the last decade, there have been only five formal findings of no breach.[31]

Third, an individual's ability to seek compensation under the *Privacy Act* is limited to the mechanism provided by section 52: he or she has **no direct right to seek compensation in a court** of law. If the respondent ultimately fails to comply with a determination by the Commissioner under section 52, the Commissioner or the complainant may bring proceedings in the Federal Court for an order enforcing the Commissioner's determination.[32] However, this avenue is only available if the Commissioner first makes a determination under section 52 in respect of a complaint received (or in respect of an investigation commenced on its own initiative). It is also possible to seek administrative review or judicial review of a determination under section 52. But if the Commissioner refuses to investigate the complaint or refuses to make any formal determination following its investigation, the individual has no means of litigating to seek compensation from the respondent.

As explained later in this chapter, the statutory framework for OAIC determinations requires reform to overcome these deficiencies and ensure transparency, accountability and access to justice.

Figure 3.1: Annual numbers of OAIC determinations under s 52 *Privacy Act*

[27] OAIC, 'Privacy Determinations' (OAIC website) https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations/.
[28] Annelies Moens, 'Submission – Consultation on the Privacy Review Act for Attorney-General's Department' (27 November 2020) 4.
[29] *Privacy Act*, s 96(1)(c).
[30] Salinger Privacy, *Submission in Response to the Privacy Act Review Issues Paper* (20 November 2020) 36.
[31] OAIC, 'Privacy Determinations' (n 27).
[32] *Privacy Act*, s 55A(1). This is the only stage at which proceedings may be brought in a court to obtain a remedy (other than an injunction) for an individual or group of individuals. Commentators also point out that individuals are exposed to 'extensive costs' if they appeal against a determination by the Commissioner, given that only the Federal Court has jurisdiction to hear such appeals: Salinger Privacy (n 30) 36.



Source: OAIC, 'Privacy Determinations' (OAIC website) https://www.oaic.gov.au/privacy/privacy-decisions/privacy-determinations/ Note that determinations for 2021 are only current to 31 March 2021.

Compensation is not the only remedy the Commissioner can grant under section 52. If the Commissioner determines that the complaint has been substantiated, the Commissioner can make various declarations, including a declaration that the respondent entity must take specified steps within a specified period to ensure that the conduct is not repeated or continued and/or that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant.[33] The *Privacy Act* does not expressly give the Commissioner the power to order an entity to delete personal information where the Commissioner finds the entity has collected that information inappropriately.[34] Arguably, such an order would come within the specific power to make 'a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant', but it would be appropriate to make the power to order deletion clear in the statute, lest a court interpret 'loss or damage suffered' overly narrowly to exclude the 'mere' storage of improperly collected personal information.

The OAIC has pointed out that '[i]n addition to providing outcomes for the particular complainants … more recent determinations provide insight into how [certain APPs] apply to particular factual circumstances, as well as deterring APP entities from breaching the *Privacy Act*'.[35] The recent determination by the Commissioner in *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 is a welcome example of such a determination in the context of consent.[36] While such determinations provide insights into the OAIC's views on the proper interpretation of the *Privacy Act*, these will not bind any court that subsequently interprets the APPs.

The Commissioner's formal determination under section 52, including any award of compensation, is not binding or conclusive.[37] This is in some contrast to other jurisdictions where privacy regulators are empowered to issue capped pecuniary penalties, which can

[33] *Privacy Act*, ss 52(1)(b)(ia), (iii); 52(1)(b)(ii).
[34] Falk (n 7) 127.
[35] OAIC, Annual Report (n 13) 36.
[36] See Chap 2.6.
[37] *Privacy Act*, s 52(1B); *Day v Lynn* [2003] FCA 879 [50].

create greater deterrent effect without using the regulators limited resources to litigate (as currently required in Australia). The possibility of infringement notices, backed by penalties, is discussed further below.[38]

If the respondent fails to comply with the determination, the Commissioner or the complainant may bring proceedings in the Federal Court for an order enforcing the Commissioner's determination.[39] However, as noted, this avenue is only available if the Commissioner first makes a determination under section 52 in respect of a complaint received (or in respect of an investigation commenced on its own initiative). If the Commissioner refuses to investigate the complaint or refuses to make any formal determination following its investigation, the individual has no means of seeking compensation from the respondent in a court of law. On the other hand, if the Commissioner decides to make a determination under section 52, an application made be made to the Administrative Appeals Tribunal (AAT) for review of the Commissioner's decision.[40] Both the original decision by the Commissioner and the decision on the review by the AAT may be subject to judicial review.

3.2.3 OAIC other remedies

The Commissioner may seek an injunction in the Federal Court or the Federal Circuit Court.[41] An injunctive remedy can also be sought by an individual,[42] but the individual cannot seek compensation in such a proceeding.

The OAIC is able to accept enforceable undertakings.[43] Since 2015, the OAIC has published 10 enforceable undertakings.[44] Not all of these are linked with investigations. Undertakings are often provided in response to either a voluntary notification from the relevant entity or a third party about a data breach,[45] or the OAIC separately raising concerns about a particular privacy incident or practice with an entity.[46[

Unlike the ACCC,[47] however, the OAIC has no power to issue an infringement notice where it has reasonable grounds to believe that an entity has contravened certain provisions of the *Privacy Act* in cases where there is less risk of significant harm but still a need for a formal response. The government recently announced it intends to amend the law to provide the OAIC with the power to issue infringement notices, with "penalties of up to $63,000 for bodies corporate and $12,600 for individuals for failure to cooperate with efforts to resolve

---

[38] See section 3.2.3 below.
[39] *Privacy Act*, s 55A(1). Commentators also point out that individuals are exposed to 'extensive costs' if they appeal against a determination by the Commissioner, given that only the Federal Court has jurisdiction to hear such appeals: Salinger Privacy (n 30) 36.
[40] *Privacy Act*, s 96.
[41] *Privacy Act*, ss 80V, 80W.
[42] *Privacy Act*, s 80W.
[43] *Privacy Act*, s 33.
[44] See OAIC, 'Enforceable Undertakings' (Web Page, 2019) https://www.oaic.gov.au/privacy/privacy-decisions/enforceable-undertakings/?start=0.
[45] See, eg, Australian Recoveries & Collections Pty Ltd, '*Privacy Act 1988* (Cth) Undertaking to the Australian Information Commissioner under section 114 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)' (Enforceable Undertaking, 31 August 2016) cll 2.4-2.10.
[46] See, eg Wilson Asset Management, '*Privacy Act 1988* (Cth) Undertaking to the Australian Information Commissioner under section 114 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)' (Enforceable Undertaking, 28 June 2019) cll 1-7; Organica Skin Clinic Pty Ltd (trading as Organica Cosmetic and Laser Clinic) and Brygon MC Pty Ltd (trading as Brygon Medical Centre), '*Privacy Act 1988* (Cth) Undertaking to the Australian Information Commissioner under section 114 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)' (Enforceable Undertaking, 16 May 2016), cll 2.3.1-2.3.2.
[47] See 3.3.4.1 below.

minor breaches".[48] Providing the OAIC with such a power would be a valuable step in permitting the regulator to make the most efficient use of its enforcement resources while maintaining the ability to deter breaches of this nature.

3.2.4 OAIC pecuniary penalties

The Commissioner is empowered to bring proceedings in the Federal Court seeking a civil pecuniary penalty against an entity for contravention of a civil penalty provision of the *Privacy Act*.[49] The maximum civil penalty which may be imposed under the *Privacy Act* is currently AUD 2.1 million for a body corporate.[50] By contrast, the Consumer Data Right regime provides for maximum pecuniary penalties of AUD 10 million, 10 percent of annual turnover or three times the benefit obtained from the breach, whichever is greater, where an entity breaches a Privacy Safeguard.[51]

However, the government has announced its intention to amend the *Privacy Act* to increase the maximum penalties to AUD 10 million, 10 percent of domestic turnover or three times the benefit obtained from the misuse of information, whichever is greater,[52] which would bring penalties into line with the maximum penalties available under both the Consumer Data Right regime and the *Australian Consumer Law*.

An entity may be liable for a civil penalty under the *Privacy Act* if it:

- engages in an act or practice that is a serious interference with the privacy of an individual; or
- repeatedly engages in an act or practice that is an interference with the privacy of one or more individuals.[53]

Accordingly, the OAIC has noted that the Commissioner is only empowered to seek a civil penalty for 'the most egregious conduct', rather than treating the serious or repeated nature of an interference with privacy as an aggravating factor.[54] No application for a civil penalty made be brought for an interference with privacy which does not meet this high threshold.

While the Commissioner has had the power to bring such proceedings since section 13G was inserted in the *Privacy Act* in 2012, the OAIC has only brought one such proceeding in eight years, namely the case launched against Facebook in March 2020, alleging that the social media platform committed serious and/or repeated interferences with privacy in contravention of the *Privacy Act*.[55] At the time of writing, this litigation is still in train, so there remains no precedent concerning the severity of pecuniary penalties which might be imposed for contraventions of the civil penalty provisions.

3.2.5 OAIC guidance

The OAIC also has the power to publish guidelines regarding its interpretation of the *Privacy Act* and how entities should conduct themselves to comply with the *Privacy Act*.[56] These

---

[48] Attorney-General's Department, 'Tougher Penalties to Keep Australians Safe Online' (Media Release, 24 March 2019) https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019.
[49] *Privacy Act*, ss 80U(1)-(2), 80U(3).
[50] *Privacy Act*, s 13G – 2,000 penalty units.
[51] See further Chap 6.2.3.
[52] Attorney-General's Department (n 48).
[53] *Privacy Act*, s 13G. 'Interference with the privacy of an individual' occurs if an entity or agency breaches an Australian Privacy Principle in respect of personal information or an individual: s 13(1)(a).
[54] Falk (n 7) 125.
[55] See OAIC, 'Commissioner launches Federal Court action against Facebook' (9 March 2020) https://www.oaic.gov.au/updates/news-and-media/commissioner-launches-federal-court-action-against-facebook .
[56] *Privacy Act*, s 28.

guidelines are not binding on APP entities or the courts. As discussed in chapter 2, the OAIC has published guidelines concerning appropriate 'notice' and 'consent' in the 'Australian Privacy Principles Guidelines'.[57] These guidelines are discussed further in chapter 5, which explains that the OAIC guidelines on consent generally align with the standards for consent under the European Union General Data Protection Regulation.[58] That chapter also provides numerous examples of entities – including data brokers and ad tech suppliers – not complying with the OAIC guidelines on consent, which is likely to be a function of the non-binding nature of the guidelines, the limited penalties, remedies and recourse described in this chapter, and the absence of specific legislative obligations to requiring appropriate standards of consent. Recommended legislative clarifications on the standards for notice and consent are outlined in chapter 5. If such reforms are to be effective, however, the regulatory framework must also be updated to ensure appropriate remedies and levels of deterrence.

3.2.6 OAIC funding and resources

Commentators have criticised the federal government for failing to allocate adequate resources to the OAIC.[59] In 2019-20, the OAIC received revenue from government of approximately AUD 21 million to fulfil *both* its privacy and freedom of information roles, which in fact represented a substantial increase over previous years.[60] In March 2019, the federal government committed to providing AUD 25 million in additional funding over three years to the OAIC "to give it the resources it needs to investigate and respond to breaches of individuals' privacy and oversee the online privacy rules".[61] In contrast, the government has so far provided funding of well over AUD 100 million over five years for the implementation of the Consumer Data Right, with the central goal of encouraging consumers to share and make use of their personal data to negotiate for better prices and services in certain sectors.[62] Protecting Australians from the long-term harms and disempowerment that can result from improper collection and use of their personal information is, if anything, more critical than the promotion of possible consumer benefits through data portability.

The OAIC should be provided with adequate staff and resources, including enforcement and investigative tools, to fulfil its roles under the *Privacy Act*, including by bringing more risky test cases and meeting the growing challenges of personal data practices in the digital era. The effects of the underfunding of the OAIC are exacerbated by the fact that all complaints in respect of interferences with privacy under the *Privacy Act* must be made to the OAIC. Practitioners argue that this has led to delays over several years in the resolution of some complaints, particularly in representative proceedings, where courts would be better equipped to deal with the matters directly.[63]

---

[57] See Chap 2.7.3.
[58] See Chap 5.5.
[59] See, eg, Australian Privacy Foundation, *Bringing Australia's Privacy Act up to International Standards: Submission in Response to the Privacy Act Review Issues Paper* (18 December 2020) 7; Peter Leonard, *Submission of Data Synergies in Response to Privacy Act Review: Issues Paper* (December 2020).
[60] OAIC, Annual Report (n 13) 91.
[61] Attorney-General's Department, 'Tougher Penalties to Keep Australians Safe Online' (24 March 2019) https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019.
[62] The government committed over AUD 90 million to the implementation of the CDR in the 2018-19 Budget and 2018-19 MYEFO for the five years from 2018-19 to 2022-23: The Treasury, Australian Government, 'Consumer Data Right: Overview' (September 2019) 6. The government subsequently announced funding of a further AUD 19.2 million over 12 months in July 2020: The Treasurer, 'Economic and Fiscal Update: July 2020' (23 July 2020) https://budget.gov.au/2020-efu/economic-fiscal-update.htm.
[63] Maurice Blackburn, 'Submission in Response to the Issues Paper for the Review of the *Privacy Act* 1988' (December 2020) 8-10. See also Annelies Moens, 'Submission – Consultation on the Privacy Review Act for Attorney-General's Department' (27 November 2020) 4.

The OAIC itself has expressed the view that the 'escalation model' reflected in the *Privacy Act* is no longer an efficient model for the protection of privacy in Australia and argued for a more 'risk-based approach to regulation' under which the statute would 'provide a flexible tool kit of regulatory options, supported by appropriate powers and enforcement processes'. The OAIC considers that it could then 'take the most proportionate and effective action in the circumstances'.[64]

3.3 Australian Competition & Consumer Commission

3.3.1 ACCC – formal inquiries, recommendations and advocacy

The Australian Competition & Consumer Commission (ACCC) has also more recently begun to play a significant role in attempting to address deficiencies in the notice and consent mechanisms of entities which collect personal information from Australian consumers. The ACCC's work in this area has taken the form of recommendations to government following formal inquiries,[65] advocacy, enforcement of the *Australian Consumer Law* ('*ACL*') and joint supervision (for a period) of the recently legislated Consumer Data Right.[66] One of the ACCC's stated priorities for 2019 was: '[t]he impact on consumers arising from the collection and use of consumer data by digital platforms, with a focus on the transparency of data practices and the adequacy of disclosure to consumers.' Numerous inquiries, initiatives and investigations were launched as a result of the ACCC's recognition of this priority, with ongoing results in subsequent years.

Most significantly, in 2019, the ACCC published the Final Report of the Digital Platforms Inquiry ('DPI Report'). The DPI Report included serious criticisms of common practices of digital platforms in purportedly notifying consumers of their data practices and/or obtaining consent for uses of consumers' personal information, including vague and broad wording, reference to multiple documents or webpages, defaults to less privacy and 'bundled' consents.[67] The ACCC concluded that the manner in which many digital platforms currently seek consent from consumers:

> leverages bargaining power imbalances between digital platforms and consumers and deepens information asymmetries between them. They have the effect of preventing consumers from providing meaningful consent to the collection and use of their personal information and user data.[68]

The DPI Report made numerous recommendations for wide-ranging reform to Australia's privacy and data protection laws which aimed to address the imbalances in bargaining power and information asymmetries which exist between individual consumers and the entity they deal with. In addition to recommendations that the maximum civil penalties under the *Privacy Act* be increased, recommendations included:

- updating the definition of 'personal information' to capture technical data and other online identifiers;[69]
- strengthening existing notification requirements;[70]
- strengthening consent requirements and requiring pro-consumer defaults;[71]

---

[64] Falk (n 7) 120, 123.
[65] Including the ongoing Digital Platform Services Inquiry 2020-2025: Treasurer (Cth), *Competition and Consumer (Price Inquiry – Digital Platforms) Direction 2020* (10 February 2020).
[66] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth); Australian Competition and Consumer Commission, 'Consumer Data Right Rules made by ACCC' (Media Release, 5 February 2020).
[67] ACCC, 'Digital Platforms Inquiry: Final Report' (June 2019) chap 7.
[68] Ibid 400.
[69] Ibid, Recommendation 16(a).
[70] Ibid, Recommendation 16(b).
[71] Ibid, Recommendation 16(c).

- introducing a direct right of action to enforce privacy obligations under the *Privacy Act*;[72]
- introducing a right to erasure under the *Privacy Act*;[73] and
- introducing a statutory tort for serious invasion of privacy.[74]

Of these recommendations, the federal government has supported the first four recommendations 'in principle' and 'subject to consultation'. These and the last two bulleted recommendations above will be considered as part of the *Privacy Act* Review in 2021.

The ACCC has been vocal in its advocacy for better standards of consent through the Digital Platforms Inquiry and subsequent related inquiries, reviews and proceedings,[75] as well as in the consultation leading to the framing of the Consumer Data Rules in the context of the Consumer Data Right.

3.3.2 ACCC funding and resources

In contrast to the OAIC, the ACCC is a well-resourced regulator with powers and responsibilities in an extraordinarily broad range of fields, including *ACL* enforcement and education. It has also developed a reputation for its active enforcement. In 2019-2020, the ACCC concluded 66 in-depth *ACL* investigations;[76] commenced 10 *ACL* court cases;[77] and secured total penalties of $198.2 million from litigated consumer protection matters.[78] In the same period, the OAIC commenced one court case and secured no penalties from litigated privacy matters. The OAIC's annual reporting does not reveal how many complaints it investigated in this period.

The ACCC has also shown far greater willingness to test the law through litigation. ACCC Chair Rod Sims has been vocal about his view of the regulator's obligation to take on risky cases to this end. In his first major speech as Chair, Sims stated:[79]

> The ACCC's success rate in first instance litigation stands at almost 100%. This is frankly too high. It may sound strange to say so, but benchmarking against our international counterparts we are sitting at a much higher level of success. Of course I'm happy with the implication that ACCC staff handle cases well, but the flip side is that we have been too risk-averse. We need to take on more cases where we see the wrong but court success is less assured.

The government in turn has made provision for the ACCC to take such risks in the cases it litigates. Beyond its litigation budget, the ACCC is allowed to incur an operating loss as a result of excess litigation costs since the ACCC Litigation Contingency Fund is applied to these costs, and the Fund 'is periodically replenished by government through equity injections to ensure sufficient funds are available'.[80]

---

[72] Ibid, Recommendation 16(e).
[73] Ibid, Recommendation16(d).
[74] Ibid, Recommendation 19.
[75] See, eg, ACCC, 'Customer Loyalty Schemes: Final Report' (December 2019). See further Rod Sims, '2019 Compliance and Enforcement Policy' (Speech, Committee for Economic Development Australia, 26 February 2019).
[76] Down from its previous three-year average of 84 in-dept investigations per year: *ACCC and AER Annual Report 2019-20* (2020) 75.
[77] Ibid 288.
[78] Ibid 12.
[79] Rod Sims, 'ACCC: Future Directions', Speech delivered at Law Council Competition and Consumer Workshop 2011 (28 August 2011). See further Rod Sims, 'Address to the Law Council of Australia Competition Law Workshop 2019', Speech delivered at Law Council of Australia - Competition Law Workshop 2019 (30 August 2019): "We have also not shied away from the more complex cases with less clear-cut outcomes."
[80] ACCC and AER Annual Report 2019-20 (2020) 19.

3.3.3 ACCC investigative powers

The *Competition and Consumer Act 2020* (Cth) ('*CCA*') gives the ACCC extensive investigative powers to allow the Commission to carry out its enforcement role. The ACCC is empowered to require, by written notice, that a person provide it with information, produce documents or give evidence where it has 'reason to believe' that person 'is capable of furnishing information, producing documents or giving evidence relating to a matter that constitutes or may constitute a contravention'.[81] Its inspectors also have the power to enter premises to search for evidence.[82] Importantly, this includes powers for the inspector to make copies of documents, access equipment and remove things found on the premises for further examination, powers not currently granted to the Commissioner under the *Privacy Act*.

3.3.4 *Australian Consumer Law*

3.3.4.1 Remedies under the *ACL*

Private enforcement

In contrast to the position under the *Privacy Act*, under the *ACL*, consumers may apply directly to a court for damages[83] or a compensation order[84] in respect of contraventions of the *ACL*, including, for example, contraventions of the prohibitions against misleading or deceptive conduct, or misleading conduct in respect of the nature and characteristics of services,[85] where the entity's representations about its data practices are likely to mislead.[86] A compensation order may be made even where the complainant is *likely* to suffer loss or damage because of the conduct, and not only where the complainant has actually suffered such loss or damage.

A consumer may also apply for a declaration that a term of a consumer contract is unfair and therefore void.[87] This may become relevant in the present context if a term in respect of an entity's data practices is incorporated in a consumer contract (for example, in its terms of use or a privacy policy that amounts to part of a contract) and the term meets the definition of 'unfairness' under the *ACL*.[88] Although the term is automatically void under the *ACL* if it meets these requirements,[89] if the court also makes a declaration that the term is unfair, a consumer may apply for a compensation order if the entity subsequently purports to apply or rely on the term that has been declared void.[90]

Any person may apply for an injunction where an entity is engaging in, or proposing to engage in, conduct that would contravene certain provisions of the *ACL*, including the prohibitions against various false or misleading representations.[91] This right is not restricted to consumers who have suffered damaged, or are likely to suffer damage, because of the contravening conduct. The court has a discretion whether to grant such an injunction, and may also grant interim injunctions where the court considers it desirable to do so.[92]

---

[81] *CCA*, s 155.
[82] *CCA*, Pt XID.
[83] *ACL*, s 236.
[84] *ACL*, s 237.
[85] *ACL*, ss 18, 34. See further chap 2.11.1.
[86] *ACL*, ss 236, 237.
[87] *ACL*, s 250. See further chap 2.11.3.
[88] *ACL*, s 24.
[89] *ACL*, s 23(1).
[90] *ACL*, s 237(1)(a)(ii).
[91] *ACL*, s 232(1)-(2).
[92] *ACL*, s 234(1).

Public enforcement

In contrast to the 'escalation model' under the *Privacy Act*, under the *ACL*, the ACCC[93] is empowered to adopt a wide range of enforcement strategies from administrative resolutions to litigation (including applications for significant civil pecuniary penalties), as proportionate to the potential risk of consumer detriment resulting from the conduct.[94] That is, the ACCC is not required to first attempt conciliation or other 'milder' measures in every case.

The ACCC may seek **pecuniary penalties** for contraventions of the *ACL*, including contraventions of the prohibitions against false representations and unconscionable conduct.[95] This is not restricted to cases of serious or repeated contraventions. However, pecuniary penalties cannot be sought for misleading or deceptive conduct under section 18, bearing in mind that such conduct may contravene even in the case of unintentional misrepresentations. The maximum penalty for a body corporate is the greater of AUD 10 million, 10 percent of domestic turnover, or three times the benefit obtained from the breach.

The ACCC may seek **injunctions**,[96] as well as **compensation orders** on behalf of one or more persons injured as a result of an entity contravening certain provisions of the *ACL*, if that person(s) has consented in writing.[97] The ACCC may also seek orders to redress or prevent actual or likely loss or damage suffered in relation to the contravening conduct by consumers who are *not parties* to the proceedings.[98] Such **non-party redress** can also be sought in respect of unfair contract terms which a court has previously declared void.[99]

On the application of the ACCC, court may also make **non-punitive orders** under section 246 of the *ACL*, for example, requiring the respondent to:

- publish an advertisement;
- provide affected consumers with information about the relevant conduct;
- provide a service to the community or a section of the community; and / or
- establish compliance, education or training programs.

Where there is less risk of significant consumer detriment from the relevant conduct but still a need for a formal response, the ACCC may decide to issue an **infringement notice** where it has 'reasonable grounds to believe that a person has contravened an infringement notice provision'.[100] This procedure is an alternative to proceedings seeking a civil pecuniary penalty.[101] Infringement notices can be issued, for example, in respect of alleged contraventions of the prohibition of specific claims or statements that may be false or misleading under section 29 of the *ACL*.

The issue of an infringement notice does not amount to a finding that the entity has contravened the relevant provision or the imposition of a financial penalty, since, as a matter of constitutional law, the ACCC would be prohibited from making such a finding or imposing such a fine. However, it allows the ACCC to allege that such a contravention has occurred and the entity to elect to pay the penalty specified in the infringement notice, failing which the ACCC may commence proceedings for the imposition of a civil penalty. This procedure

---

[93] While enforcement of the *ACL* is shared between various Commonwealth, state and territory agencies, this chapter will focus on the ACCC's role as the most significant regulator enforcing this law.
[94] See SG Corones, *The Australian Consumer Law* (Thomson Reuters, 3rd ed, 2016) 540-541.
[95] *ACL*, s 224(1).
[96] *ACL*, s 232, 234.
[97] *ACL*, s 237(1)(b).
[98] *ACL*, s 239(1)-(3).
[99] *ACL*, s 239(1)(a)(ii).
[100] *Competition and Consumer Act 2010* (Cth) ('*CCA*'), s 134A.
[101] *CCA*, s 134(1).

has the obvious benefit of permitting the regulator and the entity to avoid the costs of extended litigation, without losing the deterrent effect of a formal response and financial penalty.

Before the issue of an infringement notice, the ACCC can issue a **substantiation notice** where the relevant entity has made a claim or representation promoting the supply of its services,[102] which may become relevant where, for example, the entity appears to promote the privacy-enhancing qualities of its service. The substantiation notice may require the entity to give information and/or produce documents to the ACCC 'that could be capable of substantiating or supporting' the relevant claims or representations. Such a notice might be used where the regulator does not have ready access to the relevant information, such as evidence of the entity's actual data practices. If the information and/or documents provided by the entity do not appear to substantiate the claims, the ACCC may decide to take further enforcement action.

3.3.4.2 Proceedings brought by the ACCC under the *ACL*

During and after the DPI, the ACCC has brought proceedings against several companies for contraventions of the *ACL* in respect of representations made to consumers concerning the entity's data practices. In this respect, the ACCC's enforcement actions are similar to actions brought by the United States Federal Trade Commission in respect of misleading or deceptive practices under section 5 of the Federal Trade Commission *Privacy Act*, in instances where US entities have not abided by the privacy promises made to consumers in their privacy policies or otherwise created misleading or deceptive impressions through representations about their data practices.[103]

The ACCC first brought proceedings in the Federal Court against HealthEngine, in which HealthEngine admitted that over a four-year period it disclosed 135,000 patients' non-clinical personal information records to third parties without the sufficiently informed consent of those patients, and particularly without informing patients that their consent to receiving 'a free call from our private health insurance experts' would result in their personal information being provided to a third-party insurance broker.[104] This conduct contravened sections 18 and 34 of the *ACL*. Of the AUD 2.9 million fine imposed on HealthEngine in respect of three types of conduct, approximately AUD 1.4 million related to these misrepresentations as contraventions of section 34.

The Federal Court also made a non-punitive order under section 246 of the *ACL*, requiring HealthEngine to email the affected patients within 28 days, with information including the fact of disclosure of their personal information; the nature of the personal information; the identity of the relevant insurance broker(s); the fact that the conduct amounted to a contravention of the *ACL*; and instructions on how the patient could request that their personal information be deleted.[105] The Court made an order under the same section, requiring HealthEngine to arrange for an independent annual review of its *ACL* compliance program over the following three years.

The ACCC has also brought proceedings under the *ACL* against:

---

[102] *ACL*, s 219(1)(a).
[103] See Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114 *Columbia Law Review* 583, 628-638.
[104] *ACCC v HealthEngine Pty Ltd* [2020] FCA 1203; ACCC, 'Health Engine in Court for Allegedly Misusing Patient Data and Manipulating Reviews' (Media Release, 8 August 2019).
[105] *ACCC v HealthEngine Pty Ltd* [2020] FCA 1203.

- Google – alleging that Google's privacy settings in respect of the collection and retention of users' location data were likely to mislead consumers;[106]
- Google – alleging that Google engaged in misleading conduct when it promised in its privacy terms that it would not combine DoubleClick and Google datasets (which included personal information of users) without users' active opt-in consent and later amended its privacy terms to remove this promise;[107] and
- Facebook – alleging that Facebook misled consumers by representing that its Onavo Protect app would keep users' personal activity data private and protected, and that the data would only be used for providing Onavo Protect's products, when in fact it allegedly collected, aggregated and used significant amounts of users' personal activity data for Facebook's commercial benefit.[108]

The ACCC has sought the maximum pecuniary penalties under the *ACL* in respect of these practices. The litigation is still underway in each case.

During the current ACCC Ad Tech Inquiry, the Chair of the ACCC has also foreshadowed further potential cases under the *ACL*.[109]

3.3.5 Competition law

The Australian competition legislation is less likely to play a role in addressing deficiencies in informed consent for personal data practices, but it is possible for such deficiencies to result in competition law contraventions. For example, companies that compete to supply services in a certain market might make an arrangement, or engage in a concerted practice, by which the rivals impose more detrimental data practices on consumers, substantially reducing competition on the quality of privacy terms. It is also conceivable that a company would contravene the misuse of market power prohibition[110] if it possesses substantial market power and it engages in conduct which prevents other companies from offering privacy-enhancing competition, say by excluding privacy-enhancing offers from its digital platform service. However, this conduct would only contravene if it had the effect, likely effect or purpose of substantially lessening competition. This would generally require the exclusion of a number of rivals on the same basis.

A corporation contravening these provisions would face maximum penalties up to the greater of AUD 10 million, three times the value of the benefit obtained, or 10 percent of annual turnover.[111] The corporation's rivals and customers could potentially obtain an injunction,[112] and/ or claim damages for loss or damage suffered, or likely to be suffered, as a result of the contravention.[113]

3.4 Proposals for reform

It is encouraging to observe the recent actions taken by the ACCC in bringing proceedings to test the application of the *ACL* in respect of online privacy policies, increasing incentives for

---

[106] ACCC, 'Google Allegedly Misled Consumers on Collection and Use of Location Data (Media Release, 29 October 2019).
[107] ACCC, 'ACCC Alleges Google Misled Consumers About Expanded Use of Personal Data' (Media Release, 27 July 2020).
[108] ACCC, 'ACCC Alleges Facebook Misled Consumers When Promoting App to 'Protect' Users' Data' (Media Release, 16 December 2020).
[109] Ben Butler, 'Australia's Competition Regulator Flags Legal Cases Against Tech Companies Over Ads' (*The Guardian Australia online*, 14 January 2021).
[110] *CCA*, s 46(1).
[111] *CCA*, s 76(1A)(b).
[112] *CCA*, ss 82, 87(1). The Commonwealth Director of Public Prosecutions may prosecute cartel offences and seek criminal penalties, where further elements of intent and knowledge are established: *CCA*, ss 45AF, 45AG.
[113] *CCA*, s 80.

firms to be more transparent in their notices to consumers, and advocating for substantial law reform. The Consumer Data Right regime has also provided a precedent for providing individuals with much more substantial remedies and recourse, although it is only in operation in the banking sector to date.[114] However, the OAIC, as the regulator tasked with enforcing the *Privacy Act*, should be properly empowered and funded to fulfil that role effectively across all sectors and entities covered by the legislation, and individuals should be provided with appropriate recourse under the *Privacy Act*.

Direct right of action

The effective operation of the *Privacy Act* is currently impeded by the limited recourse and remedies it provides for individuals. This is evident in minor compensation awards which are unlikely to incentivise compliance; individuals left without any remedy where the OAIC declines to make a formal determination; and the absence of a substantial body of case law establishing the OAIC's, let alone the courts', interpretation of the *Privacy Act*. The law should be reformed to provide individuals with both a direct right of action to seek compensation for contraventions via the courts, and low-cost, transparent recourse through the OAIC.

As to the first of these, individuals should have a right to approach a court directly to seek compensation for contraventions of the *Privacy Act*. This is a vital reform to ensure that the presently very limited body of judicial interpretation of the *Privacy Act* is increased for the benefit of individuals and APP entities alike; to ensure individuals' access to justice is not hampered by the finite resources of the OAIC; and to increase the deterrent effect of potential compensation orders or damages under the *Privacy Act*. Such a right is already available in respect of breaches of the Privacy Safeguards under the Consumer Data Right regime. This would also be in keeping with the provision for direct action by individuals in privacy legislation in other jurisdictions, including the rights provided to individuals under the General Data Protection Regulation in the European Union.[115]

While some have argued that a direct right of action would in fact increase the cost of redress for individuals,[116] this will not be the case if the OAIC determination regime is also retained with necessary reforms, as it should be.[117] Contrary to the submissions of Google and Facebook,[118] individuals who have the resources to pursue compensation for contraventions through the courts should be entitled to do so without any prior investigation, conciliation or determination by the OAIC. Requiring the involvement of the OAIC in these ways would perpetuate the unnecessary cost, delay and potential for obstruction which may arise under the current system. The absence of such a requirement is also in keeping with the absence of any such a requirement in respect of the ACCC under the *ACL*.

The introduction of a direct right of action should not be avoided on the basis of the concern expressed by Facebook that such a direct right for individuals would create an undue burden on court resources.[119] Nor should the government accept Facebook's submission that a direct right should therefore only be provided in respect of "serious interferences with

---

[114] See chap 6.2.3 on the Consumer Data Right.
[115] General Data Protection Regulation, arts 79, 82. See further, eg, the South Korean Personal Information Protection Act which permits both mediation by the privacy regulator and direct action for damages in a court of law by any data subject who suffers damage as a result of a contravention: Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford, 2014) Chap 5.
[116] See, eg, Patrick Zhang and David Masters, *Atlassian's Submission to the Attorney-General in relation to the Privacy Act Review Issues Paper* (Atlassian, 4 December 2020).
[117] As discussed below.
[118] Google, *Submission to the Attorney General's Department Privacy Act Review* (29 November 2020); Facebook, *Submission to the Australian Privacy Act Review issues paper* (6 December 2020) 46.
[119] Facebook, *Submission to the Australian Privacy Act Review issues paper* (6 December 2020). See further Data Republic, *Submission to the Attorney-General's Department Privacy Act Review* (29 November 2020), arguing it would be "difficult to avoid a range of vexatious cases through the courts".

privacy" after "the Commissioner confirms that attempts at conciliation by the Commissioner have not been successful".[120] As in the case of private enforcement under the *ACL*, the disincentive provided by the potential for adverse costs orders, in addition to the immediate cost of litigation in time and resources, is likely to ensure that there is not a surge of trivial claims by individuals under the *Privacy Act*.

Section 52 determinations

In addition to a direct right of action, the section 52 determination regime should be retained. This would provide a low-cost alternative for individuals who lack the resources to pursue litigation directly. However, the existing regime should be amended to provide greater transparency and accountability. The Commissioner may currently decide not to investigate, or not to investigate further, an act or practice which is the subject of a complaint, without making any formal determination under section 52, if the Commissioner is satisfied that:

- the act or practice is not an interference with the privacy of an individual;[121]
- an investigation or further investigation is not warranted having regard to all the circumstances;[122]
- the respondent has dealt, or is dealing, adequately with the complaint.[123]

In each of these cases, it would be better for the Commissioner to be required to make a formal determination under section 52 if the complainant requests a formal determination. Given that the statute still permits the Commissioner to decline to investigate further where 'the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith',[124] this would not require the Commissioner to formally determine these kinds of complaints.

Further OAIC investigative powers

In the context of its search and seizure powers, the Commissioner should be expressly empowered to:

- make copies of copies of information and documents specified in the warrant and operate electronic devices to determine whether the kinds of information and documents specified in the warrant are accessible; and
- seek a warrant to preserve or secure relevant documents or make it an offence to destroy documents reasonably required by the Commissioner.

Resources

The OAIC must be provided with funding and resources necessary to be an active regulator capable of:

- addressing increasingly concerning privacy contraventions in the digital age;
- incentivising compliance; and
- testing the law, including by litigating some more 'risky' cases.

Alternative funding sources might also be considered, including, for example, that of the UK Information Commissioner's Office, which obtains the vast majority of its funding through

[120] Facebook (n 119) 46.
[121] *Privacy Act*, s 41(1)(a).
[122] *Privacy Act*, s 41(1)(da).
[123] *Privacy Act*, s 41(2)(a).
[124] *Privacy Act*, s 41(1)(d).

tiered fees paid by entities regulated by the legislation, depending on the entity's nature, number of staff and annual turnover.[125]

Further remedies

Civil penalties under the *Privacy Act* should at least be increased to the greater of AUD 10 million, three times the benefit obtained or 10 percent of turnover, as the government has proposed. This would bring *Privacy Act* penalties into line with those under the *ACL* and for breaches of Privacy Safeguards under the Consumer Data Right regime. Given that the turnover in this case is likely to be interpreted as local turnover, these penalties are still well below other jurisdictions which impose penalties for privacy contraventions based on a percentage of global turnover,[126] and may still therefore lack deterrent effect in some cases.

As foreshadowed by the Treasurer,[127] the OAIC should also have the power to issue an infringement notice backed by penalties. This would allow entities to elect to cooperate with the Commissioner and pay a fine to resolve a minor breach, rather than the matter being heard by a court.[128]

Further, there is no reason why an entity should be permitted to retain personal information that it has improperly collected. In the context of section 52 determinations, the statute should expressly give the Commissioner the power to order an entity to delete personal information where the Commissioner finds the entity has collected that information inappropriately.

Making these modest reforms would work to offset to some extent the imbalances in bargaining power and information that currently confront individuals in attempting to exercise agency in respect of their privacy, in the face of growing incentives and encouragement for firms to collect, aggregate and mine vast quantities of personal data.[129]

---

[125] Information Commissioner's Office, UK Government, ''Data Protection Fee Payment and Online Registration' (ICO website) https://ico.gov.uk/for-organisations/data-protection-fee/faqs-data-protection-fee-payment-and-online-registration

[126] See Australian Privacy Foundation, *Bringing Australia's Privacy Act up to international standards: Submission in response to Privacy Act Review – Issues Paper* (18 December 2020) 34, citing EU and South Korean laws.

[127] Attorney-General's Department, 'Tougher Penalties to Keep Australians Safe Online' (Media Release, 24 March 2019) https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019.

[128] Ibid.

[129] See chapter 5.

ROB NICHOLLS

4. Chapter 4 – Informed consent to online standard form agreements

4.1 Introduction

This chapter focuses on the unease with which traditional notions of informed consent have been applied to online standard form agreements. It discusses why the protective elements of unconscionability and unfairness have been disregarded in favour of freedom to contract and commercial convenience. The procedural and highly complex nature of standard form agreements entered into online are poorly understood by policy makers. This is reflected in the academic literature and case law addressing online standard form agreements. It is evidenced by a patchwork regulatory environment. This chapter attempts to address this situation. Instead of attempting to conform normative theories of contract, the chapter focuses on the influence of technological advancement. It examines the impact of actual and desirable increases in economic efficiency and the effects that these factors have had on the development of regulation dealing with online standard form agreements. The focus is on informed consent and the chapter argues that this essential element of contract theory has been abandoned. The chapter concludes by providing a more relevant understanding of truly informed consent to online standard form agreements.

Standard form agreements, also known as fine print or boilerplate contracts and contracts of adhesion, are widely used where consumers acquire services. The *Australian Consumer Law* (*'ACL'*) provides that a standard form agreement is typically prepared by one party to the contract and is not subject to negotiation between the parties—that is, it is offered on a 'take-it-or-leave-it' basis to the non-drafting party.[1] In the European Union, the Treaty on the Functioning of the European Union article 169 sets out the basic principles of consumer protection; ie the protection of consumer interests and the promotion of rights.[2] The Unfair Contract Terms Directive (93/13/EEC) protects consumers against unfair standard contract terms in standard form agreements. These agreements are relied upon for billions of commercial transactions per year and account for the vast majority of contracts. Despite the prevalence of these agreements, for almost 80 years scholars and policy makers have not addressed the procedural and formative distinctiveness of the agreements.[3] That is, they have not provided or proposed mechanisms to ensure that the non-preparing party is fully informed. According to McMahon:

> online consumer contracts distinguish themselves from conventional contracts in a manner that is theoretically significant, in that agreements are relational and enduring but not deliberative, and consent is qualified.[4]

The steps of offer, acceptance, intention to create a legally binding agreement, consideration, a legal capacity and consent are usually regarded as the foundations of an enforceable contract. This classical model of contract assumes the parties will discuss, agree upon and understand all important terms before entering into an agreement. This

---

[1] *Australian Consumer Law (ACL) Schedule 2 to the Competition and Consumer Act 2010.*
[2] Beyond these general principles, there are four main Directives: the Product Liability Directive 1985, Unfair Terms in Consumer Contracts Directive 1993, Unfair Commercial Practices Directive 2005 and the Consumer Rights Directive 2011.
[3] Friedrich Kessler, 'Contracts of Adhesion-Some Thoughts About Freedom of Contract' (1943) 43 *Colum. L. Rev.* 629.
[4] Christopher McMahon, 'IPromise: How Contract Theory Can Inform Regulation of Online Consumer Contracts' (2018) 21 *Trinity College Law Review* 174

model procedural process could not be further from the reality of the standard form agreements. This is particularly true in respect of online standard form agreements, which are contracts that are almost always provided on a take-it-or-leave-it basis. That is, the consumer has the choice of agreeing to the standard form agreement or not being able to acquire the service at all.

Instead of recognising the uniqueness of these agreements, futile attempts at conforming standard form agreements to traditional notions have contract have focused on increased disclosure of unfavourable terms[5] and minor revisions to existing legislation. This position is changing in the EU and in Australia. For example, the Australian Competition and Consumer Commissions' 2018 Digital Platform Inquiry[6] into the impact of online search engines, social media and digital content aggregators (digital platforms) on competition in the media and advertising services markets, provided 23 recommendations aimed at identifying and minimising potentially adverse consequences that result from the growth of digital platforms. Online standard form agreements were a significant focus in the final report.

4.2 Standard Form Agreements – An Overview

Despite the economic efficiencies that are derived from using standard form agreements, academic arguments criticising their flaws are less resolute. According to Bagchi:

> As scholars of different stripes have brought their respective concerns and expertise to the problem, we are left with a multi-dimensional diagnosis.[7]

Key criticisms focus on market failures, behavioural biases and a degradation of the democratic process.[8] The lack of a cohesive and definitive understanding of the issues presented by standard form agreements has resulted in a piecemeal approach to regulating the agreements worldwide. Countries vary in their application of competition, consumer, privacy and data protection law depending on the social, legal and economic constructs of the market in which they operate.

In 1971, Slawson claimed that the realities of mass production and a consumer economy have undermined the theoretical basis for much of traditional contract law.[9] Korobkin, in the context of oral representations and a subsequent standard form agreement, acknowledged the universal unfairness of these agreements and that consumers enter into standard form agreements with very little understanding to what they were agreeing to or the terms that were being imposed on them.[10] Even fifty years ago, Griffin recognised:

> [w]e are faced with an historic choice in contracts. We can lump together standard forms and classic contracts, or we can treat the former differently.[11]

In the five decades that have passed, the non-drafting party to standard form agreements remain in the same predicament. Instead, according to Preston and McCann, standard form agreements have been left to become 'a beast untied from the contexts in which form contracts gained (limited) legitimacy'. The authors go on to liken the agreements to a 'wild

---

[5] Kenneth K Ching, 'What We Consent to When We Consent to Form Contracts: Market Price' (2015) 84(1) *UMKC Law Review* 1.
[6] Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry Final Report* (2019) https://www.accc.gov.au/system/files/Digital platforms inquiry - final report.pdf.
[7] Aditi Bagchi, 'At the Limits of Adjudication: Standard Terms in Consumer Contracts' http://papers.ssrn.com/abstract=2772733.
[8] W David Slawson, 'Standard Form Contracts and Democratic Control of Lawmaking Power' (1971) 84(3) *Harvard Law Review* 529.
[9] Ibid.
[10] Russell Korobkin, 'The Borat Problem in Negotiation: Fraud, Assent, and the Behavioral Law and Economics of Standard Form Contracts' (2013) 101(1) *California Law Review* 51.
[11] Ronald C Griffin, 'Standard Form Contracts' (1977) 9 *NC Cent. LJ* 158.

horse while forgetting that such beasts were only originally allowed into civilized communities because they were in a corral.'[12]

Another, earlier criticism, by Kessler stated:

> [f]reedom of contract enables enterprises to legislate by contract and, what is even more important, to legislate in a substantially authoritarian manner without using the appearance of authoritarian forms.[13]

In a standard form agreement, the assenting party does not agree to all the private law that will govern the contractual relationship, instead they agree 'to only a part - and usually only a very small part -and delegate to one of them (usually the seller of the product or service involved) the power to make the rest.'[14] The price is usually the part that is agreed upon, and the drafting party is left to unilaterally stipulate the terms of the agreement.

This kind of privately made law characterises standard form agreements and controls our society to a greater extent than most people realise. The power to contract in standard form agreements is the power of one party to impose whatever terms he likes on the other.[15] Concerns for the welfare of consumers have been responded to with various sources of hard and soft laws, without much success. As Slawson suggests:

> Those who are subject to private laws without their consent need the protection which only judicial review can provide, and judicial review is not likely to be forthcoming unless private law-making is recognized as law-making.[16]

Allowing private law making to continue unregulated and unrestricted increases the risks consumers face and foundationally alter the legal culture of a society, in a way that generally goes against public interest.[17] For example, when a standard term prevents class action lawsuits or access to judicial remedies, the default procedural protections of the law are swept away.

In assessing the validity of specific terms included in standard form agreements, traditional tests have focused on 'awareness', 'consistency and regularity' and 'fairness and reasonableness'.[18] As Wang instructs:

> [t]he cornerstone element for the incorporation of terms (by signature, by notice and by course of dealing) is the awareness test, namely, reasonably sufficient/conspicuous notice and manifested unambiguous consent.[19]

An application of the 'awareness' test to online standard form agreements would suggest that the drafting party is obliged to draw attention to the existence of contract terms. Traditional notions of 'consistency and regularity' could be satisfied in an online context by the regulatory provision of a specific procedural format and the 'reasonableness and fairness' test for unfair terms in contracts be understood through the lens of unfair contract terms, as they have been applied and understood in the context of consumer law.

The most widely criticised terms in standard form agreements are arbitration clauses that displace legal remedies and often prevent parties from accessing traditional dispute

---

[12] Cheryl B Preston and Eli W McCann, 'Unwrapping Shrinkwraps, Clickwraps, and Browsewraps: How the Law Went Wrong from Horse Traders to the Law of the Horse' (2011) 26 *BYU J. Pub. L.* 1.
[13] Kessler (n 3).
[14] Slawson (n 8).
[15] Sandra Fredman and Darcy Du Toit, 'One Small Step Towards Decent Work: Uber v Aslam in the Court of Appeal' (2019) 48(2) *Industrial Law Journal* 260.
[16] Slawson (n 8).
[17] Adam Ship and Danny McMullen, 'The Legal Relevance of Bargaining Power in U.S. and Canadian Franchise Litigation' (2015) 34(4) *Franchise Law Journal* 571.
[18] F Wang, 'The Incorporation of Terms into Commercial Contracts: A Reassessment in the Digital Age'.
[19] Ibid.

resolution mechanisms.[20] These unilateral clauses are contrary to the best interests of consumers. Other contentious terms include forum selection clauses,[21] shortened statute of limitations periods,[22] bans on class action suits,[23] liability waivers,[24] unilateral modification of terms and consent expiry dates.[25]

In Australia and many other countries around the world, standard form agreements are enforced on the basis that they are a valid contract. However, according to Slawson:

> [s]ince a contract is in theory the agreement of the parties to it, and since an agreement which is uncoerced expresses the consent of each person making it, the assumption upon which standard forms are commonly enforced carries with it the conclusion that the law of which they consist. The conclusion to which all this leads is that practically no standard forms, at least as they are customarily used in consumer transactions, are contracts. They cannot reasonably be regarded as the manifested consent of their recipient because an issuer could not reasonably expect that a recipient would read and understand them.[26]

Despite the logic of Slawson's conclusions, when faced with regulating standard form agreements, regulators are left with a decision to prioritise consumers by protecting them against unfair contract terms or to focus on transparency.[27] When focusing on transparency, as long as the terms are available to the non-drafting party in the pre-contractual process and they are given an option to read, then the agreement is deemed enforceable.

Courts around the world have demonstrated a reluctance to declare contracts void as against public policy, because it has long been held that:

> men of full age and competent understanding shall have the utmost liberty of contracting, and that their contracts when entered into freely and voluntarily shall be held sacred and shall be enforced by Courts of Justice.[28]

In 1943, Kessler cautioned that as long as society and the lawmakers fail to realise that freedom of contract means different things in the context of different types of contracts the illusion that the 'law' will protect the public against any abuse of freedom of contract will continue.[29] Kessler further advocated that the meaning of contract must shift in accordance with the social importance of the type of contract and the degree of monopoly power held by the drafter.[30]

Standard form agreements are an essential component of a society driven by mass production and consumerism. As a society, we have allowed the existence of monopolies in many online markets. Freedom of contract in these markets is very much a one-sided privilege. Arguably, the freedom of contract under English common law means that the consumer could have a good faith obligation under a standard form agreement.[31]

When the doctrine of freedom to contract was being developed, the courts could not have predicted the pervasiveness and role of standard form agreements consented to in an online

---

[20] Margaret Jane Radin, 'Reconsidering Boilerplate: Confronting Normative and Democratic Degradation' (2012) 40(3) *Capital University Law Review* 617.
[21] Yannis Bakos, Florencia Marotta-Wurgler and David R Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts' (2014) 43(1) *Journal of Legal Studies* 1.
[22] 'Al-Safin v. Circuit City Stores, Inc., 394 F.3d 1254, 1259 (9th Cir. 2005)'.
[23] Kristin B Cornelius, 'Standard Form Contracts and a Smart Contract Future' (2018) 7(2) *Internet Policy Review*.
[24] Bagchi (n 7).
[25] Bart Custers, 'Click Here to Consent Forever: Expiry Dates for Informed Consent' (2016) 3(1) *Big Data & Society* 2053951715624935.
[26] Slawson (n 8).
[27] Ibid.
[28] Kessler (n 3).
[29] Ibid.
[30] Ibid.
[31] Paul S Davies, 'The Basis of Contractual Duties of Good Faith' (2019) 1(1) *The Journal of Commonwealth Law* 1.

environment. The steps of offer, acceptance, intention to create a legally binding agreement, consideration, a legal capacity and consent are vastly different and unique in their procedural process, when compared with traditional forms of contract. Online standard form agreements are fundamentally influenced by the technical design and interface of the user interface (whether a website or an application). When dealing in online environments, Wang believes that the availability of terms, the provision of unambiguous consent and the content of terms are key considerations in determining the validity of an agreement.[32] This differs to the traditional assessment of methods of incorporation and protection against unfair terms. There is a total failure in online contracting environments to secure informed consent. In many examples of access to free online services a user is presented with a 'take-it-or-leave-it' clickwrap agreement, which they must assent to before being able to use the product or service.

Online standard form agreements have evolved to a point where consumers are not required, or even encouraged, to open the terms and conditions of the agreement. The agreements provide a sense of order and act as a 'relationship manual' and are typically only pored over in detail when a dispute arises. However, their prevalence is also product of their substance. We contract with each other at a rate that is prohibitive to anyone stopping and reading the terms and conditions to which they are agreeing, ie becoming informed. Consumers are simply not willing to dedicate time to read and understand lengthy documents. Standard form agreements are therefore legitimised by the parties who continue to consent to the one-sided terms and by the courts and policymakers who fail to recognise that these agreements need to be viewed through a new framework and not reworked to be understood in the context of traditional doctrines of contract law. This lack of informed consent in online standard form agreements is discussed below.

4.3 Informed Consent

> No customer in a thousand ever read the conditions. If he had stopped to do so, he would have missed the train or the boat.[33]

Consent has been described as the master concept that defines the law of contracts. Consent can be express or implied, informed, voluntary, current and adequately understood. We know, and have known, for over a century that people don't read standard form agreements. We also know that it is near impossible to obtain fully informed consent to standard form agreements.[34] Studies have shown that one demographic is any more likely to read than any other. We live in a culture where non-informed consent is given freely and routinely. Bechmann refers to this as a blind non-informed consent culture.[35]

The definition of informed consent varies between each jurisdiction and between each sector. In the European Union, a definition of informed consent is outlined in the Data Protection Directive 1995 (95/46/EC):

> Consent is any freely given specific and informed indication of the data subjects wishes by which the data subject signifies his or her agreement to personal data relating to him/her being processed.

Further, according to the Article 29 Data Protection Working Party Opinion 15/2011 consent:

> [c]an only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation coercion or significant negative consequences if he or she does not

---

[32] Wang (n 18).
[33] *Thornton v Shoe Lane Parking Ltd* [1971] 2 QB 163' (1971).
[34] Bakos, Marotta-Wurgler and Trossen (n 21).
[35] Anja Bechmann, 'Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook' (2014) 11(1) *Journal of Media Business Studies* 21.

> consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free.

In Australia, consent is defined in the *Privacy Act 1988* (Cth). Accordingly, consent can be 'express' or 'implied' consent. According to the Australian Guidelines to the National Privacy Principles, express consent is given explicitly, either orally or in writing.[36] On the other hand, implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation.[37] However, the *Privacy Act* does not outline any criteria for valid or informed consent.

The basis of disclosure in standard form agreements is to give a person of ordinary intelligence a reasonable opportunity to know to what they are assenting. Informed consent can only result when terms are transparent and the non-drafting party comprehends the contents of disclosure documents, privacy statements and/ or terms and conditions. Friedman et al[38] formulated a series of five principles that determine whether the non-drafting party could reasonably be in a position of providing their informed consent to a standard form agreement. These include disclosure, competence, comprehension, voluntariness and agreement.

While, according to Bashir, the key elements of informed consent include comprehension and voluntariness.[39] Bashir acknowledges that because readers do not take the time to read the terms and conditions, their comprehension of these agreements is likely to be low.[40] For Bashir, comprehension refers to an individual's accurate interpretation of the significance of disclosures.[41] In order to demonstrate comprehension, individuals should be able to restate the key conditions of a disclosure agreement in their own words and apply its contents to another context.[42]

Similarly, Bechmann focuses on coercion in the context of consent.[43] She says that a choice can be construed as being coerced if the chooser perceives that not to choose in one way will result in consequences which he strongly desires to avoid.[44] Bechmann further instructs:

> A standard form contract is not always adhesive, and the absence of a standard form does not guarantee that the contract is not adhesive. But the predominance of standard forms increases the proportion of contracts that are adhesive. Standardization reduces the number of choices and so makes more likely the possibility that in any particular instance there will be only one that is reasonable.[45]

In a recent case, *State of Tasmania v Herlihy* [2019] TASSC 5, the Supreme Court of Tasmania considered behaviour amounting to 'consent' with reference to the Electronic Communications Act 2000 (Cth). According to section 3 of that Act:

---

[36] Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2019) https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf.
[37] Ibid.
[38] Batya Friedman, Daniel C Howe and Edward Felten, 'Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design' in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (IEEE, 2002) 10.
[39] Masooda Bashir et al, 'Online Privacy and Informed Consent: The Dilemma of Information Asymmetry' in *Proceedings of the 78th ASIS&T Annual Meeting: Information Science with Impact: Research in and for the Community* (American Society for Information Science, 2015) 43.
[40] Ibid.
[41] Ibid.
[42] Bashir et al (n 39).
[43] Bechmann (n 35).
[44] Ibid.
[45] Ibid.

consent includes consent that can reasonably be inferred from the conduct of the person concerned, but does not include consent given subject to conditions unless the conditions are complied with.

Specifically, it was determined in this case that the provision of an email address did not establish valid consent to be contacted via email.

4.4 What is informed consent in the context of an online SFA?

Consent in online standard form agreements is reduced to a fleeting transaction in which the non-drafting party knowingly forfeits their privacy or data in exchange for access to a 'free' service or to finalise a purchase, subscription or user account. The forced choice dilemma is a ubiquitous issue facing users of web platforms and parties to online standard form agreements. In online environments, it is common for users to be presented with a situation where they can either accept a service provider's terms and conditions or simply not use the service at all. In many jurisdictions, this forced choice does not meet the threshold requirements for invalidation of the agreement, as assent is quite obviously, involuntary. Despite this reality, enforceability of online standard form agreements is still judged on the notion of procedural fairness. As long as there is transparency (that is, the terms are disclosed), then the agreement is deemed to be fair and enforceable.

In 2013, the Australian Communications and Media Authority (ACMA) published a report which acknowledged the difficulty of '…securing an individual's informed consent to the collection and use of their personal information… in an environment characterised by increasingly frequent, varied and complex transactions in the digital information economy.'[46] While, according to the European Commission,'[o]nline platforms can be described as software-based facilities offering two-or even multi-sided markets where providers and users of content, goods and services can meet.' For Kerber a well-functioning online market will not be possible without continual (re)definition and (re)specification of property rights to personal data and ongoing review of privacy policies against new kinds of privacy violations.[47]

In Australia and the UK, specific terms are generally considered transparent if:

- they are presented to the non-drafting party at the time that they enter into an agreement;
- there is a reasonable opportunity for the non-drafting party to become aware with them;
- they are presented in clear, jargon free language and decent sized print;
- the sentences, paragraphs and overall contract are well structured; and
- appropriate prominence is given to particularly substantively detrimental terms.[48]

These conditions are not typically present in online standard form agreements for a range of reasons. According to McMahon online standard from agreements 'distinguish themselves from conventional contracts in a manner that is theoretically significant, in that agreements are relational and enduring but not deliberative, and consent is qualified'.[49]

There is increasing criticism from scholars and a reluctance from policymakers to rely on the informed consent model as the foundation for privacy and data protection laws. This is because the consumer is:

- unlikely to understand how their data will be captured, stored or disseminated; and

---

[46] Stephen Corones and Juliet Davis, 'Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions' (2017) 45(1) *Federal Law Review* 65.
[47] Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11(11) *Journal of Intellectual Property Law & Practice* 856.
[48] Chris Willet, 'Transparency and Fairness in Australian and UK Regulation of Standard Terms' (2013) 37 *UW Austl. L. Rev.* 72.
[49] McMahon (n 4).

- likely to be presented with a take-it-or-leave-it agreement where there is no real consent to the terms.

Additionally, the privacy of a society as a whole should not be left in the hands of private lawmakers unilaterally creating agreements that strip away the fundamental privacy rights of the populace.[50] It is common practice for companies to circumvent data handling and privacy regimes using their own consent forms.

While the problems with standard form agreements were recognised by scholars such as Kessler and Slawson long before the invention of the world wide web, many of these issues have been exacerbated by the online environment.[51] For example, the presentation of a lengthy, hard copy contract may cause a non-drafting party to think twice about the seriousness of the agreement to which they are entering. Further, in an online environment, the agreement is often presented in a hyperlinked clickwrap form, that is optional for the non-drafting party to open before 'clicking' consent. It is paradoxical then, that technology, which is created to increase efficiencies and enhance the user experience and empower consumers is then the same environment that has been found to restrict access to information and deceive users on the use of their personal information and data privacy.

Online environments are being designed to exploit consumers in ways that they may not even realise. Simply by browsing a webpage, a consumer can have entered into an agreement. In this scenario, meaningful consent cannot possibly have occurred. As Schell warns '[i]f you can control where someone is going to look, you can control where they are going to go'.[52] The visual interface affords the drafting party considerable with unlimited opportunities to shape how consumers interact with their platform. For example, strong and inviting visual content has been found to increase the amount of goods sold to impulse buyers.[53] In the absence of specific regulation governing design interfaces, online platforms are created intentionally to deepen information asymmetries and to allow consumers to agree to terms with minimal thought and consideration. The primary objective of which is to prevent users from meaningfully consenting to and understanding the privacy policy and resulting collection, use and distribution of their data.

The ACCC Digital Platform Inquiry concluded that digital platforms have the ability to design user interfaces that will lead users to make privacy-intrusive selections.[54] This can be made possible by appealing to certain psychological or behavioural biases, using design features such as privacy-intrusive defaults or pre-selections.[55] The Inquiry concluded that the Australian regulatory framework does not adequately address data practices, such as website design principles, that are intended to exploit the information asymmetries, behavioural biases and power imbalances between digital platforms and reasonable users of the internet.[56]

Researchers are beginning to call for an application of the established principles of informed consent as they apply to hard copy agreements to online standard form agreements.[57] While, in theory, unfair contract terms legislation that take into account tests of reasonableness and fairness, apply to online standard form agreements in the same way that they do to paper-based transactions, case law suggests that this is not been the

---

[50] Slawson (n 8).
[51] Kessler (n 3); Slawson (n 8).
[52] Jesse Schell, *The Art of Game Design: A Book of Lenses* (AK Peters/CRC Press, 2019).
[53] McMahon (n 4).
[54] ACCC (n 6).
[55] Ibid.
[56] Ibid.
[57] Bagchi (n 7).

definitive approach,[58] and that there needs to be further consideration of the specific influences of the online environment.

In the recent Australian Digital Platform Inquiry, clickwrap agreements, take-it-or-leave-it terms, and bundling of consent were identified to degrade the quality of consent in online standard form agreements. The report outlined a series of conditions for valid consent in online environments. These included a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). In practice, the authors of the Digital Platform Inquiry final report suggest that 'any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled.'[59]

Other solutions specific to online environments have been proposed by Friedman et al,[60] Cornelius[61] and Van Der Geest et al.[62] Friedman et al propose a series of five principles of web design that centre around cookie management capabilities purposed with ensuring informed consent. The principles include disclosure, competence, comprehension, voluntariness, and agreement. Similarly, Cornelius discusses notions of genuine effort signal 'reasonable communicativeness' in online environments, suggesting that an application of the doctrine of procedural unconscionability with factors such as awareness, agreement, presentation, and meaningful choice.[63] Finally, Van Der Geest et al compare consent in online environments with consent in medical settings, concluding by offering a list of six items that ought to be used in user profiling consent forms that would lead to greater levels of informed consent.[64]

Compounding the failure to read problem evidenced in both traditional and online standard form agreements, is the fact that many online consumer transactions now take place with no monetary payment. For example, social media platforms, web browsers, search engines and email accounts are now typically offered 'free of charge'. In a subconscious quid pro quo arrangement, the consumer agrees to unilaterally give up all their data privacy rights.

Online contracting environments have served to systematically enhance the disparity between businesses and consumers. As is evidenced by the many unsuccessful attempts at minor and unsystematic intervention to mitigate negative consequences of online standard form agreements, traditional contract law theory and frameworks cannot be successfully adapted to the online environment.[65] As McMahon suggests, this different type of consumer contract merits a distinct approach, one that has sufficient flexibility to adapt to business practice to continue to protect the consumer.[66]

It becomes clear through an analysis of the literature and case law that there are behavioural, economic, legal and social considerations and explanations for why standard form agreements continue to be enforced despite the absence of informed consent. It is

---

[58] Kate Mathews-Hunt, 'CookieConsumer: Tracking Online Behavioural Advertising in Australia' (2016) 32(1) *Computer Law and Security Review* 55.
[59] *Digital Platforms Inquiry Final Report* (n 6).
[60] Friedman et al (n 38).
[61] Cornelius (n 23).
[62] Thea Van Der Geest, Willem Pieterson and Peter De Vries, 'Informed Consent to Address Trust, Control, and Privacy Concerns in User Profiling' [2005] *Privacy Enhanced …* 1 http://www.utwente.nl/ctit/cfes/docs/EN_artikelen/2005-Informed_Consent.pdf.
[63] Cornelius (n 23).
[64] Geest, Pieterson and Vries (n 62).
[65] Robert A Hillman, 'Consumer Internet Standard Form Contracts in India: A Proposal' (2017) 29(1) *National Law School of India Review* 70.
[66] McMahon (n 4).

also evident that policy makers cannot continue down the same path of looking for policy solutions in siloed areas of the law.

4.5 Factors impacting informed consent

As demonstrated above, informed consent doesn't occur in online standard form agreements. Here, the legal, economic, behavioural and social/cultural influences are discussed. These influences offer an insight into and explanation for why informed consent has not been taken seriously in the context of online agreements.

4.5.1 Legal considerations

Informed consent in the context of online standard form agreements has foundations in competition, consumer, and data protection and privacy law. When referring to consent, often scholars refer to a 'consent dilemma' in the context of regulatory intermediation.[67] The consent dilemma is a continuum that places privacy self-management at one end and legal intervention at the other.

Freedom to contract is perhaps the most common argument against legal intervention in standard form agreements. The time-honoured principle is grounded in autonomous decision-making theory and Kantian deontological values, the conditions of which are capacity, voluntariness and factual understanding.[68] Despite the reality that these conditions are seldom present in online standard form agreements, the principal has still been applied by courts and scholars worldwide.[69] In protecting an individual's freedom to contract, the doctrines of duress and undue influence are thought to be sufficient protections, allowing individuals to remain 'autonomous beings' and capable of making 'choices for him or herself without unjustifiable interference from others'.[70] Further, as Corones and Davis suggest:

> [s]ociety, therefore, has to give the parties freedom of contract; to accommodate the business community the ceremony necessary to vouch for the deliberate nature of a transaction has to be reduced to the absolute minimum. Furthermore, the rules of the common law of contract have to remain *Jus dispositivum* - to use the phrase of the Romans; that is, their application has to depend on the intention of the parties or on their neglect to rule otherwise.[71]

The objective of disclosure in online standard form agreements is to 'give the person of ordinary intelligence a reasonable opportunity to know what is prohibited.'[72] Hillman argues that online standard form agreements are enforceable on the basis that:

> people rarely read criminal statutes or understand many of the intricacies of rules governing even those wrongs of which they are aware, such as murder or theft. The point is that people could gain access to these materials, which legitimizes the rules as law.[73]

Consumer law has rarely been applied to 'free' online services, for which there is no monetary transaction. So far, according to Helberger:

> services that are not rendered against a monetary price will often fall outside the scope of consumer law. As a result, consumers who receive services in exchange for data or attention are

[67] Bechmann (n 35).
[68] Nadia N Sawicki, 'Modernizing Informed Consent: Expanding the Boundaries of Materiality' (2016) 2016(3) *University of Illinois Law Review* 821.
[69] Ibid.
[70] Eliza Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8(1) *Law, Innovation and Technology* 1.
[71] Corones and Davis (n 46).
[72] Hillman (n 65).
[73] Ibid.

entitled to a lower level of protection than consumers that pay money for the service, even if the service is the same.[74]

Instead, much of the case law centres on competition law issues. There are a number of well-known international competition cases, including the European Google search engine case[75] and the Google Android investigation into abusive behaviour in the context of privacy, competition and market power.[76]

Another legal consideration for online standard form agreements is an understanding of the role and character of a reasonable person. Reasonableness is a characteristic referred to in many areas of the law, with a 'reasonable understanding' being the basis of determining the standard to which the law holds most of us need protection of special paternalistic character. According to Corones and Davis, in determining the 'reasonableness' of an ordinary consumer's action, the Australian Information Commissioner (OAIC), will consider a number of factors including 'the clarity of the representation, whether qualifying information is conspicuous, the importance of any omitted information (and whether such information is available elsewhere), and the familiarity of the public with the product or service.'[77] Corones and Davis advise that the Commissioner will assume the perspective 'of an ordinary, reasonable member' of whichever type of individual is relevant to the context of the case at hand.[78]

The analysis of regulatory approaches to online standard form agreements suggests that the current approach of defining informed consent in the context of a specific regulatory instrument focusing on a specific field of law is misguided. It is impossible to discuss informed consent to standard form agreements from the perspective of competition law without also referencing data protection, consumer and privacy laws. Online standard form agreements require a definition of informed consent that is grounded in each of these legal specialities and consideration of both the human rights and economic foundations.

4.5.2 Behavioural biases

Consent to standard form agreements is neither rational nor efficient.[79] The academic literature is replete with justifications grounded in behavioural psychology theories for why consumers cannot give informed consent to traditional standard form agreements. These behavioural biases are exacerbated in online markets for 'free' services where there is a fundamental lack of transparency and information on uses of personal data. Scholars recognise that some deficiencies in the contract formation process do not concern information failures but more complex, cognitive factors that affect the origin of the decision.[80]

---

[74] Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54(5) *Common Market Law Review* 1427.
[75] 'Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising - Press Release 20 March 2019', *European Commission Press Release* (online at Brussells, 20 March 2019) 3 https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.
[76] Sascha Dethof, 'European Union: European Commission: Fines Google Record € 4.34 Billion For Abusing Market Power (Android)', *European Commission Press Release* (online at Brussells, 18 May 2018) 5 https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581.
[77] Corones and Davis (n 46).
[78] Ibid.
[79] Ching (n 5).
[80] *Digital Platforms Inquiry Final Report* (n 6).

Theories and their consequent biases identified in the literature include the privacy paradox,[81] non-belief in law of large numbers,[82] group think,[83] information overload,[84] social loafing,[85] disconnect between how consumers think data is being treated and how it is actually being treated,[86] shared information bias,[87] over-optimism,[88] cognitive dissonance,[89] confirmation bias,[90] irrationality,[91] bound of reasonableness,[92] present bias[93] and consent fatigue.[94]

'Free' online services present a range of problems for consumers. The notion of something being 'free' immediately puts consumers into a mindset where they focus entirely on the zero monetary cost of the transaction at hand, disregarding the costs associated with providing their data and failing to focus on the complex decision that they ought to be making. While there is no monetary transaction associated with entering into agreements for these free online services, there is still a cost incurred by the user when their data is collected, stored and disclosed. The ACCC Digital Platforms Inquiry Final Report summarises these costs to include and increased risk of data breach and cybercrime (such as identity fraud), reputational injury, decreased privacy, and potential increases in unsolicited targeted advertising and third parties leveraging information against the consumers' interests, or targeting of scams.[95]

The privacy paradox, perhaps the most widely discussed behavioural theory in the context of online standard form agreements, focuses on why individuals believe they value privacy, while simultaneously giving away their privacy information recklessly through free online subscriptions and services. Over-optimism, under-estimation of risk and the non-belief in law of large numbers are other common consumer decision-making deficiencies. These theories centre on the premise that do not understand the future value of the data that this collected. According to Ching, human beings are not very good at estimating risk.[96] While one of the main objectives of contracts is to allocate risks, these theories argue that consumers cannot be deemed to be behaving in a rational way when consenting to online standard form agreements. Compounding this reality is the fact that there is a substantial disconnect between how consumers think their data should be treated and how it is actually treated online contracting environments.[97] According to the ACCC Digital Platforms Inquiry, there is concern that the 'existing regulatory frameworks for the collection and use of data have not held up well to the challenges of digitalisation and the practical reality of targeted advertising that rely on the monetisation of consumer data and attention'.[98] Bechmann's study on the privacy features of Facebook concluded that users did not comprehend the

---

[81] Kerber (n 47).
[82] Ignacio N Cofone and Adriana Z Robertson, 'Consumer Privacy in a Behavioral World' (2017) 69 *Hastings LJ* 1471 https://ssrn.com/abstract=3165200.
[83] Ching (n 5).
[84] Bechmann (n 35).
[85] Ibid.
[86] Katharine Kemp and Ross P Buckley, 'Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model' (2017) 18(3) *Georgetown Journal of International Affairs* 35.
[87] Bechmann (n 35).
[88] Ching (n 5).
[89] Ibid.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] ACCC (n 6).
[94] Ibid.
[95] Ibid.
[96] Ching (n 5).
[97] Kemp and Buckley (n 86).
[98] ACCC (n 6).

privacy issues of using the social media site in other features such as their Facebook inbox or secret groups.[99] Bechmann's research confirmed Acquisti and Gross' earlier findings that users of free online services simply did not know that that their data could be retrieved in many ways.[100]

Relatedly, non-belief in law of large numbers, group think and social loafing affects decision-making in online environments in a way that prevents consumers from reading the terms and conditions under the assumption that they are not the first to have agreed to the terms and conditions, therefore there should not be anything too damaging buried in the fine print. Janis uses the term 'groupthink' to describe the tendency for groups of individuals to strive towards similarity and unity and assent to online standard form agreements representing the status quo.[101] Decision-making in groups, according to Ching leads to poor or misinformed decisions and tends to increase with rapid decision-making.[102] These phenomena are no more evident than in the social media culture present in societies world over.

Relatedly, it is often theorised that consumer decisions are affected by cognitive dissonance and confirmation bias. These theories suggest that that once a consumer has decided to enter into a transaction, they are unlikely to read the terms and conditions as the process of doing so may undermine the intended benefit and utility of the transaction. Instead, consumers are likely to seek out signals and information that affirm their decisions.[103]

Other justifications for poor decision-making centre on consumers erroneously having confidence in the fact that courts would not enforce unconscionable and unfair agreements[104] and the argument that the decision to enter into an online standard form agreement is in fact rational to the consumer in the sense that the benefits they get from consenting outweigh costs.[105]

In the Australian context, it is now well established that online standard form agreements are typically enforceable. The Australian position is that irrespective of whether a consumer does not read the contents of a contract, as long as the terms are presented in a transparent and physically obvious way, then consent is presumed to be valid.[106]

4.5.3 Economic perspectives

In an economic sense, for example, an online platform allows or facilitates an exchange between two sides in a market.[107] As discussed above, advocates of free markets reject concerns over the failure to read on the basis that a minority there are a minority of people who will read and understand the agreements and that these people can advocate against and limit the inclusion of any unfair terms. Through this argument, it is in a company's best interests to take into account this informed minority and raise the quality of their agreements.[108]

From the perspective of the *homo economicus*, proceeding without opening the envelope is enormously useful. It is rational for consumers not to read online standard form agreements

---

[99] Bechmann (n 35).
[100] Ibid.
[101] Irving L Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd edition (Houghton Mifflin, 1982).
[102] Ching (n 5).
[103] Ibid.
[104] Mathews-Hunt (n 58).
[105] Ching (n 5).
[106] Mathews-Hunt (n 58).
[107] Jamila Venturini et al, 'Terms of Service and Human Rights: An Analysis of Online Platform Contracts' (Editora Revan, 2016).
[108] Ibid.

given the low likelihood that they will be able or willing to take any action over unfavourable terms. Therefore, it would be irrational for non-drafting parties to spend time reading, let alone comprehending, the terms in the agreement, as it would be a waste of time.

The decision not to provide their data, that is, agreeing to the terms and conditions of an online standard form agreement, comes at a cost to consumers. Often this cost is not being able to use the particular service or platform. Faced with this reality, consumers typically elect not to delve into the terms and conditions under the assumption that the contents of the agreement are going to be less of a detriment to their personal preferences than not accessing the service or platform.

Some scholars argue that market failures are not reducible to flaws in the process of individual consent to online standard form agreements.[109] Instead, they argue that they are the result of market concentration and monopoly power.[110] Online marketplaces and platforms are hubs of monopolistic behaviour and this has led to serious concerns about competition problems in the digital economy and how competition laws should be designed to deal with these issues.[111]

Market failures result from information overload that leads to cognitive bias. Information overload causes an otherwise rational consumer to undervalue their personal data and privacy, and thus consent to unfavourable terms in an online environment. By providing too much data at a low price, Cofone argues that this leads to an inefficiently low level of consumer privacy in the economy.[112] The notion that market price is the bound of a reasonable consumer becomes an accurate portrayal. Ching suggests:

> [s]urplus will still be generated by parties engaging in voluntary exchanges and satisfying their subjective preferences. If markets are competitive, then a market price standard should validate all transactions that occur in that market. If a market is not competitive, we should be concerned about people being taken advantage of through form contracts, and the competitive market price standard should be used to invalidate unequal transactions.[113]

Courts have the power to restore economic and social efficiency by enforcing terms that lead to the efficient operation of a well-functioning market and refusing to enforce those terms that are inefficient and unfair, leading to monopolistic behaviour and one-sided markets. Serious market failures call for regulatory remedies. This has been the case with Google and Facebook, who both hold a dominant market position. Both platforms have been accused of excessively collecting user's private data and offering an insufficient range of privacy options that align with the privacy preferences of their users.[114]

A range of perspectives for why consumers do not provide informed consent to online standard form agreements, one final, convincing perspective offered by Ching suggests when we consent to online standard form agreements, we consent to pay market price.[115] Market price is the public's acceptance of a level of privacy. Through this perspective, there is a need for education that raises the acceptable standard of online standard form agreements and brings the level of groupthink to a standard that rejects unfair and unfavourable online standard form agreements.

---

[109] Bagchi (n 7).
[110] Ibid.
[111] ACCC (n 6).
[112] Cofone and Robertson (n 82).
[113] Ching (n 5).
[114] ACCC (n 6).
[115] Ching (n 5).

4.5.4 Social perspectives

The need to protect an individual's right to privacy can be derived from the basic values of autonomy and human dignity.[116] It is clear from the legal analysis that social values impact the significance of informed consent in online standard form agreements. For example, the European approach places the utmost importance on the fundamental rights of the contracting party in determining whether to enforce an agreement. In Australia, it is evident that fundamental rights are a secondary concern behind economic considerations and the efficient functioning of markets from the perspective of the corporation. This is unsurprising as Australia's regulatory regime is more typically devised through an economic lens.

There is a disconnect between consumer expectations of the way in which they their information and privacy preference are being treated by organisations. The organisational failure to honour consumer expectations leads to a breach of trust and the social contract being violated.

Finally, privacy is a social good, with the value of privacy being subjective and determined through the perspective of privacy as a final good or privacy as an intermediate good (advantages of keeping things private).[117] Through the analysis of approaches to regulation of online standard form agreements in different jurisdictions, it is evident that privacy is context specific and heterogenous.

4.6 Unconscionability and unfairness

In common law, a vitiating factor is something that affects the validity of a contract. It spoils the contract, rendering it imperfect. When a vitiating factor is present, the contract is generally rescinded, and damages may be available. Throughout this chapter, arguments have been presented that demonstrate the unfairness and unconscionability of terms included in online standard form agreements and the obvious lack of informed consumer consent to these agreements. Despite the presence of these vitiating elements, the agreements are routinely enforced.

According to the *ACL*, a term of a consumer contract is unfair if it:

- would cause a significant imbalance in the parties' rights and obligations arising under the contract;
- is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by the term; and
- would cause detriment (whether financial or otherwise) to a party if it were to be applied or relied on.[118]

In determining if a term is unfair, the transparency of the term and impact of the term on the contract as a whole is taken into consideration. If a term incorporated into a standard form agreement is believed to be unfair, they can apply to have the term declared unfair and thus void. It is important to note, however, that provided the remainder of the contract can continue without the void term, it will continue to be enforceable.

The doctrine of unconscionability has been described by some scholars as 'the most revolutionary technique' of 'curbing reliance on standard conditions'.[119] Unfortunately, in the context of online standard form agreements in Australia this is far from the experience of consumers.

---

[116] Kerber (n 47).
[117] Kemp and Buckley (n 86).
[118] *ACL*.
[119] McMahon (n 4).

In Australia, the *ACL* prohibits unconscionable conduct. Unconscionable conduct does not have a precise legal definition. It is an evolving concept that has been developed by courts over time. In a general sense, conduct may be unconscionable if it is particularly harsh or oppressive. To be considered unconscionable, conduct must be more than simply unfair—it must be against conscience as judged against the norms of society.

The current regulatory regime in Australia does not penalise businesses that incorporate unfair contract terms into their agreements. Instead, consumers must seek individual redress for any loss that is sustained because of a term in a standard form agreement that is deemed to be unfair. This process is biased and promotes unethical behaviour. The regulatory focus on fairness in the context of online standard form agreements has thus far predominately centred on procedural and not substantive fairness. According to Willet substantive unfairness in online standard form agreements is generally tolerated by the courts, so long as there is transparency in the pre-contractual process (the terms are presented clearly).[120] The experience in the United Kingdom is analogous with the Australian experience. The definition of fairness as outlined in the United Kingdom's Consumer Rights Bill focuses on drawing attention to terms and rights.[121]

In a 2015 report commissioned into Facebook by the Belgian Privacy Commission, it was concluded that Facebook's Statement of Rights and Responsibilities contained a number of terms that did not comply with the EU Unfair Contract Terms Directive ('Directive').[122] The Directive covers all consumer contracts for the supply of goods and services, including 'free' services. Facebook's violations specifically centred on the inclusion and reliance on substantially unfair contract terms.

The same procedural focus is evident in the determination of unconscionability in online standard form agreements. According to Cornelius, procedural unconscionability in online contracting environments is determined by factors such as awareness, agreement, presentation, and meaningful choice.[123] Cornelius builds on the work of Hillman, who argues that digitised contracts procedurally sacrifice consumer rights and that there is an increased likelihood of unconscionability.[124] Procedural unconscionability means looking at how a user or reader might encounter a contract as part of a digital interface and how notions of genuine effort signal to courts a 'reasonable communicativeness' in these spaces.[125]

In the United States, through the application of the doctrine of unconscionability, courts have generally acknowledged the unique position of a consumer online standard form agreements, particularly in instances where the consumer has little education.[126] The doctrine was elaborated in the 1965 United States District of Columbia Circuit court decision *Williams v Walker-Thomas Furniture Co*, where when referring to a standard form agreement concluded in a traditional hard copy form, Judge Wright concluded that the contract encompassed 'an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favourable to the other party'.[127] The decision in this case was to not enforce the unconscionable terms against the non-drafting party. The doctrine as it stood following Judge Wright's decision was that unfairness contained two essential elements. Firstly, that unfairness must not only be present in the substantive terms of the contract and secondly that there must also be a degree of unfairness in the contract

---

[120] Willet (n 48).
[121] Section 64 of the Consumer Rights Bill states that terms must be both transparent and prominent.
[122] Brendan van Alsenoy et al, *From Social Media Service to Advertising Network. A Critical Analysis of Facebook's Revised Policies and Terms V1.3* (2015).
[123] Cornelius (n 23).
[124] Ibid.
[125] Ibid.
[126] '*Williams v. Walker-Thomas Furniture Co.*, 350 F. 2d 445' (1965) https://h2o.law.harvard.edu/collages/45189.
[127] Ibid.

formation process. Unfortunately, in the decades since this judgment, courts have tended to focus on either procedural or substantive unfairness, not both. This is a mistake.

In its present form, the 'unconscionableness' test in the United States is analogous to the 'reasonableness and fairness' test outlined in the United Kingdom's Consumer Rights Bill. Whereby, both tests specifically focus on drawing the assenting parties' attention to the terms in a transparent way. The directives and regulation addressing unconscionability in the United Kingdom, United States and Australia are accompanied by a list of non-exhaustive examples of unfair behaviour. Some of these examples focus on procedural issues, such as conditions under which contracts can be provided and others focus on the substantive nature of the terms, such as circumstances under which terms can be unilaterally modified.[128]

A focus on substantive unconscionability would instead consider the content of the clauses, including the language used and format of the agreement, the consumer's level of education, and the nature of the contract itself – as an agreement that is presented on a 'take-it-or-leave-it' basis.

4.7 Conclusion

There are many possible explanations for why courts and regulators look the other way when it comes to recognising substantive unfairness and unconscionability in online standard form agreements. In this chapter, the legal, economic, behavioural and social dynamics of informed consent have been unpacked and discussed in the context of the Australian marketplace.

In Australia, the focus on procedural unfairness and procedural unconscionability as threshold requirements have prevented the notion of informed consent from voiding particular terms. As long as there was notice and an opportunity to read, for regulators in Australia, the actual content of the terms seems to have limited importance. For Kim, procedural unconscionability is a toothless tiger.

The answer is not and never will be to remove standard form agreements. However, in Chapter 6 I set out a series of 'quick wins' and longer-term opportunities for transforming Australia's privacy framework into an internationally recognised standard.

[128] Cornelius (n 23).

KATHARINE KEMP

5. Chapter 5 – Regulation of the use of personal data by data brokers and adtech providers

5.1 Introduction

Many consumers are increasingly concerned about their online privacy, while trust in the way organisations handle personal data is declining.[1] Surveys reveal that consumers often feel they lack real information or choices about how their personal data is collected or used.[2] The majority believe that they should be given options about whether their data is used for purposes other than the original purpose for which it was provided.[3] Most Australian users of digital platforms consider certain practices to be misuses of their personal data, including, when the consumer is not logged in to a service:

- keeping track of the consumer's online behaviour such as the consumer's browsing history, viewing habits or search history;
- creating profiles or enabling targeted advertising; or
- using the information the platform has on the consumer (including from third parties) to show the consumer personalised advertisements.[4]

Considering these expressed attitudes, it is particularly concerning that the data practices consumers find objectionable are in fact commonplace, particularly in the context of data brokerage and adtech services.

An individual consumer's personal data is daily passed between hundreds, sometimes thousands, of firms most consumers have never heard of.[5] This personal data is used for commercial purposes well beyond the purpose for which the consumer originally provided their information.[6] Further, firms collect a large proportion of consumer data without any action or awareness on the part of the consumer, using digital surveillance tools which track individual behaviour online and offline. This profusion of tracking, collection and disclosure is almost entirely invisible to the average consumer.

These data practices are driven by three commercial imperatives in particular. First, firms have increasingly sought to accumulate vast amounts of 'big data', including personal data, for the purposes of applying machine learning to extract new commercial insights from that

---

[1] Office of the Australian Information Commissioner, Australian Government, *Australian Community Attitudes to Privacy Survey 2020* (Report, 2020) 17, 56.
[2] Phuong Nguyen and Lauren Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use & Sharing* (Consumer Policy Research Centre, 2017) 4, 36-38.
[3] Ibid 4, 36-38.
[4] ACCC, *Digital Platforms Inquiry: Final Report* (June 2019) 389-390. Similarly, the Office of the Australian Information Commissioner (n 1) ii, revealed that:
- only 21 percent of Australians were comfortable with targeted advertising based on their online activities; and
- only 17 percent of Australians were comfortable with social networking companies keeping databases of information on their online activity.
[5] See Information Commissioner's Office, United Kingdom, *Update Report into Adtech and Real Time Bidding* (Report, 20 June 2019) 20, on the number of organisations involved in a single adtech transaction. See further Norwegian Consumer Council, *Out of Control: How Consumers are Exploited by the Online Advertising Industry* (Report, 14 January 2020) 14, referring to the 'thousands of interconnected entities' that generally 'do not have any direct relationship with users'.
[6] See section 5.5.2.3 below.

data.[7] Second, many firms seek to create highly detailed, individual consumer profiles for their own marketing purposes, and/or to sell to or exchange with other firms.[8] Third, these consumer profiles and other personal data are used for the purposes of behavioural advertising – which targets marketing on the basis of the individual consumer's behaviour – as well as measuring the outcome of such advertising by tracking the consumer's subsequent behaviour.[9] The competition to gain ever deeper 'insights' and advantages from monitoring, profiling, segmenting and targeting consumers has driven firms to conduct such pervasive collection of personal data that it has been justifiably described as 'surveillance'.[10]

In Australia, the *Privacy Act 1988* (Cth) ('*Privacy Act*') imposes obligations on most of the firms concerned.[11] These obligations apply in respect of 'personal information', as defined under the *Privacy Act*.[12] Among other things, the firm must not deal with an individual's personal information without providing certain notices to the individual; and the firm must not engage in a number of data practices without obtaining the individual's consent.[13] Firms generally justify the uses of personal data outlined above on the basis that the consumers have had notice of, or impliedly consented to, these data practices by virtue of the firm's publication of a privacy policy; and/or that much of the data used does not constitute 'personal information'.

This chapter argues that neither of these justifications should be upheld where, as is commonly the case, the 'consent' is not express, active, clear, unbundled consent and where the data in question relates to a consumer who the firm seeks to address as an individual based on their individual behaviour. At a minimum, legislative clarification should be provided on the meaning of 'consent' and 'personal information' to ensure that individuals are not tracked, profiled and targeted without valid consent.

This chapter proceeds as follows. Part 5.2 explains three key drivers of the vastly increased collection and use of personal data, namely big data mining, consumer profiling, and behavioural advertising (particularly with the use of real-time bidding for advertising inventory). Part 5.3 maps the ecosystem of data brokerage and ad tech businesses which is generally hidden from consumers, by identifying and describing the various actors collecting and disclosing personal data for these purposes, as well as the nature of this data. Part 5.4 explains firms' claims that much of the data in question is not 'personal information' notwithstanding the nature of 'people-based marketing', and argues for amendments to clarify the meaning of 'personal information' under the *Privacy Act*, in light of advances in tracking technology. Part 5.5 explains the deficiencies in the 'consent' that firms claim consumers impliedly give to these data practices and argues for amendments to the *Privacy Act* to clarify the appropriate standard for consent.

---

[7] See, eg, Viktor Mayer-Schönberger and Thomas Ramge, *Reinventing Capitalism in the Age of Big Data* (John Murray, 2018) 77-78, 84-85.
[8] See section 5.2.2 below.
[9] See section 5.2.3 below.
[10] See, eg, John Gilliom and Torin Monahan, *SuperVision: An Introduction to the Surveillance Society* (University of Chicago Press, 2013) 47 ff; Norwegian Consumer Council (n 5) 11; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile, 2019).
[11] See section 5.4.1 below.
[12] See section 5.4.1 below.
[13] See Part 5.4 below.

5.2 Key drivers of increased collection and use of personal data

5.2.1 Big data accumulation and data mining

Over the past decade, firms have been encouraged to accumulate and make use of 'big data'.[14] The goal is to collect large volumes of data from a wide variety of up-to-date and accurate sources, and to subject this data to analysis with the aid of machine learning to reveal insights previously unavailable with much smaller quantities of data from more traditional sources. To this end, many firms have created their own 'data lakes' – a combination of all data collected by a firm, both structured and unstructured, including personal data acquired from third parties – with the intention of making these large datasets accessible for the application of machine learning which will identify trends and attributes and predict future trends to assist the firm in its business strategy.[15] The process of analysing big data with the aid of machine learning to discover new patterns and insights is referred to as 'data mining'.[16]

Among other things, this analysis may reveal strategies for profiling and segmenting customers according to a wide variety of attributes;[17] extracting greater value from existing customers; identifying customers with highest 'lifetime value';[18] improving products or developing new products;[19] and identifying fraud. The drive to accumulate 'big data'[20] for analysis and insights from machine learning has led many firms to track consumers pervasively and collect far more personal data than consumers could reasonably expect.[21]

These big data collections incorporate first party data collected by the firm itself as well as second- and third-party data which the firm collects from other firms.[22] A firm's use of data collected by various other parties greatly decreases the likelihood that the consumer has any awareness of this record or use of their personal information. The huge variety of sources of data pooled together also makes it unlikely that proper notice has been given, or consent

---

[14] See, eg, Productivity Commission, Australian Government, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017); Mayer-Schönberger and Ramge (n 7) 77-78, 84-85; Manyika et al, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (Report, McKinsey Global Institute, May 2011); Jay R Galbraith, 'Organization Design Challenges Resulting from Big Data' (2014) 3 *Journal of Organization Design* 2, 2.

[15] According to Paul Needleman et al, Deloitte, 'Pump Your Own Data: Maximizing the Data Lake Investment' (*Deloitte Insights*, 18 February 2019) https://www2.deloitte.com/us/en/insights/industry/public-sector/chief-data-officer-government-playbook/maximizing-data-lake-investment.html, '[d]ata lakes combine distributed storage with rapid access to data', 'stor[ing] the full spectrum of an enterprise's data' and 'provid[ing] business users with direct access to raw data without significant IT involvement'.

[16] Manyika et al (n 14) 28, defined 'data mining' as '[a] set of techniques to extract patterns from large datasets by combining methods from statistics and machine learning with database management. These techniques include association rule learning, cluster analysis, classification, and regression.'

[17] Ibid 23. See further section 5.3.1 below.

[18] See, eg, Experian 'Customer Management Strategies' https://www.experian.com.au/customer-management

[19] Jay R Galbraith, 'Organization Design Challenges Resulting from Big Data' (2014) 3 *Journal of Organization Design* 2, 7-8.

[20] See, eg, Paul Needleman et al, Deloitte, 'Pump Your Own Data: Maximizing the Data Lake Investment' (Deloitte Insights, 18 February 2019) https://www2.deloitte.com/us/en/insights/industry/public-sector/chief-data-officer-government-playbook/maximizing-data-lake-investment.html.

[21] See Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (Oxford University Press, 2016) 51-58, on consumer preferences and lack of transparency in data practices. On the imperative to accumulate larger pools of data, Derek Wange, 'Why You Don't Need to be a Data Scientist to Reap the Benefits of Big Data' (*Martech Advisor*, 18 October 2019) https://www.martechadvisor.com/articles/marketing-analytics/why-you-dont-need-to-be-a-data-scientist-to-reap-the-benefits-of-big-data-4/?zd_source=editors_pick explains:
'The system needs to be able to learn by acquiring information and rules for using the information. It must then be given rules to reach conclusions and self-correction. Of course, the *larger* the data pool with which to train the system, the better the conclusions and analysis. Large in this instance refers to millions of records or more.'

[22] The terms 'first-', 'second-' and 'third-party data' are explained in section 5.2.2 below.

received, for the planned uses and can be tracked for each data item.[23] The vast range of personal data combined by firms for the purposes of consumer profiling, both from the firm's own collection and from third parties, is explained in the following section.

Another problematic aspect of these big data collections is that, at the time of collection, firms often lack a clear idea of what the data might ultimately be used for. The goal of applying machine learning is to gain insights and identify patterns that could not be identified by human analysts.[24] Accordingly, the firm may only know that they wish to collect, store and analyse the data for some purpose which may emerge in future. In this situation, it is highly unlikely that the firm has adequately informed the consumer of the purposes for which it intends to use that data.[25]

5.2.2 Building consumer profiles and segments

Many firms seeking to attract and retain 'high value' customers compile detailed consumer profiles and segments using various sources of personal data. Firms often refer to this practice as 'customer data management'. For these purposes, firms combine data they themselves collect on consumers from the extensive data collection and tracking outlined above, including email and online chat interactions; customer loyalty scheme data; online and offline purchases; social media; retail beacons;[26] web logs; 'clickstream';[27] and the firm's broader 'data lake'.[28] However, firms also combine their own first party data with second party data from 'data partners' as well as third party data from data brokers. Data brokers are firms that are in the business of collecting, combining, matching, buying and selling personal data collected from other suppliers.[29]

At this point, it is useful to distinguish three categories of data commonly identified in the context of data services, and consumers' likely level of awareness of the data collection and use.

'First party data' refers to data a firm collects about its own customers or consumers who interact directly with its website, service or product. The consumer is likely to be aware that they have had some interaction with the collecting firm, although they may not be aware of

---

[23] See 'Why 'data provenance' will be the New Media-Transparency Issue in 2020' (*Digiday Online*, 30 December 2019) https://digiday.com/marketing/data-provenance-will-new-media-transparency-issue-2020/, on the difficulty of establishing compliance.
[24] See Mayer-Schönberger and Ramge (n 7) 77-78.
[25] See Part 5.5 below.
[26] According to location data broker, Fysical: 'A 'beacon' is a small Bluetooth-enabled device that may be placed in retail stores or other locations which emits a unique signal that our Customers' applications can detect.' https://fysical.com/privacypolicy/enduser/index.html accessed 3 March 2020.
[27] 'Click stream' refers to a list of URLs visited by the user.
[28] 'Data lakes' are defined in section 5.2.1 above. Data analyst, Amperity's process is explained as follows by Slalom & Amperity, 'Slalom Consulting provisions a Customer Data and Identity Platform Powered by Amperity' https://appsource.microsoft.com/en-cy/product/web-apps/amperity.amperity_slalom_cdp?tab=overview : 'Amperity's solution begins by ingesting all your customer data in its native format from every source – online, offline, historical and streaming – no schema planning or extract-transform-load (ETL) required. Next, proprietary machine learning algorithms probabilistically and deterministically resolve customer identities across records even when data is incomplete, inconsistent, and lacks linking keys. Then all behavioral, contextual, and transactional data is merged to form actionable customer 360 views with out-of-the-box attributes, affinities, and insights.'
[29] See Nico Neumann et al, 'How Effective is Third-Party Consumer Profiling and Audience Delivery? Evidence from Field Studies' (Working Paper, Forthcoming in *Marketing Science-Frontiers*, 12 June 2019) 2. CoreLogic, a data broker, enjoins businesses to '[m]ake sure you are collecting all the data you can about your customers and their behaviours, make sure you can store and link it to internal and external data to create insights, and most important know how you can use those insights to get better at service and at pro-actively meeting your customers' needs. If you aren't, someone else will.' https://www.corelogic.com.au/resources/are-you-data-smart

the *extent* of the data collection, particularly where the firm tracks the consumer's behaviour over time, for example, by placing a cookie on the consumer's device.

'Second party data' refers to data a firm acquires from a second firm where that data constitutes first party data of the second firm, for example, in the context of a 'data partnership' under which the two firms agree to disclose their first party data to each other.[30] In this case, the consumer is likely to be aware that they have had some interaction with the second firm, although they may not be aware of the extent of the data collection or the fact that the collecting firm is disclosing that data to other firms.

'Third party data' refers to consumer data a firm acquires from a second firm, where the second firm did not have a relationship with the consumer themselves. For example, the second firm may be a data broker that has collected second party data from a large number of other firms and public sources, as well as placing cookies on the consumer's devices when the consumer accesses another firm's website ('third party cookies').[31] The consumer is unlikely to be aware of the existence of the third party or the third party's aggregation of the consumer's personal information.

5.2.3 Behavioural advertising and real-time bidding

5.2.3.1 Actors in behavioural advertising

A key driver of the vastly increased exposure of personal data, and consumer profiling in particular, is behavioural advertising. Behavioural advertising makes use of consumer profiles and other data about a consumer's online and offline behaviour to target marketing. The behavioural advertising transaction involves:

- a **publisher** who sells advertising opportunities ('ad inventory') and publishes the advertisement to its audience, for example, on its website, app, podcast, or programmatic television;
- a **marketer** who purchases the opportunity to market its product to the consumer by displaying an advertisement on that site, and thus seeks to gain, retain, or increase its profit from, customers; and
- the **consumer** who visits the site where the advertisement is displayed, and whose behaviour is often tracked before and after this display. The consumer is both a member of the publishers' audience and an actual or potential customer of the marketer.

This advertising transaction is frequently conducted with the assistance of a number of **third party 'adtech' vendors** who aim to facilitate the purchase and/or sale of ad inventory; finer targeting of consumers; and the measurement and attribution of the consumer's behaviour following the advertisement. In so doing, each vendor takes a cut of the advertising expenditure and frequently collects and discloses consumers' personal data.

These vendors are third parties in the sense that they are neither the publisher selling the ad inventory nor the marketer purchasing the advertising opportunity. These include supply side platforms; ad exchanges; demand side platforms; and ad verification, attribution and measurement providers. Data brokers, data analysts, and data management platforms also provide data services which contribute to these transactions.

---

[30] See Quantcast, 'Big Data Advertising for Branding' (2016) 8. Cf Matthew J Schneider et al, 'Protecting Customer Privacy When Marketing with Second-Party Data' (2017) 34 *International Journal of Research in Marketing* 593, 593-594, who define 'second-party data' as the combination of the first-party data of two or more firms. See further the description of data partnerships via 'data management platforms' in section 5.3.1 below.
[31] Data brokerage is explained in section 5.3.1 below.

Although the average consumer is unlikely to recognise the name of any of these entities as adtech vendors, their personal data may be handled by thousands of them.[32] Adtech businesses often compete to provide publishers and marketers with services on the basis of: the number of consumers they profile (generally numbering in the millions); the accuracy with which they can identify individual consumers; and the level of detail and real-time information their consumer profiles contain.

5.2.3.2 The debatable advantages of behavioural advertising

Numerous services provided by data brokers and adtech vendors are designed to support a particular type of advertising, namely behavioural advertising. Behavioural advertising purports to use data about consumers' past behaviour to match the relevant advertisement to an individual who is likely to respond to that advertisement. As such, it is promoted as highly efficient on the basis that it reduces wasted advertising expenditure and consumer search costs.[33] However, as discussed later in this section, a number of stakeholders have expressed growing misgivings about the superiority of behavioural advertising.

Behavioural advertising can be contrasted with more traditional **broadcast advertising**. Broadcast advertising displays the same advertisements to all members of a wider audience – everyone watching a certain television channel or listening to a particular radio station – even though a large percentage of that audience will have little interest in the product in question and little prospect of buying it in the near future. For example, all viewers of the six o'clock news will be shown the same advertisement for discount power tools. Broadcast advertising may result in a substantial proportion of wasted advertising expenditure due to the large number of mismatched consumers: those viewers of the six o'clock news who have no interest in power tools, for example.

Behavioural advertising can also be distinguished from **contextual advertising**, which changes the advertisement displayed based on the immediate context of the app or website interaction.[34] In the digital context, for example, when a person enters 'meal replacement shakes' in a search engine, the search results page may display contextual advertisements for protein shakes, weight loss programs and fitness accessories. When a person browses a trail running blog, the blog webpage may display contextual advertisements for trail running shoes and camping holidays. Contextual advertising improves efficiency by selecting the advertisement to be displayed based on inferences that can be made about the consumer's interests from the short-term interaction.[35]

Behavioural advertising, on the other hand, selects the advertisement displayed based on the profile of the individual who is believed to be watching that advertisement, or a segment of consumers to which that individual has been allocated. That profile or segmentation is in turn based on the assumed interests and characteristics of the person in question, which are inferred from that person's behaviour online (and sometimes offline) over time.[36] For example, if a person has been browsing the 'for sale' section of an online real estate

---

[32] See Information Commissioner's Office (n 5) 20, on the number of organisations involved in a single transaction. See further Norwegian Consumer Council (n 5) 14, referring to the 'thousands of interconnected entities' that generally 'do not have any direct relationship with users'.
[33] See Katherine J Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' (2013) *University of Chicago Legal Forum* 95, 102-105. Cf Omid Rafieian and Hema Yoganarasimhan, *Targeting and Privacy in Mobile Advertising* (Working Paper, 30 January 2020), arguing that contextual advertising may be more effective than behavioural advertising.
[34] Katherine J Strandburg, 'Free Fall: The Online Market's Consumer Preference Disconnect' (2013) *University of Chicago Legal Forum* 95, 99.
[35] See Omid Rafieian and Hema Yoganarasimhan, 'Targeting and Privacy in Mobile Advertising' (Working Paper, 30 January 2020), arguing that contextual advertising may be more effective than behavioural.
[36] See Norwegian Consumer Council (n 5) 102.

platform and using the interest rate calculator on their bank's website, the person may be shown advertisements for home loans while browsing the weather website.

Behavioural advertising can also be more significantly more subtle and manipulative.[37] For example, an online profile developed about a consumer could reveal that the consumer is female, between 17 and 19 years old, has read online articles about how to use make-up to diminish nose size, and interacts with social media in a way that reveals she tends to feel most depressed and unattractive on Monday mornings.[38] This information could be used to target young women with a similar profile with advertisements for cosmetic procedures at the start of the week. Alternatively, consumers who have searched for 'chronic pain management' in a search engine may be shown pharmaceutical advertisements for dangerous opioids with escalating messages on various other websites they visit.[39]

Behavioural advertising relies on far greater collection, use and storage of personal data than contextual or traditional advertising, since it depends on profiling and targeting consumers based on data about their past behaviour and not merely their immediate interaction with the publisher.[40] Publishers and marketers often refer to behavioural advertising as 'interest-based advertising' or 'personalised advertising' and state that they 'provide' consumers with this tailored advertising.[41] However, since the advertising is chosen and paid for by marketers interacting with publishers without input from the relevant consumer, this cannot seriously be viewed as a service provided to consumers.

Notwithstanding the claims made regarding the efficiency of behavioural advertising, strong doubts have been raised about its superiority relative to contextual advertising in particular. Research suggests that, for publishers, there may be very little increase in revenue from behavioural, as opposed to contextual advertising.[42] Publishers also complain of the degradation of high quality online content when audience targeting, rather than content quality, becomes the focus.[43] Marketers have complained of a general lack of transparency in the adtech supply chain; unacceptable levels of ad fraud; and the wastefulness of the 'adtech tax' claimed by the numerous third-party vendors in the programmatic, behavioural advertising supply chain.[44]

Behavioural advertising has also given rise to an ever-increasing number of firms relying on vague, opaque terms in lengthy privacy policies to broadly use and disclose personal data for commercial gain, without the knowledge of consumers.[45]

---

[37] See, eg, Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy and Manipulation' (2019) 8 *Internet Policy Review* (forthcoming); Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995.

[38] See Lucia Moses, 'Data Points: Talk to Her' (*Adweek*, September 2013) 16, identifying that '[w]omen feel ugliest on Mondays and weekends', as well as 'The Top 5 occasions when women feel least attractive'.

[39] See Alison Branley, 'Google Search Data Used by Pharma Giant to Bombard Users with Ads for Addictive Opioids' (*ABC Online*, 13 July 2019).

[40] See George J Stigler Center for the Study of the Economy and the State and The University of Chicago Booth School of Business, *Stigler Committee on Digital Platforms Final Report* (September 2019) ('Stigler Report') 44-45.

[41] See, eg, Google Privacy Policy, which lists as one of the purposes for which it uses consumers' personal data: 'Provide personalised services, including content and ads'.

[42] See, eg, Veronica Marotta, Vibhanshu Abhishek and Alessandro Acquisti, 'Online Tracking and Publishers' Revenues: An Empirical Analysis' (*Preliminary Draft*, May 2019).

[43] Joseph Turow, *The Daily You: How the New Advertising is Defining Your Identity and Your Worth* (Yale University Press, 2011) 84-86.

[44] Ibid 84; Stigler Report (n 40) 61-63; Ivan Guzenko, 'How Programmatic Evolved Within 8 Years' (*Martech Advisor online*, 7 November 2019): 'Programmatic chains may disclose little to no information regarding what part of the impression cost reaches the publisher after service commissions and margins are subtracted from the total sum.'

[45] Explained in Part 5.4 below.

Lack of transparency about the cost of, value added by, and data flows required by ad tech services in the supply of behavioural advertising hinders the introduction of privacy preserving subscription models for online content, as well as privacy preserving methods of targeted advertising, such as those based on data which does not leave the consumer's browser.[46] This lack of transparency also makes the question of whether contextual advertising has comparable or superior welfare effects more difficult to answer.[47]

5.2.3.3 Programmatic advertising and real-time bidding

A large proportion of digital behavioural advertising takes the form of **programmatic advertising**. The advertising is programmatic in the sense that it is automated: a significant part of the advertising transaction is performed by algorithms, rather than directly negotiated by humans.

Some programmatic advertising takes the form of a direct deal negotiated between the publisher and marketer for a certain period of time. In other cases, programmatic advertising is purchased by 'real-time bidding', an algorithmic auction involving a number of third-party adtech vendors.[48]

The essence of the **real-time bidding process ('RTB')** is as follows.[49] When a consumer uses an app or browses a website, the publisher has an opportunity to sell certain advertising space. While the web page or app is loading, an automated auction takes place to determine which marketer will have the right to place an advertisement in each of the available advertising spaces and at what price. A similar process may take place when a consumer listens to a podcast, or views a program on a connected television.

The publisher broadcasts a bid request and ultimately selects a winning bid from the numerous marketers who respond to the bid request. In the process, the publisher sends data about the consumer to various marketers and third-party adtech vendors, allowing these firms to match the consumer visiting the website or app with other existing data on the consumer for the purposes of matching an advertisement to that visit.[50] For example, some marketers may only be willing to bid for advertising inventory where the consumer is male, aged between 18 and 25, with an interest in Mardi Gras events; or a female, aged over 50, with an interest in incontinence products.

5.3 Actors and data

5.3.1 Data brokerage, data management and data analytics

This section explains the services provided by firms that sell, exchange, manage, analyse and/or 'enhance' data, including consumers' personal data, for other firms. These include data brokers, location data brokers, data management platforms and data analytics

---

[46] See, eg, Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum and Solon Barocas, 'Adnostic: Privacy Preserving Targeted Advertising' (*Network and Distributed System Symposium*, March 2010).
[47] See generally Katharine Kemp, *Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper* (26 April 2020).
[48] See Interactive Advertising Bureau (IAB), *Programmatic 101 for Direct Sellers* (2014), defining 'programmatic' advertising as 'the process of executing media buys in an automated fashion through digital platforms such as exchanges, trading desks and demand- side platforms'. Aside from the sale of ad inventory via auctions, programmatic advertising can also take the form of 'automatic guaranteed' and 'preferred deals', both of which are automated and receive priority over purchases of ad inventory via auction.
[49] See further Information Commissioner's Office (n 5) 5, 8. Other programmatic advertising takes the form of 'direct deals' between a publisher and a marketer, without an auction process.
[50] This matching is often performed without reference to the consumer's name, but through the use of other identifiers including device identifiers; advertising identifiers; encrypted email addresses; and other unique identifiers, as explained in section 5.4.2 below. The disclosure of consumers' personal data in the ad tech supply chain is explained in section 5.3.2 below.

providers. While these services are each explained in turn, a number of firms provide combinations of these services and/or further adtech services. Adtech services are described separately in section 5.3.2, since data collection or disclosure tends to be incidental to these services, rather than the core product.

Data brokers specialise in the collection of enormous amounts of personal data about consumers from a variety of online and offline sources which the data broker combines for the purposes of providing services to other firms. Data brokers do not generally collect this personal information from the consumer themselves, but from various other firms and sources.[51] Examples of data brokers in Australia include Quantium, Acxiom, Adobe, Datalogix, Equifax, Experian, Eyeota and LiveRamp.

Services provided by data brokers include:

- marketing (including consumer profiling and segmenting for behavioural advertising);
- consumer behaviour analytics;
- people search;
- identity verification;
- employee screening;[52]
- fraud detection; and
- credit scoring.

Data brokers' sources of information are extensive, incorporating online and offline data on consumer characteristics and behaviour.[53] Sources of data collected and combined by data brokers may include:

- data purchased from other data brokers;
- customer loyalty scheme data;[54]
- online and offline purchase history;
- online search history;
- online browsing history and browsing behaviour, including hovering, scroll speed and clicking;
- email communications and online chats;
- social media data, including posts, comments, connections, profile information, reactions, employers and positions with employers;
- apps installed and app usage, including frequency and duration of use, device location, and biometric data recorded by the app;
- location data, including GPS, wifi, IP address, Bluetooth;
- consumer survey responses and online 'quiz' or 'personality test' responses;
- 'guest wifi' history;
- internet of things (IoT) logs, for example, from digital personal assistants, smart televisions, smart fridges, smart thermostats;[55]
- wearable devices, such as 'smart watches' and fitness devices;
- unique identifiers associated with the consumers' collection of devices, including advertising identifiers (eg Android advertising identifier), IP addresses, mobile device

---

[51] See Norwegian Consumer Council (n 5) 19.
[52] For example, data broker Equifax has an employee screening subsidiary, fit2work, which promises: 'As part of Workforce Management Solutions, fit2work has access to Equifax unique credit and financial data sets and a full suite of human resource and onboarding solutions.' https://www.equifax.com.au/fit2work/about-us
[53] See, eg, Epsilon Privacy Policy, cl 1. https://us.epsilon.com/privacy-policy
[54] See ACCC, *Customer Loyalty Schemes: Final Report* (December 2019) 51-53, 67-73.
[55] See Lipi Khandelwal, 'What is Customer Analytics? Definition, Process, Key Trends and Examples' (26 May 2020) https://www.martechadvisor.com/articles/data-management/what-is-customer-analytics/ accessed 31 March 2021

identifiers, cookie identifiers and 'device fingerprinting'[56] information such as device type, browser, operating system, apps, screen resolution;
- publicly available census data, electoral rolls, property records and court records (including family proceedings); and
- credit information, including loan applications, loan repayment histories, loan defaults.

This aggregation of personal data becomes even more concentrated when data businesses acquire other data businesses.[57] For example, when the Publicis Group acquired the international data broker Epsilon in 2019, it was reported that:[58]

> the connection between Epsilons data sets and Publicis Medias 'billions of touchpoints' will provide 'superior intelligence' to build consumer IDs, segment audiences and maximise media buying ROI by measuring and optimising campaigns in real time.

All these sources of information can be combined to create a highly detailed profile of an individual. Data brokers often market their ability to provide a 'single customer view' or a '360 view' of individual consumers.[59]

The consumer profile may include, or permit inferences about, the consumer's age, gender, relationship status, pregnancy, children, income, health issues, financial position, property ownership, purchasing intentions, sexual orientation, sexual activity, drug use, alcohol consumption, psychological biases, political views, religious affiliations, ethnicity, consumption preferences and personality predictions. The goal is to make the individual consumer as transparent as possible for commercial gain.[60]

---

[56] Norwegian Consumer Council (n 5) 116.
[57] See ibid 100, on Foursquare's purchase of the Placed location data broker from Snapchat.
[58] Josh McDonnell, 'Publicis acquires Epsilon for $3.95bn' (*AdNews online*, 15 April 2019) https://www.adnews.com.au/news/publicis-acquires-epsilon-for-3-95bn accessed 31 March 2021
[59] See also Amperity, 'Learn How AI is the Key to Unifying All Your Disparate Customer Data: Guide' (Amperity website) https://amperity.com/resources/whitepaper/intelligent-identity-resolution accessed 31 March 2021, promising:
'You'll also learn how Amperity helps brands: Circumvent arduous data preparation; Combine diverse data sets at massive scale including historical data sets; Deliver truly comprehensive 360 views from previously impossible-to-connect data sources'.
Adobe, 'Adobe Audience Manager' (Adobe website) https://www.adobe.com/au/analytics/audience-manager/audience-insights.html accessed 31 March 2021, states:
'[T]he quality of the insight is based on the quality of the data. Often times, that data is incomplete. But when you can merge together all your audience data from browser cookies to customer IDs and fill in the gaps with third-party data, you'll have one of the key components for better insights — the coveted 360-degree view of your customer.'
The data broker Epsilon promises that it can "[c]onnect billions of online and offline intent signals with predictive AI to know what each person really wants, then deliver personalized messaging to them at the moment they're ready to act": Epsilon, 'Success in Three Steps' (Epsilon website) https://www.epsilon.com/us/products-and-services/epsilon-peoplecloud accessed 31 March 2021.
[60] Neil M Richards and Jonathan H King, 'Three Paradoxes of Big Data' (2013) 66 *Stanford Law Review Online* 41, 42-43, refer to the 'transparency paradox'. Lipi Khandelwal, 'What is Customer Analytics? Definition, Process, Key Trends and Examples' (26 May 2020) https://www.martechadvisor.com/articles/data-management/what-is-customer-analytics/ accessed 31 March 2021 states:
'Specifically [sic] for customer data, organizing it is also about building complete, unified profiles of individual customers or segments. In case of first party data for martech applications, this would involve processes such as probabilistic or deterministic identity resolution, building identity graphs, 360-profiles of customers and integrating consent into customer data, to ensure compliance.'
Acxiom's former managing director, Esther Carlsen, described the company's data broking business as 'the connective tissue' between advertisers, agencies and tech platforms, tying 'all the different customer data points back together to one identity': Lindsay Bennett, 'Esther Carlsen on her next move at Acxiom' (AdNews online, 31 May 2018) https://www.adnews.com.au/news/esther-carlsen-on-her-next-move-at-acxiom accessed 31 March 2021

Data brokers market their services by highlighting the large number of consumers tracked by their databases and the detailed and comprehensive information collected on each consumer. For instance, Consumer Lens by Equifax offers marketing and analytics services to business customers, promising 'rich demographic, behavioural and lifestyle profiles on 16 million Australian adults', with 'more than 40+ descriptive and predictive attributes' including '[p]ropensity to be in market for home loans, credit cards or personal loans'.[61]

Experian, another data broker, promised that it could:

> Enrich your existing database with demographic, consumption or attitudinal information. Use Experians consumer data to infill missing information and gain additional insight into your customers. Use Lifestage to understand your customers family and household circumstances, or Children at Address to predict the likelihood of the presence of children at the address.
>
> Containing over 500 variables, segmentations and propensities, Experians consumer data is unique in its breadth and depth, the inclusion of a market leading demographic segmentation (Mosaic) and its ability to link offline and online data. ConsumerView is refreshed constantly, ensuring that it accurately reflects the universe of Australian consumers at any point in time.[62]

In addition to profiling, brokers may create consumer segments or 'audiences' based on attributes, interests and purchasing intentions. Given that brokers and their clients do not publish this information to consumers, it is highly unlikely that the consumers included in these lists or segments are aware of this, or the fact that their inclusion might work to their disadvantage.

In 2013, the US Federal Trade Commission (FTC) investigated the practices of data brokers in the United States, which permitted the FTC to compel nine data brokerage firms to provide the FTC with information about how the firms collect and use information about consumers. In its final report, the FTC identified many segments to which data brokers allocated individual consumers, including:

- 'Leans Left';
- 'Allergy Sufferer';
- 'Financially Challenged';
- 'Plus-size Apparel';
- 'Bible Lifestyle'; and
- 'Bikers/Hells' Angels'.[63]

A similar investigation into the profiling and segmentation practices of data brokers has not been conducted in Australia, but some data brokers' segmentation categories are publicly available through websites targeted at marketers seeking data services. For instance, Quantium promises its marketing customers audience segments, or 'Q Crowds', that include:

- 'Suburban Thrift';
- 'Neighbours with Kids';
- 'Countryside Elite'; and
- 'Affluent Adventurers'.[64]

---

[61] Equifax, 'Data-Driven Marketing: Consumer Lens' (Equifax website) https://www.equifax.com.au/datadrivenmarketing/what-we-do/our-data/consumer-lens accessed 31 March 2021

[62] Experian 'Customer Insight' (Experian website) https://www.experian.com.au/customer-insight accessed 2 March 2020

[63] Federal Trade Commission, United States, 'Data Brokers: A Call for Transparency and Accountability' (*Report*, May 2014) 20-21.

[64] Quantium, 'Q.Segments Crowds Brochure' (Quantium website) https://quantium.com/wp-content/uploads/2018/10/Q.Segments_Crowds_brochure_2018_V3.pdf accessed 31 March 2021.

Quantium advertises its ability to reflect the real behaviour of 80 percent of Australian households based on transaction data from a major bank and a grocery loyalty program, namely NAB and Woolworths Rewards.[65] It emphasises that it allows customers to reach 'the people who matter' rather than 'devices that behave like them':

> Australia's first lifestyle segmentation based entirely on real-world people and their realworld transactions. Crowds group Australian consumers into 15 distinct segments, blending millions of lifestyle and purchase data points with Quantium's rich insight and analytical heritage. While others rely on recall, sampling, website interests and postcode mapping, Crowds deterministic match gives your clients the confidence in knowing they are reaching the people who matter, not devices that behave like them.[66]

Several other customer loyalty programs feed data about consumers' individual behaviour to data broker businesses, sometimes combining data from a number of loyalty programs. Datalogix (operated by Oracle) has gathered data on consumer spending 'thanks to collection of data from loyalty programs'. It claims to 'provide marketers and publishers with the richest understanding of consumers across both digital and traditional channels based on what they do, what they say, and what they buy' enabling marketers 'to personalize and measure every customer interaction'.[67]

Red Planet, the data broker which is part of the Qantas group of companies, draws on data from Qantas Frequent Flyer members,[68] and tells prospective data clients that:

> We connect with millions of Australians, as we have hundreds of data fields about their interests, values, lifestyle and so much more.[69]

Red Planet has also promised marketing customers that it could match the customers' website visitors – both those who are known to the customer and those who are not – with 'our databased of online Australians' to 'uncover insights behind the clicks'.[70]

Location data brokers are a specialist category of data brokers, which focus particularly on collecting and combining information about a consumer's location data and movements for the purposes of selling detailed location histories to other firms.[71] Location data is now sufficiently varied and precise that it can permit a consumer to be tracked indoors to the specific floor of a building.[72] Individual location histories can reveal daily routines, interests, likely medical treatments, religious and political affiliations, and likely purchase intentions, among other things. Other data brokers also use location data to add to the broader profile on a certain consumer, for the purposes of permitting further inferences about that consumer.

Data management platforms aim to permit firms to organise and combine data to create more detailed consumer profiles and/or gain greater insights into consumer behaviours

---

[65] Ibid.
[66] Ibid.
[67] Emphasis added.
[68] On earlier versions of its website, Red Planet explained that 'Red Planet is a customer-insights and marketing business that leverages nearly 30 years of experience from Qantas Frequent Flyer in order to help organisations better understand their customers, and engage with them. With millions of insights on millions of Australian consumers, Red Planet offers integrated, end-to-end solutions that enable you to create valuable relationships with your audiences – at scale – through actionable, data-driven insights.'
[69] Red Planet, 'People, not numbers' (Red Planet website) https://www.redplanetgroup.com.au/ accessed 31 March 2021.
[70] Ibid, accessed 3 March 2020.
'By matching website visitors, you know, and those you don't, with our database of online Australians, we can help you uncover insights behind the clicks. We can also help you discover the factors that influence these visitors, so you can better tailor your content.'
[71] Near and Safegraph are examples of location data brokers.
[72] Norwegian Consumer Council (n 5) 96.

individually or in aggregate.[73] While many large firms have *internal* data management platforms that perform these functions, this is also offered as an external service by third party service providers.[74]

In the case of external data management platforms, the service often promises that firms can use the platform to *add* information to their customer databases using customer data from other firms or to form 'data partnerships' with other firms. This could include publishers and marketers combining data on their existing customers with second party data or data from third party vendors, linking profiles on individual consumers across different contexts and devices.[75]

Data Republic, for example, advertises itself as a data management platform that, in part, allows firms to 'enrich' their customer databases. According to its website, Data Republic permits companies to enhance their existing consumer profiles using data from the customer data of other companies and to '[m]atch datasets'.

Data analytics is a service offered by numerous data brokers, which can also be offered as a stand-alone service by specialist firms that do not collect and combine data themselves.[76] Data analysis may be conducted, for example, to aid in segmenting, targeting, determining 'customer lifetime value', predicting personal attributes or purchasing behaviour and campaign measurement.[77]

5.3.2 Adtech third-party vendors

Throughout the adtech supply chain, personal data is collected by and disclosed to numerous firms. These firms use the personal data to facilitate the ad placement but often retain that personal data for other purposes, including the creation of more detailed consumer profiles, feeding into the goals of big data accumulation and consumer profiling.[78]

Third-party vendors in the adtech supply chain focus on facilitating and adding value to programmatic advertising transactions. They are third parties in the sense that they are neither the publisher selling the ad inventory nor the marketer purchasing the advertising opportunity. Instead these vendors provide services intended to match advertisements to the consumers most likely to make a purchase; aggregate purchasing and selling of ad inventory to benefit from economies of scale; and gauge the success of advertising by measuring and attributing consumers' subsequent behaviour. In so doing, these vendors each take a cut of advertising expenditure and frequently collect and disclose consumers' personal data.

It is not possible to categorise the adtech third-party vendors according to the services they provide since a single firm may perform several of these functions in various combinations. This section therefore describes various key functions performed by third party vendors, and the types of data collected and disclosed, rather than suggesting fixed categories of service providers. The special case of major platforms, which integrate a number of these functions internally, is explained further in the section 5.3.3 below.

---

[73] See ACCC, *Ad Tech Inquiry: Issues Paper* (10 March 2020) 13.
[74] Data management platforms include LiveRamp, Data Republic, Adobe Audience Manager, Lotame, Salesforce DMP, Oracle BlueKai.
[75] Norwegian Consumer Council (n 5) 37.
[76] Evidon, Google Analytics, Adobe Analytics and Tapad are examples of data analytics providers.
[77] See ACCC *Ad Tech Inquiry* (n 73) 13. Data may include website traffic data and conversion data.
[78] Norwegian Consumer Council (n 5) 39.

Supply side platforms (SSPs) act on behalf of publishers to manage their ad inventory and optimize the price received for that inventory.[79] SSPs make the advertising opportunities on the publisher's app or website known to potential marketers by aggregating the advertising opportunities of various publishers. Each publisher may, in turn, license several SSPs to act on their behalf.

When an ad is about to be loaded on an app or website, the SSP may facilitate the broadcast of a bid request on behalf of the publisher. The bid request can incorporate data about the person and/or device loading the app or website, which may include the URL of the website, device information (including brand, model and operating system), the consumer's location, the consumer's IP address, profile data compiled by data brokers, app usage, and/or other unique identifiers or profile information that allow marketers to determine whether they wish to bid for that ad placement.[80]

The personal data transmitted by the SSP as part of the bid request can be very revealing.[81] For example, the Norwegian Consumer Council has pointed out that a person's use of the Grindr app 'is in itself a strong indicator of sexual preferences, as the app is geared toward homosexual, bisexual, and trans people'.[82] The UK ICO noted that information included in the bid request may include categories such as 'Heart and Cardiovascular Diseases', 'Mental Health', 'Sexual Health', 'Infectious Diseases', 'Reproductive Health', 'Substance Abuse', 'Health Conditions', 'Politics' and 'Ethnic & Identity Groups'.[83]

The bid request is generally broadcast to various demand side platforms and other adtech players.

Demand side platforms (DSPs) act on behalf of marketers to assist with advertising campaigns, receive bid requests and allow marketers to bid in real-time for ad placements on publisher apps or websites.[84] Using a DSP also gives a marketer access to a wide range of advertising inventory without needing to make contact with the numerous publishers.

On receiving the bid request, DSPs and other third-party vendors wish to determine which marketers will be most interested in the relevant consumer for behavioural advertising purposes. To do this, they may seek to identify the consumer more closely by a process of 'ID syncing' or 'ID mapping'. Essentially, various third-party vendors may already have data associated with the relevant consumer which they have received via their own third-party cookie[85] placed on the consumer's device. ID syncing or mapping synchronises the various pseudonymous identifiers the third-party vendors respectively associate with that particular consumer via their own cookies, allowing the vendors to identify the relevant consumer in their own databases.

---

[79] SSP services are, eg, provided by MoPub, Google Ad Manager, OpenX, AppNexus, Rubicon Project and PubMatic.

[80] See Norwegian Consumer Council (n 5) 36-37, 55-59; Information Commissioner's Office (n 5) 12-13. According to the ICO, this further information can include the consumer's online activity (scrolling, clicking, highlights, media views), search queries, session time and demographic data: at 13.

[81] Norwegian Consumer Council (n 5) 36, 55-59.

[82] Ibid 123.

[83] Information Commissioner's Office(n 5) 13.

[84] DSP services are, eg, provided by DataXu, Rocket Fuel, adcash, AppNexus, SmartyAds, DoubleClick Bid Manager, Simplifi, The Trade Desk, MediaMath and Amazon DSP.

[85] Cookies are small text files placed on a consumer's device which allow the originator of the cookie to retrieve information about the consumer which is stored in that text file over time. A third-party cookie is a cookie that originates from a party other than the operator of the website which the consumer is visiting. These are also referred to as 'tracking' or 'targeting' cookies. See further section 5.4.4 below on the 'death' of the third-party cookie.

The data contained in the bid request is used by the DSPs to determine whether a particular marketer should place a bid, but it may also be retained by third-party vendors, including data brokers, to add to existing consumer profiles.

Ad networks also facilitate the sale of publishers' ad inventory. They collect digital ad inventory from numerous publishers, add a margin and sell packages of this ad inventory to marketers.

In the earlier days of ad networks, the networks tended to buy the unsold inventory of publishers and sell it at a discount.[86] More recently, however, ad networks have concentrated on acquiring and marketing 'premium' advertising inventory. Ad networks may hold detailed profiles on large numbers of consumers which allow the networks to promise marketers the ability to target consumers who have specific characteristics via particular publishers.[87]

An **ad exchange** may sit between publishers and marketers, or between SSPs or ad networks and DSPs (although a number of SSPs now incorporate an ad exchange in their own services).[88] The ad exchange provides a central platform or market for the automated buying and selling of ad placements.[89] The transactions take place through the real-time bidding process, where the ad exchange automatically receives offers of ad inventory (bid requests) from supplier websites via SSPs. Meanwhile marketers generally connect with the ad exchange through a DSP to indicate the maximum bid the marketer is willing to make for certain types of ad inventory.

Ad exchanges may be open (anyone can participate), private (only invited DSPs, SSPs, ad networks can participate), or 'preferred deal' (publishers can sell digital ad inventory to specific advertisers, once the parties have negotiated a price).[90]

Publisher ad servers determine which advertisements to display to consumers on the various parts of the publisher's app or website, and when the advertisement will be displayed.[91] Publisher ad servers incorporate decision engines which place ads from external marketers, as well as determining which of the publisher's own internal promotions will be displayed and when. In the case of the former, the publisher ad server may sit between the publisher and the SSP.

Advertiser ad servers provide creative management, store data about each advertising transaction and collect ad performance data.[92]

Ad measurement, attribution and verification services are provided to determine what a marketer must pay to the publisher for an advertisement (where that fee depends on the

---

[86] Joseph Turow (n 43) 74.
[87] See David S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy' (2009) 23 *Journal of Economic Perspectives* 37, 41 and ibid 74-78.
[88] See Chiradeep BasuMallick, 'What is an Ad Exchange? Definition, Functioning, Types and Examples' (*Martech Advisor Online*, 30 September 2019) https://www.martechadvisor.com/articles/ads/what-is-an-ad-exchange/?zd_source=mta&zd_campaign=8915&zd_term=chitraiyer , on the types of information exchanged and used by the DSP and SSP at the ad exchange.
[89] Alternatively, an advertising mediation platform might be integrated in the software of an app or website, creating a forum in which various ad networks compete for ad placements: Norwegian Consumer Council (n 5) 38. Ad exchanges are, eg, provided by OpenX, Rubicon Project, Yahoo Ad Exchange, Xandr, Google / Doubleclick Ad Exchange, Microsoft, SmartyAds.
[90] See BasuMallick (n 88).
[91] Examples of publisher ad servers include DoubleClick for Publishers, OpenX, AdButler, adzerk, Xandr and Facebook Audience Network.
[92] Examples of advertiser ad servers include Xandr, Sizmek, Google Ads and Facebook Ads.

consumer's response to the advertisement), to verify that the advertisement was displayed according to the parties' contract and to determine the success of the advertisement.

Measurement vendors determine the types of audiences being reached by the advertisements and whether advertising campaign goals are being met.[93] Adtech vendors also provide **verification** services to confirm that the marketer's advertisement was actually displayed on the agreed type of website at the agreed time.

Whereas in earlier years online advertisers paid 'per impression' for their advertisements, it is increasingly common for advertising fees to be based on the subsequent actions of the consumer,[94] for example, whether the consumers clicks on the advertisement, or subsequently takes up a subscription with the marketer, or makes an online or offline purchase with the marketer.[95] These payment models require further monitoring and tracking of the consumer's behaviour for **attribution** purposes to determine the advertising fee that must be paid. Datalicious by Equifax, for example, measures consumers' 'granular user-level data in near-real time', online and offline, to attribute credit for sales to different elements of digital marketing.[96]

5.3.3 Major platforms: Google and Facebook

So far, this outline omits two of the most important players in this ecosystem. Google and Facebook are the two largest digital platforms operating in Australia and both firms depend on digital advertising for the vast majority of their revenue. However, rather than relying on the services of various third-party adtech vendors, these platforms integrate most of the functions outlined above within the businesses of one organisation.[97]

Google is by far the largest provider of online advertising and adtech services globally. For publishers, Google integrates the functions of an SSP, ad exchange and publisher ad server in one set of businesses. For marketers, Google integrates the functions of a DSP, data management platform, data analytics provider and advertiser in another set of businesses, which allows marketers to place advertisements on Google owned sites (such as Google Search, YouTube and Gmail) as well as third party publisher sites which sell ad inventory through Google.

Facebook's business model is different to Google's, but also highly integrated. For marketers, Facebook integrates the functions of a DSP, data management platform, data analytics provider and advertiser ad server in 'Facebook Ads'. Facebook Ads allows marketers to place advertisements on their choice of Facebook's own platforms (Facebook, Instagram and Messenger) as well as third party publisher websites that are part of the 'Facebook Audience Network'.[98] Facebook promises marketers that they can use the same 'Facebook targeting' capabilities on its own platforms and these third party websites.[99] Facebook also essentially integrates the functions of an SSP, ad exchange and publisher ad

---

[93] Norwegian Consumer Council (n 5) 24.
[94] See David S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy' (2009) 23 *Journal of Economic Perspectives* 37, 38-39.
[95] Payment models include: CPM (cost per mille – cost per thousand impressions); CPC (cost per click); CPA (cost per acquisition); CPV (cost per view – video).
[96] See datalicious, 'Media Attribution' (datalicious website, accessed 23 April 2020) https://www.datalicious.com/our-services/media-attribution. See further 'Glossary' (datalicious website, accessed 23 April 2020) https://www.datalicious.com/resources/glossary#mta.
[97] Norwegian Consumer Council (n 5) 121-122.
[98] ACCC, *Digital Platforms Inquiry: Final Report* (June 2019) 124, 128.
[99] See Facebook, 'Facebook for Business: Facebook Audience Network' (Facebook website) https://www.facebook.com/business/marketing/audience-network accessed 31 March 2021

server in its Facebook Audience Network, which places ads on third party publisher sites on behalf of those publishers in addition to placing advertisements on its own platforms.[100]

One of the many ways Google and Facebook have accumulated increasingly detailed and expansive personal data on consumers is by acquiring third-party adtech vendors, and merging the third-party vendors' consumer databases with the platform's own consumer database.[101] Google and Facebook also constantly accumulate enormous quantities of personal data covering a wide range of the consumer's activities, via their numerous businesses operating in a broad range of markets. For Google, products include online search, video, email, education tools, data analytics, in-home assistants, and digital advertising. For Facebook, products include social media, messaging, live streaming, photo sharing and digital advertising. Through their advertising customers (publishers and marketers), these companies also collect vast amounts of personal data which can be added to existing profiles they have compiled on individual consumers.[102] Users do not have effective means to avoid this collection of their personal data.[103]

Both Google and Facebook have frequently pointed out that they 'do not sell' personal data, or only share it with other companies in very limited circumstances,[104] apparently as evidence of their respect for consumer privacy. However, while it is true that these platforms do not generally sell personal data, this should not be seen as ensuring individuals' privacy.

First, both Google and Facebook have suffered a number of major data breaches.[105] Based on this history, data stored by these firms is quite likely to be subject to improper use or

---

[100] ACCC, *Digital Platforms Inquiry: Final Report* (n 4) 124, 128.

[101] See Norwegian Consumer Council (n 5) 22; ACCC, *Ad Tech Inquiry: Issues Paper* (n 73) 21, listing Amazon's acquisition of DSP TubeMogul, Google's acquisition of DoubleClick, AdMob and Adometry, and Taboola's acquisition of Outbrain.

[102] The Facebook Data Policy (https://www.facebook.com/policy.php) states that:
'Advertisers, app developers and publishers can send us information through Facebook Business Tools that they use, including our social plugins (such as the Like button), Facebook Login, our APIs and SDKs, or the Facebook pixel. These partners provide information about your activities off Facebook – including information about your device, websites you visit, purchases you make, the ads you see and how you use their services – whether or not you have a Facebook account or are logged in to Facebook. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its shop. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.'
The Google Privacy Policy (https://policies.google.com/privacy?hl=en-US accessed 31 March 2021) provides that:
'We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.'
And later (https://policies.google.com/privacy/embedded?hl=en accessed 31 March 2021):
'[A] website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings, and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.'

[103] See Privacy International, 'No, Facebook is not telling you everything' (Privacy International website, 24 February 2020).

[104] The Facebook Data Policy (www.facebook.com/about/privacy/update/printable) states, 'We don't sell any of your information to anyone and we never will.' The Google Privacy Policy (www.policies.google.com/privacy/google-partners?hl=en-us) states, eg, 'We don't share information that personally identifies you with our advertising partners, such as your name or email, unless you ask us to share it.'

[105] See, eg, Lily Hay Newman, 'A New Google+ Blunder Exposed Data from 52.5 Million Users' (*Wired online*, 12 October 2018); Emily Glazer, Tracy Ryan and Jeff Horwitz, 'Facebook Penalty is Set at $5 Billion' (*The Wall Street Journal online*, 13 July 2019); Josh Taylor, 'Facebook sued by Australian information watchdog over Cambridge

access and suffer major data breaches in future. Concentrating data pools of unprecedented size and reach in the hands of a small number of large firms does not ensure the security of that data.

Second, Google and Facebook themselves can also use the personal data amassed on each individual against that individual's interests, including by increased data exposure, manipulative targeted marketing, and the potential for exclusion or discrimination.[106]

Third, Google and Facebook have both shown themselves determined to collect as much personal data as possible for commercial purposes, even if these data practices contradict the privacy preferences revealed by consumer surveys.[107] This personal data may be used for the platforms' behavioural and contextual advertising businesses, and/or to permit the platform to gain a competitive advantage in other markets or to enter new markets.

Importantly, while both platforms provide users with some capacity to opt out of receiving targeted advertising, they do not permit consumers to avoid the tracking of their online behaviour and the use and retention of that data for the platforms' other commercial purposes. In fact, both Google and Facebook constantly collect data on consumers who have no direct connection with Google or Facebook businesses in situations where the consumer is unlikely to be aware of this data collection.[108]

Amazon is another major digital platform which may become increasingly significant in the ad tech sector. Aside from its position as the world's largest online retailer, Amazon has extended its operations to numerous other markets, including digital advertising. Amazon has amassed enormous quantities of consumers' personal data, including data from the operation of its online store and the Amazon Marketplace, a platform it provides for other merchants to sell their own products alongside Amazon products. The company has been criticised for using that data to advantage its own operations across markets, as well as allegedly advantaging sales of its own products at the expense of Amazon Marketplace merchants.[109]

Amazon does not yet enjoy a substantial share of digital advertising or ad tech services, but a number of factors make it likely to increase its presence in digital advertising in Australia, including the penetration of its businesses globally, its extensive datasets (particularly transaction data), its ability to link online data with growing search data from its in-home

---

Analytica-linked data breach' (*The Guardian online*, 9 March 2020); Darren Davidson and Dana McCauley, 'Zuckerberg protects his privacy, not ours' (*The Australian online*, 12 April 2018) regarding Facebook data breaches.

[106] See, eg, Alex Hern and Frederik Hugo Ledegaard, 'Children 'interested in' gambling and alcohol, according to Facebook' (*The Guardian online*, 10 October 2019); Gautham Nagesh, 'Google on 'Spy-Fi': We Failed Badly' (*The Hill online*, 22 October 2010).

[107] See ACCC, *Digital Platforms Inquiry: Final Report* (n 4) 379-381, on the growing volume and scope of data collected by Google and Facebook respectively.

[108] See, eg, Katharine Schwab, 'Google's reCAPTCHA has a dark side' (*Fast Company online*, 27 June 2019); Katharine Kemp, 'Australia's privacy watchdog is taking Facebook to court' (*The Conversation online*, 11 March 2020) regarding collection of non- user data on websites with a Facebook 'Like' button or other Facebook technologies. The Google Privacy Policy - 'your activity on other sites and apps' link) – (https://policies.google.com/privacy/embedded?hl=en accessed 31 March 2021) states:
'Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your account settings, and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.'

[109] See, eg, Lina M Khan, 'Amazon's Antitrust Paradox' (2017) 126 *Yale Law Journal* 710, 780-783.

assistant 'Alexa', and its competitive advantage in 'proximity to point of purchase'.[110] In marketing the services of the Amazon DSP, for example, the company has promised marketers access to 'Amazon audiences' across Amazon sites, apps and devices, as well as on third-party sites and apps, and a 'full view of the customer journey from awareness to loyalty'.[111]

5.4 Do businesses use 'personal information'?

5.4.1 Application of the *Privacy Act* to 'personal information'

Many publishers, marketers and adtech vendors claim that at least some of the data they use for marketing and behavioural advertising purposes is not 'personal data' or 'personal information'.[112] These firms often state that the relevant data has been 'anonymised' or 'de-identified' such that it is no longer personal information. The implication is that use of this data poses no risk to the consumer and/or is not governed by the Australian Privacy Principles (APPs) under the *Privacy Act*, such that the firm may use it for any purpose whatsoever.[113]

These claims should be carefully scrutinised. At the outset, there are strong arguments that de-identification efforts are increasingly ineffective.[114] In the context of data brokers and adtech providers, there is the question of whether the relevant data does, or should, fall within the definition of 'personal information', given its association with a unique person.

The *Privacy Act* imposes obligations on 'APP entities'. Most firms described in sections 5.3.1 to 5.3.3 above are likely to come within the definition of an 'APP entity', since, in most cases, the firm:

- has annual revenue over AUD 3 million in the previous financial year, or
- 'discloses personal information about another individual to anyone else for a benefit, service or advantage', or

---

[110] Joseph Brookes, 'Prepare for the Digital 'Triopoly' as Amazon's Advertising Model Emerges' (*Which-50 online*, 22 January 2019).

[111] Katherine Osteen, 'Developing the Amazon DSP: An interview with Ryan Mayward' (24 October 2018) https://advertising.amazon.com/blog/developing-the-amazon-dsp-an-interview-with-ryan-mayward accessed 31 March 2021

[112] See Norwegian Consumer Council (n 5) 133. See, eg, the Sizmek by Amazon Privacy Policy (https://www.sizmek.com/privacy-policy/ accessed 31 March 2021) which states:
'The information we collect is associated with your cookie identifiers and/or mobile advertising identifiers (if you are using a mobile device), as well as your IP address. We never collect information about your actual identity. ... [O]ur technology employs cookies, device identifiers and similar technologies (like pixels and statistical device identifiers) to collect information about your browser or device, the sites it has visited and the apps it has used, the advertisements served to it, interactions with those advertisements, and, where available, the approximate geographic location of the device ('ad serving information'). ...
This ad serving information, which does not enable Sizmek to determine your actual identity, may be shared with our customers and Sizmek's and our customers' partners for our customers' advertising purposes.'

[113] See, eg, The Australian Financial Review Privacy Policy (https://www.afr.com/privacy-policy accessed 31 March 2021):
'We may also collect anonymous data (which is not personal information) relating to your activity on our websites (including IP addresses) via cookies, or we may collect information from you in response to a survey. We generally use this information to report statistics, analyse trends, administer our services, diagnose problems and target and improve the quality of our products and services. To the extent this information does not constitute personal information because it does not identify you or anyone else, *the Australian Privacy Principles do not apply and we may use this information for any purpose and by and [sic] means whatsoever*.' (emphasis added)

[114] See, eg, Vanessa Teague, 'Submission to the Attorney General's Review of Australia's *Privacy Act*' (27 November 2020); Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 *Law in Context* 49.

- ‘provides a benefit, service or advantage to collect personal information about another individual from anyone else’.[115]

Under the *Privacy Act*, ‘personal information’ means:

> information 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.[116]

Accordingly, digital records and inferences made about an individual may fall within this definition. The term ‘de-identified’ is also defined. According to the *Privacy Act*, ‘personal information is ***de-identified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’.[117]

The critical question for businesses will often be whether the information or opinion is ‘about an identified individual, or an individual who is reasonably identifiable’. These concepts currently lack clarity under Australian law, as explained in the following sections.

5.4.2 ‘De-identified’ data, unique identifiers, ID syncing and resolution

Firms stating that certain of their data practices only involve ‘de-identified’, ‘anonymised’ or ‘aggregated’ data imply that this data is not about an identified individual or an individual who is reasonably identifiable.[118] It is clear, however, that many of these businesses aim to distinguish, profile and interact with individual consumers by using this ‘de-identified’ data. They often achieve this objective by using ‘unique identifiers’, that is, unique strings of numbers and/or letters that are assigned to a particular device or individual in the absence of a name or email address.[119]

Unique identifiers intended to track a consumer’s activity include identifiers derived from email addresses (such as ‘hashed’ email addresses); cookie identifiers; device identifiers; IP addresses; and advertising identifiers (such as the Android Advertising ID). These are not random identifiers dissociated from any actual individual. On the contrary, these identifiers are intended to permit firms to associate information across devices, companies, services and transactions with a particular individual, whether or not that individual is identified by name.[120] Adtech firms refer to this as ‘people-based marketing’.[121]

---

[115] *Privacy Act*, s 6D.
[116] *Privacy Act*, s 6(1).
[117] *Privacy Act*, s 6(1).
[118] The Google Privacy Policy appears to imply that it does not regard information tied to a unique identifier as personal information, but it fails to clarify this. The policy (https://policies.google.com/privacy/embedded?hl=en accessed 31 March 2021) states:
‘When you’re not signed in to a Google Account, we store the information that we collect with unique identifiers tied to the browser, application or device you’re using. …
When you’re signed in, we also collect information that we store with your Google Account, which we treat as personal information.’
[119] Norwegian Consumer Council (n 5) 25.
[120] Jessica Davies, ‘Shared Identity Solutions’ (Digiday online, 23 September 2019) https://digiday.com/media/what-are-shared-identity-solutions-and-can-they-really-replace-cookies/ explains that ‘shared-ID consortiums and businesses’ are ‘working on shared versions, meaning the creation of one (anonymous) unified ID per individual that publishers and their programmatic ad partners can use to serve and target ads’.
[121] See, eg, Goodway Group, ‘What is People-Based Marketing?’ (Goodway Group website, accessed 23 April 2020) https://goodwaygroup.com/blog/what-is-people-based-marketing/:
‘At the most basic level, people-based marketing means gathering customer data from both offline and online sources and using that rich profile to more accurately recognize and reach customers on any device.’

This profiling of a given individual is given a very high priority in the adtech industry. The Interactive Advertising Bureau (IAB) is a trade association for online advertising, with 43 offices globally including an office in Australia.[122] The IAB advises its members that:[123]

> In order to deliver truly personalized and relevant messaging, marketers should not only work with cross-device identity vendors, but also with attribution providers and internal data teams to help them **not just connect and match devices with unique, people-based IDs, but also to gain an understanding of the consumer behind the device**.

Mathieu Roche, CEO of 'shared ID' provider ID5, has stated:

> An ID is a key in a database. It is **the first bit of code that you can attach all you know about the user to, but it has to be unique**. The purpose is for the same ID to be shared between publishers and brands — it has to be the same key. It is a common language for ad tech.[124]

To achieve this, some suppliers aim to 'resolve' or 'sync' the details of one consumer across different databases, devices and services, to permit firms to recognise and track the individual consumers without reference to their name or email address. These services may take the form of 'cookie syncing' (linking information from cookies placed on the consumer's device by different firms) or 'ID syncing' (linking different identifiers assigned to the same consumer).[125]

LiveRamp promised that with its IdentityLink services it could:[126]

> [c]reate targeted, people-based campaigns by **resolving first-, second-, third-party data to a single unique identifier** that can be onboarded to 500+ destinations through the LiveRamp platform for omnichannel targeting, measurement, and analytics across digital and TV.

Adobe describes its 'ID synchronization' process as follows:[127]

> ID synchronization matches IDs assigned by the ID service to IDs assigned to site visitors by our customers. For example, say the ID service has assigned a visitor ID 1234. Another platform knows this visitor by ID 4321. The ID service maps these IDs together during the synchronization process. The results add new data points to what our customers know about their site visitors. And, if the ID service can't match an ID, it creates a new one and uses that ID for future synchronization.

Claims that data brokers, publishers, marketers and adtech vendors exchange only non-personal information should be challenged. As Culnane and Leins point out, an individual may be even more accurately identifiable by their behavioural and device data than by their given name:[128]

> The data points that represent that individuals actions, devices, location, etc are often as effective, if not more effective, at identifying an individual as traditional identifiers …

---

[122] 'About IAB' (IAB Australia website) https://www.iabaustralia.com.au/about-iab-australia/about-iab
[123] IAB, 'Mobile Identity Guide for Marketers: A Best Practices Primer for Mobile & Cross-Device Marketing' (IAB, 2017) 12 https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf accessed 31 March 2021 (emphasis added).
[124] Jessica Davies, 'Shared Identity Solutions' (Digiday online, 23 September 2019) https://digiday.com/media/what-are-shared-identity-solutions-and-can-they-really-replace-cookies/ accessed 31 March 2021 (emphasis added).
[125] Norwegian Consumer Council (n 5) 27.
[126] 'Introducing LiveRamp IdentityLink' (LiveRamp website) https://liveramp.com/blog/introducing-liveramp-identitylink/ accessed 3 March 2020 (emphasis added).
[127] 'Understanding ID synchronization and match rates' (Adobe website) https://docs.adobe.com/content/help/en/id-service/using/intro/match-rates.html accessed 31 March 2021
[128] Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 *Law in Context* 49.

There can be no doubt that these strategies aim to address a single individual and to combine data about that individual from numerous databases to create an individual profile, even if that profile is not attached to individual's actual name or email address. Singled out in this way, the individual can be subjected to growing risks of re-identification, manipulation, exclusion and discrimination.

5.4.3 Recommended legislative clarification

Traditionally, an individual would be identified by their given name, combined with some other information such as a postal address, email address, employment position or family connection. However, the outline above indicates that online businesses frequently seek to single out an individual without reference to these traditional identifiers. The concept of identification should not be limited to data which is labelled with a consumer's legal name or contact details, but should extend to data used to single out one consumer as distinct from other consumers.

The UK ICO has recognised that an individual may be identifiable 'either as a named individual or simply as a unique user of electronic communications and other internet services who may be distinguished from other users'.[129]

The Australian case law on the meaning of 'personal information' does not currently provide this clarity. In *Privacy Commissioner v Telstra Corporation Ltd*,[130] the Full Federal Court upheld the decision of the Administrative Appeals Tribunal (AAT) on the narrow issue that personal information must be 'about an individual' and that those statutory words should be given substantive effect.[131] The case concerned mobile network 'metadata',[132] including Internet Protocol (IP) addresses, recorded and stored by Telstra.

The Deputy President of the AAT had concluded that the IP addresses allocated to a mobile device which the individual complainant used were not 'about' that individual since 'an IP address is not allocated exclusively to a particular mobile device'.[133] The Full Federal Court noted the Deputy President's conclusion that:

> The IP address might even change frequently in the course of a communication. For that reason, the Deputy President concluded that the connection between the person using a mobile device and an IP address was too ephemeral for the IP address to be 'about' the individual. Instead, it was about the means by which data is transmitted from a person's mobile device over the internet and a message sent to, or a connection made, with another person's mobile device.[134]

However, the appeal to the Full Federal Court did not concern this finding and accordingly the Court reached no conclusion of its own in this respect.[135] The Court did not consider the question of when various metadata could constitute 'personal information'.[136]

In the DPI Final Report, the ACCC recommended that the definition of 'personal information' under the *Privacy Act* should be updated 'to clarify that it captures data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual'.[137] The ACCC recommended in particular that the definition should

---

[129] UK ICO, 'What are identifiers and related factors?' (UK ICO website) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/ accessed 31 March 2021
[130] [2017] FCAFC 4, para 5, 73.
[131] [2017] FCAFC 4, para 80.
[132] Essentially, 'data that provides information about data': [2017] FCAFC 4, para 5.
[133] [2017] FCAFC 4, para 44.
[134] [2017] FCAFC 4, para 44.
[135] [2017] FCAFC 4, para 44.
[136] [2017] FCAFC 4, para 73.
[137] ACCC, *Digital Platforms Inquiry: Final Report* (n 4) 458.

be amended to reflect the wording of the GDPR, bringing the added benefit of alignment with international standards.[138]

The GDPR recognises that a name is only one way that a person can be identified. Various online identifiers may equally identify an individual. Article 4(1) of the General Data Protection Regulation (GDPR) specifies that:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject').

The definition proceeds to clarify that:

> 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.

Recital 30 explains the relevance of online identifiers:

> Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Under the GDPR, therefore, unique identifiers can constitute personal data.[139]

The use of strategies which single out unique individuals and create a detailed picture of 'the consumer behind the device', alongside the claim that these practices involve no personal information, exposes consumers to growing risks of re-identification, manipulation, exclusion and discrimination. This adds weight to the ACCC's recommendation in the DPI Final Report that the *Privacy Act* should be amended to clarify, in line with the GDPR, that 'personal information' includes 'data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual'.

5.4.4 The underwhelming 'death of the third-party cookie'

There has been a further development in the online identification of consumers over the last few years, driven largely by developments in online browsers. Responding to consumers' privacy concerns,[140] Apple and Firefox introduced online browsers with privacy settings which enabled consumers to block all or most third-party cookies.[141]

Cookies are small text files placed on a consumer's device which allow the originator of the cookie to retrieve information about the consumer which is stored in that text file over time. If, while a consumer is visiting a website, the operator of that website places a cookie on the consumer's device, that is regarded as a first party cookie. If, while the consumer is visiting that website, some other party places a cookie on the consumer's device, that is considered

---

[138] Ibid.
[139] Norwegian Consumer Council (n 5) 25. In the United States, on the other hand, unique identifiers are not treated as 'personally identifiable information': at 98.
[140] Kristina Monllos, "They've started to render DMPs useless': Omnicon Media Group CEO Scott Hagedorn's State of Programmatic Advertising' (*Digiday online*, 8 May 2019):
'Everyone was rushing toward a reality where we could have a central nervous system and DSP and a DMP that was plugged in the multiple DSPs and multiple ecosystems. That was going to be the future of behavioral media and the future of advertising. And then there's a privacy backlash and people being like, 'Well, how exactly do you know that I was here on another screen and now they're on this one? How is my data being utilized?"
[141] See Gerrit de Vynck, 'Firefox follows Apple in blocking third-party cookies online' (*Bloomberg online*, 4 June 2019); Nick Statt, 'Apple updates Safari's anti-tracking tech with full third-party cookie blocking' (*The Verge online*, 24 March 2020).

to be a third-party cookie. These are also referred to as 'tracking' or 'targeting' cookies. Many of these third-party cookies had been placed on consumers' devices for the purpose of identifying an individual consumer between websites and providers, adding to that consumer's profile across providers and displaying targeted advertising to the consumer.

Many publishers and marketers saw the blocking of third-party cookies by Apple and Firefox browsers as problematic, claiming that, without identification via third party cookies, advertising opportunities and therefore advertising revenue decreased.[142] This concern greatly increased in January 2020, when Google announced that it would be disallowing third party cookies on its Chrome browser from 2022.[143]

However, the predicted 'death of the third-party cookie' cannot be regarded as an overwhelming victory for consumer privacy for several reasons.

First, while Google's announcement was the most substantial development, given the company's size and market share, Google has only resolved to remove third party cookies. The firm made no suggestion that it will stop tracking consumers itself via its own websites and apps, or combining that data with data it collects via the first party cookies of its publisher and marketer clients.[144] This is likely to mean that consumers will continue to be monitored, if by a smaller number of more powerful firms.

Second, publishers, marketers and adtech businesses have a number of other means of identifying consumers even in the absence of third-party cookies. Numerous players propose to rely more heavily on their own first party cookies as well as 'registration walls', that is, requiring consumers to register and login to use their sites.[145] This will allow the firm to track activity of individual consumers via that login identification, and increase their first party data.[146] Some publishers have moved to form more 'data partnerships', by reaching agreements to disclose first party personal data about their own customers in exchange for second party data, that is, personal data about the other firm's customers.[147]

Beyond this expansion of first- and second-party data, there are numerous ways to identify consumers across different devices and websites even in the absence of third-party cookies. These include 'device fingerprinting',[148] as well as the use of persistent advertising identifiers such as Apple's Identifier for Advertising and Google's Android Advertising ID.[149] Still more argue that diverse customer records can now be matched using machine learning

---

[142] See Ariel Bogle, 'Google wants to kill third-party cookies: Here's why that could be messy' (*ABC online*, 21 January 2020). Some commentators have seen this development as a battle for control between 'browser tech' and 'adtech'.
[143] Justin Schuh, 'Building a more private web: A path towards making third party cookies obsolete' (*Chromium blog*, 14 January 2020) https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html?mod=article_inline; Bowdeya Tweh and Sahil Patel, 'Google Chrome to Phase Out Third-Party Cookies in Effort to Boost Privacy' (*The Wall Street Journal online*, 14 January 2020); Nat Ives, 'Marketers and Ad Agencies Ask Google Not to Kill Cookies Too Soon' (*The Wall Street Journal online*, 16 January 2020).
[144] Ariel Bogle, 'Google wants to kill third-party cookies: Here's why that could be messy' (*ABC online*, 21 January 2020); Seb Joseph, 'Winners, losers and fallout from Google's plan to drop cookies' (*Digiday online*, 16 January 2020).
[145] Tim Peterson, 'The industry is looking to first-party data to replace cookies, but the open web may lose out' (13 February 2020) on the threats to the 'open web' from the 'registration wall' approach.
[146] This also has the advantage for the publisher of establishing deterministic identity, rather than probabilistic identity, for targeted advertising and attribution.
[147] See Lucinda Southern, ''The Google doomsday clock is ticking': Publishers scramble to benefit from post-third-party cookie data partnerships' (*Digiday online*, 26 February 2020).
[148] 'Device fingerprinting' refers to the process of using a set of information to 'single out, link or infer a user, user agent or device over time': Article 29 Data Protection Working Party, 'Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting' (25 November 2014) 4.
[149] IAB, 'Mobile Identity Guide for Marketers: A Best Practices Primer for Mobile & Cross-Device Marketing' (IAB, 2017) 4 https://www.iab.com/wp-content/uploads/2017/06/Mobile-Identity-Guide-for-Marketers-Report.pdf

in the absence of these identifiers.[150] There are also proposals to adopt a universal, unique identifier for each consumer which would be broadcast to adtech firms, but which might permit consumers to make privacy choices (other than not having a unique identifier apparently).[151]

In short, in response to efforts to block pervasive tracking of consumers by third party cookies, many firms have simply begun to establish other ways to persistently identify and track consumers, rather than permitting consumers to choose not to be persistently identified in their online activities.

5.5 Consumer consent to data practices

5.5.1 Notice and consent requirements under the *Privacy Act*

One of the justifications firms raise for the data practices explained above is that consumers have been notified of these data practices via the relevant firms' privacy policies and that consumers have at least impliedly consented to these practices since the firms provide a link to their privacy policies on their respective websites. These justifications refer to notice and consent obligations under the APPs established by the *Privacy Act*.

The APPs set out the obligations of APP entities in their dealings with personal information. The APPs broadly include obligations regarding notice; consent; access; correction and updating; security; and deletion. Here, we focus on the notice and consent obligations.

APP entities must notify individuals that personal information about them has or will be collected.[152] APP entities must also publish a 'clearly expressed and up to date' privacy policy 'about the management of personal information by the entity'.[153] These privacy policies must include notice about what kinds of personal information the entity collects, how the entity collects and holds that information and the purposes for which they used and disclose it, among other things.[154]

Further, an APP entity must not engage in certain activities unless the relevant individual consents, including:

- collecting sensitive information about an individual;[155]
- using or disclosing personal information for a purpose other than the particular purpose for which it was collected;[156]
- using or disclosing sensitive information about an individual for the purpose of direct marketing;[157] and
- disclosing personal information to an overseas recipient.[158]

---

[150] Eg, data analyst, Amperity, explains in 'What We Do' (Amperity website) https://amperity.com/what-we-do/data-foundation 3 March 2020 stated:
'Amperity applies a patented machine learning-powered approach to accurately and comprehensively unify records from every system, even when records lack an email address, phone number, loyalty number, or other traditional identity marker.'

[151] See Paige Murphy, 'Industry reacts: Experts welcome Google Chrome's third-party cookie removal' (*AdNews online*, 24 January 2020) https://www.adnews.com.au/news/industry-reacts-experts-welcome-google-chrome-s-third-party-cookie-removal.

[152] APP 5.

[153] APP 1.3.

[154] APP 1.4.

[155] With some exceptions, APP 3.3.

[156] With some exceptions, APP 6.1.

[157] APP 7.4.

[158] If certain further conditions are met: APP 8.2.

There is no comprehensive definition of 'consent' under the *Privacy Act*. The *Privacy Act* only states that 'consent' means 'express consent or implied consent'.[159] The OAIC has published non-binding Australian Privacy Principles Guidelines which include guidance on appropriate standards for consent ('the OAIC Guidelines').[160]

5.5.2 Purported notice and consent under existing privacy policies

5.5.2.1 Elements of consent in the OAIC Guidelines

The OAIC Guidelines identify four key elements of consent in its Guidelines as follows:

- the individual is adequately informed before giving consent;
- the individual gives consent voluntarily;
- the consent is current and specific; and
- the individual has the capacity to understand and communicate their consent.

In many cases, the consents to consumer profiling and adtech uses of personal data alleged by the firms described in this chapter fall short of the standards recommended by the OAIC.

5.5.2.2 'Bundled' consent is not voluntary

Consumer consent should not be regarded as voluntary where it is obtained by the bundling of consents for different uses and purposes in the relevant privacy policy. Nonetheless, in the case of publishers' and marketers' privacy policies, the firm's notice about data practices necessary for the firm to provide the relevant service to the consumer almost universally includes purported consents for other broad marketing purposes, with no provision for the consumer to consent to one and refuse the other.

For example, a major bank might provide a privacy policy which states that it will use the consumer's personal information to supply the consumer with financial services as well as disclosing that personal information to a broad category of third parties who 'share information for marketing purposes',[161] without providing any options in this respect.

Similarly, a consumer purchasing a subscription to 'The Australian' newspaper is required to accept the 'News Corp Australia Privacy Policy', which provides in part that:[162]

> We may combine information that we hold about you with information about you that we collect from other trusted businesses with whom you also have a relationship or from public sources and we may associate your browser and/or device with other browsers or devices you use. We may also share information we hold about you with those trusted businesses so that they can do the same thing.

Consent to such broad, unrelated purposes should not be regarded as voluntary where it is bundled with the primary purpose in this way.

5.5.2.3 Vague, open-ended privacy policies do not adequately inform

Publishers, marketers and data brokers often claim consumers consent to the use of their data for additional purposes relating to marketing or commercial data sharing arrangements on the basis of vague, open-ended terms in privacy policies, which do not provide the necessary specificity.

---

[159] *Privacy Act*, s 6(1).
[160] See further Chap 2.7.3.
[161] See, eg, 'NAB Privacy Policy' https://www.nab.com.au/content/dam/nabrwd/documents/policy/banking/nab-privacy-policy.pdf accessed 31 March 2021:
'We may disclose your personal information to third parties outside of the Group, including: …
- organisations we sponsor and loyalty program partners, including organisations the NAB Group has an arrangement with to jointly offer products or has an alliance with to share information for marketing purposes;'
[162] News Corp Australia Privacy Policy (https://preferences.news.com.au/privacy accessed 31 March 2021).

The relevant terms are often phrased in a way that the consumer cannot determine the actual uses of the personal data and the entities to whom that data will be disclosed. The terms used are entirely open-ended. For example, the publisher, Fairfax Media Ltd, states in 'The Australian Financial Review Privacy Policy':[163]

> We may disclose your personal information to: … our existing or potential agents and/or business partners ...

The Policy does not identify or limit the entities that might fall within these categories.

Google has for several years provided its reCAPTCHA security product to a large number of publisher websites worldwide, including businesses in Australia. The reCAPTCHA badge displayed on these websites is underscored by a small link titled 'Privacy'. Following that link will take the consumer to the general Google Privacy Policy. Although reCAPTCHA collects a range of data about the consumer's device and activity on websites,[164] the Google Privacy Policy makes no mention of the reCAPTCHA product or the data practices associated with it.

The privacy policy for the publisher TikTok, a popular social media app, states:

> We also share your information with business partners, other companies in the same group as TikTok Inc, content moderation services, measurement providers, advertisers and analytics providers.

The TikTok Privacy Policy does not list or limit the advertisers, measurement providers or analytics providers to whom users' personal information can be disclosed.

As the Norwegian Consumer Council pointed out in its report on the privacy policies and data practices of popular mobile apps, consumers 'have no way of knowing which entities process their data and how to stop them'.[165] The UK ICO has noted that the transfer of consumer's personal data to numerous third-party vendors gives rise to a very significant risk that the data will be improperly stored and used, particularly since the original collector of the data no longer has control over it.[166]

5.5.2.4 Consent received via numerous or unidentified third parties is insufficient

The effect of these inadequately informed, bundled consents snowballs as third parties in turn rely on these broad permissions as consent for their own data practices. Numerous privacy policies include terms intended to provide permission for the firm to receive the consumer's personal data from third parties and combine it with the firm's first party data about that consumer. Again, the consumer is not provided with options in this respect.[167]

The Woolworths Rewards privacy policy previously stated:[168]

> We collect personal information about Woolworths Rewards Members from other persons or entities. For example, we collect personal information for marketing purposes from other

---

[163] The Australian Financial Review Privacy Policy (https://www.afr.com/privacy-policy accessed 31 March 2021)
[164] On these uses, see Katharine Schwab, 'Google's reCAPTCHA has a dark side' (*Fast Company online*, 27 June 2019).
[165] Norwegian Consumer Council (n 5) 6.
[166] Information Commissioner's Office(n 5) 20-21.
[167] Eg, the Google privacy policy states (https://policies.google.com/privacy?hl=en-US accessed 31 March 2021): 'We may also collect information about you from trusted partners, including marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertisers to provide advertising and research services on their behalf.'
[168] Woolworths Rewards Collection Notice: https://www.woolworthsrewards.com.au/collection-notice.html accessed 3 March 2020

> suppliers of goods or services who, like us, have an existing relationship with Woolworths Rewards Members. …

Now that Woolworths Rewards has updated its privacy policy to provide limited "examples" of entities from whom it collects personal information, it is not clear whether this practice continues.

The Amazon 'Cookies & Internet Advertising' policy states:[169]

> Some third-parties may provide us pseudonymized information about you (such as demographic information or sites where you have been shown ads) from offline and online sources that we may use to provide you more relevant and useful advertising.

The NAB privacy policy contains a similar statement:[170]

> We may use or disclose information about you in order to combine the information that we hold with information collected from or held by external sources. We do this in order to enable the development of customer insights about you so that we can serve you better.

Other major banks include similar terms in their privacy policies.[171]

In each of the above cases, the consumer is provided with no option to decline this collection and combination of their personal data with data from other suppliers and third parties, which is not necessary for the provision of the relevant service.[172] It appears that data brokers, data management platforms, data aggregators, data analytics providers and adtech vendors rely on such broadly worded, take-it-or-leave-it terms in the privacy policies of their clients as evidence of consumers' consent to data sharing facilitated by their services.[173]

Further, firms often rely on the validity of third-party privacy policies to justify their data practices, while disclaiming responsibility for those policies and requiring consumers to identify and analyse those policies for themselves. For example, the TikTok Privacy Policy states:[174]

> Additionally, we allow these service providers and business partners to collect information about your online activities through Cookies. We and our service providers and business partners link your contact or subscriber information with your activity on our Platform across all your devices, using your email or other log-in or device information. **Our service providers and business partners may use this information** to display advertisements on our Platform and elsewhere online and across your devices tailored to your interests, preferences, and characteristics. **We are not responsible for the privacy practices of these service providers and business partners**, and

---

[169] Amazon 'Cookies & Internet Advertising': https://www.amazon.com.au/gp/help/customer/display.html?nodeId=201380490 accessed 31 March 2021

[170] NAB Privacy Policy: https://www.nab.com.au/content/dam/nabrwd/documents/policy/banking/nab-privacy-policy.pdf accessed 31 March 2021 (emphasis added)

[171] Eg, the Commonwealth Bank of Australia Privacy Policy states (https://www.commbank.com.au/content/dam/commbank/security-privacy/privacy-policy.pdf) accessed 31 March 2021:
'New technologies let us combine information we have about you and our other customers, for example transaction information, with data from other sources, such as third party websites or the Australian Bureau of Statistics. We analyse this data to learn more about you and other customers …' (emphasis added)

[172] While the consumer may be able to opt out of receiving targeted advertising, they are not given the option of avoiding the collection and combination of their personal data from third parties.

[173] Consider, eg, Data Republic Singapore Privacy Policy (https://www.datarepublic.com/wp-content/uploads/2019/11/Data-Republic-Privacy-Policy-Singapore.pdf accessed 31 March 2021): 'We may disclose personal information for the purposes described in this privacy policy to: … specific third parties authorised by you to receive information held by us'.

[174] TikTok Privacy Policy (https://www.tiktok.com/legal/privacy-policy?lang=en) accessed 31 March 2021 (emphasis added).

> the information practices of these service providers and business partners are not covered by this Privacy Policy.

Similarly , the privacy policy for the flybuys retail loyalty scheme states that customers should review the privacy policies of various third parties in respect of certain data 'sharing' arrangements, without specifying who those third parties are:[175]

> Flybuys is **not responsible for the privacy practices or policies of** Coles, Wesfarmers and **other Participants** … and **we recommend that you visit their websites for more information about their privacy practices and policies.**

Such empty injunctions to read unspecified third-party privacy policies should not be treated as valid consent to these practices, nor absolve the firm of responsibility for these data disclosures.

5.5.2.5 Ineffective opt-outs and device settings do not indicate consent

In some instances, the privacy policies of websites or apps state that consumers can choose to opt out of certain tracking or the acceptance of cookies, by changing their device settings. Implicitly, in the absence of taking this action, consumers are allegedly consenting to the firm's tracking activities. However, attempts to make use of opt outs and device settings often have very little effect.[176]

Critically, many of the opt outs do not permit the consumer to choose not to have their behaviour tracked, monitored and recorded, but only to opt out of *receiving* targeted advertising on the basis of that personal data.[177] Consumers should have the option not to have their behaviour tracked, monitored and recorded for purposes beyond the provision of the immediate service. In fact, the default position should be that they are not tracked in this way.

In other instances, opting out requires complex, time-consuming and repeated action on the part of the consumer, which, even then, cannot produce a complete avoidance of tracking for marketing purposes.[178] Some of these policies provide that if consumers do, for example, turn off the location-based tracking or GPS on their device, the app can still infer the consumer's location by using other data, including IP address, Wi-Fi access point information, Bluetooth, and cell tower data.[179]

Similarly, when consumers who are members of the flybuys and Woolworths Rewards retail loyalty schemes choose not to scan their loyalty cards for a particular purchase, the flybuys and Woolworths Rewards operators automatically link their payment card to the consumer's membership profile regardless.[180] Neither flybuys nor Woolworths Rewards have amended their privacy terms in this respect, despite the ACCC's call for them to desist. Accordingly, a customer may believe they have stopped using their loyalty card and therefore avoided ongoing tracking, while the firm continues to track them through their payment cards.

---

[175] flybuys Privacy Policy (https://www.flybuys.com.au/about#/privacy-policy) accessed 31 March 2021 (emphasis added). See also MoPub privacy policy, referring to over 160 partners; and Smaato listing more than 1000 partners: Norwegian Consumer Council (n 5) 159.
[176] Norwegian Consumer Council (n 5) 69, 179.
[177] ACCC, *Customer Loyalty Schemes: Final Report* (December 2019) 74-75.
[178] See, eg, the description of ineffectual opting out via www.youronlinechoices.com.au in ibid 69, 74-75. See also Katharine Kemp, *Submission in Response to the Australian Competition & Consumer Commission Ad Tech Inquiry Issues Paper* (Submission, 26 April 2020) 26 (citing the example of the opt out procedure for Sizmek by Amazon).
[179] Norwegian Consumer Council (n 5) 105, 128. At 83:
'This means that, even if a consumer explicitly turns off the GPS function on their smartphone, their location can be accurately triangulated by third parties through measuring the phone signal and distance to Wi-Fi access points and cell towers.'
[180] ACCC, *Customer Loyalty Schemes: Final Report* (n 177) 65-67.

5.5.3 Recommended legislative clarification

The OAIC Guidelines were originally published in 2014.[181] However, it is clear from the prevalence of the terms described above that these non-binding guidelines have not deterred firms from relying on 'consents' which fall well short of the standards outlined by the OAIC.

In the DPI Final Report, the ACCC recommended that the requirement for consent should be extended to 'whenever a consumer's personal information is collected, used or disclosed by an APP entity', with certain limited exceptions.[182] The ACCC also recommended that '[v]alid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent)'.[183] It noted that this amendment would be 'in line with the higher standard of data protection provided under the GDPR'.[184]

'Consent' is one of the six possible lawful grounds for processing personal data under the GDPR.[185] The GDPR sets standards for consent that overlap with the OAIC guidelines to some extent.

'Consent' is defined under article 4 of the GDPR, which states that:

> consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Further, Article 7 of the GDPR clarifies that:

> When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Accordingly, under the GDPR, a firm cannot argue that a consumer consented to the processing of personal data where performance of a contract was conditional on the consumer providing consent to data processing that was not necessary for the performance of the contract. So, for example, where a bank bundles consent to data practices necessary for the provision of the relevant financial services with consent to use of the data for 'marketing and research', the alleged consent to this latter use would not be valid.

The GDPR definition is given further content in the recitals to the GDPR, including Recital 32, which states in part:

> Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Under the GDPR, therefore, the 'implied consent' currently recognised under the *Privacy Act* would not constitute valid consent. Consumers should not be required to navigate multiple, deliberately complex 'opt out' procedures, nor perform the Sisyphean task of maintaining their choice not to be tracked against constantly evolving technologies designed to circumvent that choice. In the absence of action by the consumer, default settings should favour privacy.

---

[181] The current version is version 1.3. However, the guidance referred to in this article took the same form in the original version in 2014.
[182] ACCC, *Digital Platforms Inquiry: Final Report* (n 4) 464.
[183] Ibid.
[184] Ibid 466.
[185] GDPR, Article 6(1).

5.6 Conclusion

The trends in privacy policies outlined above make the claims that consumers have consented to the privacy-degrading data practices of the data brokerage and ad tech sectors spurious, often disingenuous. Improvements in legislated standards for notice and consent and means of recourse for individuals are far from a complete solution to the lack of agency which individuals experience with respect to the collection and uses of their personal information by commercial entities and government agencies. Too often the individual concerned has made no choice in favour of a particular supplier that is collecting their personal information, let alone the uses the supplier makes of that information. In other cases, the collection and use in question is so generally negative and detrimental to the individual that it is preferable for substantive rules to be developed to prohibit those practices outright. Consent and notice will not always be sufficient to support fair data practices and the dignity and autonomy of individuals. However, the adoption of these recommendations on notice and consent is a vital first step in ensuring that publishers, markets and ad tech vendors do not rely on fictional consents to justify their data practices.

ROB NICHOLLS

6. Chapter 6 - Reform in Australia: a focus on informed consent

6.1 Introduction

The issue of online privacy and data security is of critical importance to the efficient functioning of Australian society. In a data driven economy, the amount and variety of data being collected as consumers browse, socialise and shop in online environments is increasing exponentially at an unfettered pace. This is made possible by consumers who provide uninformed consent to online standard form agreements and privacy policies. The issue with failing to ensure informed consent to online standard form agreements is the resulting exploitation of consumer data and consequences this has on an individual's privacy. All too often a consumer's consent to standard form agreements means that they transfer an irrevocable right to the drafting party to access and exploit their data for the rest of time.

Standard form agreements are enforced on the basis that they are a valid contract, ie that the steps of offer, acceptance, intention to create a legally binding agreement, consideration, a legal capacity and consent have occurred. In the Australian context, it is now well established that online standard form agreements are typically enforceable, irrespective of whether or not a consumer reads the contents of a contract. As long as the terms are presented in a transparent and physically obvious way, then consent is presumed to be valid.[1]

Comparable to other developed countries, Australia lags behind international standards when it comes to data protection regulation and lacks an adequate regulatory approach and framework for the protection of consumer data. As online activity increases, Australia must develop a privacy framework that is cohesive, evolving and provides adequate protection. While the recent Consumer Data Right ('CDR') and Digital Platform Inquiry are steps in the right direction, the Australian Government's weak response and implementation roadmap for the Digital Platform Inquiry evidences scope for improvement.

This chapter analyses the Australian privacy framework. Each of the regulatory instruments that comprise the framework are discussed in detail alongside the CDR and the findings of the Digital Platform Inquiry. Informed consent and the attitudes to unfairness and unconscionability is reviewed in the context of each of the regulatory instruments and inquiries. Finally, solutions are offered to the current patchwork approach. These solutions are analysed against and add to those which are proposed through the Implementation Roadmap developed from the Digital Platform Inquiry. The proposals for reform are split into quick policy wins and long-term solutions. The quick policy wins centre on three specific changes, including definitional updates, content and structure of online standard form agreements and enforcement, penalties and sanctions, and long-term solutions. The long-term solutions are proposed to include regulation of website design, better integration of the laws, regulators and enforcement bodies, a faster, more consistent pace of policy review and recognition of the societal and human benefit of informed consent to online standard form agreements.

---

[1] Kate Mathews-Hunt, 'CookieConsumer: Tracking Online Behavioural Advertising in Australia' (2016) 32(1) *Computer Law and Security Review* 55.

6.2 Australia's Current Privacy Framework

Australia's current approach to the protection of privacy is a 'patchwork of specific legislation'.[2] The regulatory instruments relied on for the enforcement of consumer data and privacy rights are the *Privacy Act 1988* (Cth) ('*Privacy Act*'), *Australian Consumer Law* (contained in Schedule 2 of the *Competition and Consumer Act 2010* (Cth)) ('*ACL*'), *Australian Securities and Investments Commission Act 2001* (Cth) ('*ASIC Act*') and the *Australian Information Commissioner Act 2010* (Cth), all of which to some extent attempt to define, address and mitigate the impact of unfair and unconscionable online standard form agreements that have the potential to result in privacy and data breaches. The *Privacy Act* has been the main regulatory instrument used on to regulate data privacy for the past 30 years, despite the fact that the provisions were drafted with at a time when digital platforms were far from the prevailing market platform they have become today.

In December 2017, Australian Prime Minister Scott Morrison launched an inquiry into the operation of digital platforms. Until now, Australian regulators had not made any meaningful effort by to reflect upon and understand how digital platforms were impacting consumers, society, trade and commerce. There was also limited recognition of the procedural and contextual differences between traditional face-to-face commercial transactions and transactions occurring in online environments, and virtually no attempt to statutorily define the roles and responsibilities of businesses in the context of e-commerce. As Meese explains:

> Despite embracing some European tendencies, as a whole Australia has missed an opportunity to reshape the conversation around data protection. Instead, it has presented a limited data policy that locates the vast majority of substantive rights within the context of the market.[3]

The Australian privacy framework has failed to keep up the protection and conferral of additional rights that are imperative to the efficient functioning of online marketplaces. The result has been an unsatisfactory environment where there is no 'right to be forgotten', no 'data portability' rights and no right to object to the processing of personal information (such as profiling).[4] These are just a few of the current failings.

As is demonstrated in Article 1, unfair and unconscionable terms are routinely included in online standard form agreements and there is an undeniable lack of informed consumer consent to these agreements. Despite the presence of these vitiating elements, the agreements are routinely enforced. Below, each of the regulatory instruments and reviews that make up the current Australian data protection framework are discussed in the context of how they each reference or approach unfairness, unconscionability and informed consent.

6.2.1 *Privacy Act*

Despite the fact that Australia is signatory to the International Convention on Civil and Political Rights, the international law right to privacy conferred under Article 17 has not been enacted into domestic legislation. Therefore, Australians are not, in a regulatory sense, entitled to the general law right of privacy and there are no constitutional protections afforded to Australians through Commonwealth legislation.

---

[2] James B Rule and Graham William Greenleaf, *Global Privacy Protection: The First Generation* (Edward Elgar Publishing, 2010).
[3] James Meese, Punit Jagasia and James Arvanitakis, 'Citizen or Consumer?: Contrasting Australia and Europe's Data Protection Policies' [2019] *Internet Policy Review*.
[4] Samson Yoseph Esayas and Angela Daly, 'The Proposed Australian Consumer Right to Access and Use Data: A European Comparison' (2018) 2 *Eur. Competition & Reg. L. Rev.* 187.

The *Privacy Act* establishes a legislative framework for the protection of 'personal information' in Australia. Personal information is defined as 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion'.[5] The Act applies to data companies and any private and non-profit organisations with an annual turnover of more than AU $3 million. Thirteen privacy principles (known as the Australian Privacy Principles or APP) are integrated into the *Privacy Act* and these are purposed with, inter alia, regulating the collection, use, storage and disclosure (collectively handling) of defined 'personal information', and to provide a consumer right to access and correct that information. Consent is defined in the Act to be either 'express' or 'implied'.[6]

While the *Privacy Act* imposes minor obligations on companies collecting data and trivial protections for consumers, the penalties imposed for violation of the *Privacy Act* are only applicable to serious or repeated invasions of privacy. Also, the *Privacy Act* does not contain a private enforcement mechanism affording victims of online privacy and data breaches an avenue for lodging a claim. However, the main shortcoming centres on the fact that the provisions do not apply to most of the private sector. Only organisations with an annual monetary turnover of $A3,000,000 are required to comply with its provisions, with some limited exceptions. Approximately 85% of Australian businesses are exempt from the provisions, as they do not apply to small business operators, unless they are responsible for collecting and handling health information. [7] This is a significant factor in the European Commission's determination that Australia's information privacy laws are not deemed to provide 'an adequate level of data protection' under Article 25(2) of the EU Directive 95/46/EC and have not received endorsement under the European Union's General Data Protection Regulation (GDPR).

Australia's information privacy regimes are overseen by a Privacy Commissioner responsible for resolving complaints. Before a complaint can be heard by a privacy commissioner, consumers must first lodge their complaint directly with the offending organisation. Complaints can only be escalated to the Office of the Australian Information Commissioner (OAIC) if the offending organisation has ignored their complaint, or if the complaint was not dealt with in a satisfactory manner. At a Commonwealth level, the Information Commissioner can initiate enforcement proceedings and is able to issue fines of up to AU $2,100,000. To date, however, no enforcement actions have taken place and no fines have been issued.

Unfair and unconscionable behaviour is not referenced in the *Privacy Act*.

6.2.2 *Australian Consumer Law*

Consumer protection laws are typically designed to ensure that consumers make an informed choice when entering into specific transactions.[8] In the context of online standard form agreements, the laws seek to ensure that reasonable consumer expectations are upheld, particularly regarding privacy and data security, and offer effective remedies in relation to privacy violations.[9]

The *Australian Consumer Law* (***ACL***) is contained in Schedule 2 of the *Competition and Consumer Act 2010* (Cth) (***CCA***). The *CCA* and the *ASIC Act* both contain laws pertaining to

---

[5] *Privacy Act*.
[6] Ibid.
[7] David Watts and P Casanova, 'Privacy and Data Protection in Australia: A Critical Overview' (W3C, 2018).
[8] Garry Clements, *Australian Consumer Law Review Issues Paper* (2016).
[9] Ibid.

unfair contract terms. According to the ACCC, the unfair contract term protections apply to standard form consumer contracts for the supply of goods and services, or for the sale or grant of an interest in land, to an individual for personal, domestic or household use.

The *ACL* has potentially useful public and private enforcement mechanisms. Chapter 2 offers general protections which create standards of business conduct in the market. The general prohibitions on misleading conduct (s 18), unconscionable conduct (s 21) and provision of false or misleading representations (s 29) all have potential application to situations arising where privacy is breached or when unfair and/or unconscionable terms are integrated into online standard form agreements. Despite not having been used in the enforcement of a consumer data right violation in the context of online standard form agreements, we have recently seen the ACCC testing the waters, as evidenced by the ACCC's actions against Google discussed below and a number of cases against companies who have included unfair contract terms in traditional standard form agreements.[10]

Section 18 of the *Australian Consumer Law* is particularly interesting. It states '[a] person must not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive'. In the 2013 case *Google v ACCC* [2013] HCA 1, a test was outlined that sought to facilitate the determination of whether of whether ordinary or reasonable members of a class of people were affected by the conduct would be deceived or mislead. It was concluded that Google was 'not relevantly different from other intermediaries, such as newspaper publishers (whether in print or online) or broadcasters (whether radio, television or online), who publish, display or broadcast the advertisements of others.'[11]

According to interpretations of the *ACL*, unconscionable conduct is that which is particularly harsh or oppressive.[12] Unconscionable conduct is against conscience as judged against the norms of society. Chapter 2 also states that unfair contract terms in consumer contracts are void. With unfairness being defined as a significant imbalance in the parties' rights and obligations arising under the contract; it is not reasonably necessary to protect the legitimate interests of the supplier; and it would cause financial or non-financial detriment to a party.

6.2.3 Consumer Data Right

In May 2017, the Australian Productivity Commission released a report titled 'Data Availability and Use'. This report investigated ways to improve the availability and use of public and private sector data. Specifically, the Commission looked at the benefits and costs for making more data available, analysed options for the collection, sharing and release of data, identified methods for consumers to access data – particularly their own and considered solutions for ensuring that individual privacy and control over data use was sustained.[13]

Among the final recommendations provided in the report was the creation of a new consumer data right that would support the existing privacy regulation. In November 2017, the Australian Government announced that the CDR would be introduced. The CDR was the first time the Australian government had attempted to take reformist approach towards online privacy and data collection. Instead of following the well-worn path of making minor changes and incremental amendments to existing legislation, the CDR invited major

---

[10] See for example *Australian Competition and Consumer Commission v Ashley & Martin Pty Ltd* [2019] FCA 1436.
[11] *Google Inc v Australian Competition and Consumer Commission* [2013] HCA 1.
[12] *Competition and Consumer Law Act 2010 (Cth) Sch 2 ('Australian Consumer Law')*.
[13] Productivity Commision, *Inquiry Report - Data Availability and Use* (2017).

reforms.[14] As Meese and Jagasia conclude: '[t]he CDR provides Australians with better data protection by enhancing existing privacy protections and providing meaningful redress for individuals.'[15]

The CDR recognised that 'free' services often fall out of the scope of consumer law. The new laws are designed to give consumers greater access to and control over their data, improve consumers' ability to compare and switch between products and services, and encourage competition between service providers.[16]

While the *Privacy Act* already provides Australians with the right to access their 'personal information'. Personal information only accounts for a small amount of the data footprint that individuals generate and leave behind on a daily basis.[17] The CDR will also provide a standardised way for individuals to access their data, across different platforms. Under the existing legislation, government bodies and companies were permitted to refuse the request for access to an individual's personal information if the request was not 'reasonable and practicable' to fulfil.[18] Individuals could also be charged for access to their own information. The CDR will provide individuals and businesses with the right to access and transfer data that 'relates' to them and data that is relevant to the products they use.[19] Thirteen 'Privacy Safeguards' are incorporated into the new regulation.[20]

Entities receiving transfers of consumer data must first be accredited by the ACCC.[21] The process of accreditation will ensure compliance with the relevant privacy and security safeguards. While inherently similar, the safeguards are designed to exceed the protections currently provided through the *Privacy Act*'s Australian Privacy Principles.[22] Most significantly, the CDR can also apply to small to medium enterprises previously exempt from the *Privacy Act* 1988, who have an annual monetary turnover of less than AUD3,000,000 and who voluntarily go through the accreditation process. However, these voluntarily accredited entities still remain free from compliance with the *Privacy Act 1988* (Cth).

Given the disapproving international perception of Australia as a nation that values an individual's right to privacy, the CDR has, perhaps necessarily, been pitched as sector-leading reform that will rectify the deficiencies of the existing regulatory approaches and elevate the nation to the status of a sector leader. However, as Meese and Jagasia advise:

> [t]his framing is based on an unsupported belief in the power of big data (see Tene and Polonetsky, 2012), a limited understanding of the associated risks and an inaccurate framing of the Australian legislative environment (see Nissenbaum, 2017).[23]

Further, the Australian Government will remove '500 existing data secrecy and confidentiality provisions across more than 175 different pieces of Australian Government legislation'[24] to make the safeguards possible. As cautioned by Meese and Jagasia, this practice will remove:

---

[14] Meese, Jagasia and Arvanitakis (n 3).
[15] Ibid.
[16] Australian Competition and Consumer Commission, *Explanatory Statement Proposed Competition and Consumer (Consumer Data Right) Rules 2019 – August 2019* (2019) https://www.accc.gov.au/system/files/Proposed CDR rules - Explanatory Statement - August 2019.pdf.
[17] Meese, Jagasia and Arvanitakis (n 3).
[18] Office of the Australian Information Commissioner, *Australian Privacy Principle Guidelines* (2018) https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/.
[19] Australian Competition and Consumer Commission (n 16).
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Meese, Jagasia and Arvanitakis (n 3).
[24] *The Australian Government's Response to the Productivity Commission Data Availability and Use Inquiry* (2018).

> substantive protections for the benefit of researchers and government, with the promise of vague positive outcomes in the future, with the bill empowering the government to 'authorise data sharing and release' for broad purposes like 'supporting the efficient delivery of government services or government operations.[25]

This means that while Australians will have greater access to their own data and personal information and improved abilities to transfer this information, it will be in exchange for allowing the sharing of public data between public and private organisations under a liberal risk assessment model.[26]

Consumer consent and authorisation is addressed in section 7 of the Consumer Data Right Rules Outline. Consent is limited to a period of 12 months. Section 7.10 provides a refreshingly comprehensive definition of valid consent. That includes the important recognition of complex and multifaceted nature of consent, that is particularly pertinent to online standard form agreements. Specifically:

a) Consent must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

   Consent must be voluntary and consistent with the OAIC's Australian Privacy Principles guidelines on voluntary consent. Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where duress, coercion or pressure is applied by any party involved in the transaction. Factors relevant to deciding whether consent is voluntary include:

   i) the alternatives open to the individual if they choose not to consent

   ii) the seriousness of any consequences to the individual if they choose not to consent

   iii) any adverse consequences for family members or associates of the individual if the individual chooses not to consent.

b) An accredited data recipient must not make consent a precondition to obtaining another unrelated product or service. The collection of CDR data must be reasonably necessary or required to provide the service the accredited data recipient is offering.

c) An accredited data recipient must not bundle consent with other directions, permissions, consents or agreements.

d) An accredited data recipient must present each consumer with an active choice to give consent, and consent must not be the result of default settings, pre-selected options, inactivity or silence.[27]

Surprisingly, unfair and unconscionable behaviour is not referenced in the Consumer Data Right Rules Outline.

The CDR is regulated by both the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC). This is because the content covers both competition and consumer issues, as well as the privacy and confidentiality of consumer data. According to the Explanatory Statement for the Proposed Competition and Consumer (Consumer Data Right) Rules 2019 – August 2020:

> [t]he ACCC leads on issues concerning the designation of new sectors of the economy to be subject to the CDR and the establishment of the CDR rules. The OAIC leads on matters relating to the protection of individual and small business consumer participants' privacy and confidentiality, and compliance with the CDR Privacy Safeguards (Privacy Safeguards).[28]

---

[25] Meese, Jagasia and Arvanitakis (n 3).
[26] Ibid.
[27] *Consumer Data Right Rules Outline 2019*.
[28] Australian Competition and Consumer Commission (n 16).

The legislation will apply sector by sector. The banking sector was first, with legislation taking effect on 1 February 2020. The energy and the telecommunications sectors are next thereafter. The Treasurer will then determine further sectors to which the right should apply.[29] The CDR is a step in the right direction in terms of recognition that data privacy is a complex issue, breaking down the many silos that exist in the current Australian privacy framework.

6.2.4 Digital Platforms Inquiry

In the same year the Australian Productivity Commission released their report on data availability and use, the Australian Treasurer instructed the ACCC to conduct an inquiry into digital platforms. The purpose of the inquiry was to examine 'the effect that digital search engines, social media platforms and other digital content aggregation platforms have on competition in media and advertising services markets'.[30] The main targets of the inquiry were tech giants including Google and Facebook, and the power they wield over media, advertising and consumers. It was the first attempt by Australian regulators to reflect on the role, responsibilities and impact that digital platforms have had on competition, consumers, society and the Australian economy. Analogous with the CDR, the Digital Platform Inquiry focused on data privacy and access, as well as the effect that digital search engines, social media platforms and other digital content aggregation platforms have on competition in media and advertising services markets.[31] Until this time, Australian regulators had failed to adequately account for the roles and responsibilities of digital platforms in the markets in which they operate. The DPI criticised the piecemeal approach to updating the *Privacy Act* over the past 30 years, and how this approach had resulted in an ineffective and inappropriate regulatory framework.

The final report provided 23 recommendations aimed at identifying and minimising potentially adverse consequences that result from the growth of digital platforms and aligning Australia's privacy laws with the European GDPR.

The final report identified the social and economic benefits derived from ensuring that consumers have the information and access they need to make informed choices which are aligned with their privacy preferences. The report also recognised that the current digital platform environment often prevents consumers from being able to make informed decisions and concluded that digital platform operators have the ability to design user interfaces that will lead users to make privacy-intrusive selections.[32] Digital platforms can be designed to appeal to certain psychological or behavioural biases, using features such as privacy-intrusive defaults or pre-selections.[33] The Inquiry concluded that the Australian regulatory framework does not adequately address data practices, such as website design principles, that are intended to exploit the information asymmetries, behavioural biases and power imbalances between digital platforms and reasonable users of the internet.[34] These characteristics, taken individually or as compounding factors, make it near impossible for consumers to provide meaningful consent to online standard form agreements.

The report also called for specific consent protocols for data practices that were of particular concern to consumers and accompanying legislation and penalties for companies violating or misappropriating consumer consent and data. The overwhelming majority of

---

[29] *Consumer Data Right Rules Outline 2019*.
[30] Australian Competition and Consumer Commission (n 16).
[31] Ibid.
[32] *Digital Platforms Inquiry Final Report* (2019) https://www.accc.gov.au/system/files/Digital platforms inquiry - final report.pdf.
[33] Ibid.
[34] Ibid.

Australians surveyed for the DPI believed that there should be transparency and choice in how digital platforms should collect, use and disclose certain types of user data.[35] The surveyed Australians believed that platform providers should tell users who they are providing their personal information to and only collect information needed to provide their products or services.[36] Three data practices were identified to be of particular concern. These included location tracking, online tracking for targeted advertising purposes, and the disclosure of user data to third parties.[37]

According to the final report, the current unfair contract terms (UCT) provisions included within the *Australian Consumer Law* do not have adequate application to digital platforms. While, in theory has application, unfair contract terms provisions take into account tests of reasonableness and fairness and have application to online standard form agreements in the same way that they do to paper-based transactions, case law suggests that this is not been the definitive approach.[38] Recommendation 20 advocates for the extension of the *Australian Consumer Law* UCT provisions to digital platforms. According to Greenleaf et al '[t]his recommendation would allow the ACCC to hold businesses (including digital platforms) to account for including UCTs, not just to have UCTs declared void (as is currently the case).'[39] Greenleaf et al also recommend extending and increasing the penalties to businesses relying on unfair contract terms.[40]

Informed consent to online standard form agreements was also addressed in the final report. Clickwrap agreements, take-it-or-leave-it terms, and bundling of consent were all problematic practices and contractual attributes identified to degrade the quality of consent in online standard form agreements.[41] The privacy policies used by digital platform providers are often long, complex and purposefully vague.[42] Between platforms, there are also conflicting and contradictory definitions of key terms such as 'personal information' and 'products'. For example, Facebook's privacy policy defines products to include 'Facebook, Messenger, Instagram as well as the Facebook Business Tools used by website owners, publishers, app developers, business partners and their customers'.[43] The report outlined a series of conditions for valid consent in online environments. These included a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). The final report suggests that 'any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled.'[44] Specifically, Recommendation 16(c) advocated for strengthened consent requirements and pro-consumer default standards that would require a company to obtain authorisation to collect, use or disclose a consumer's personal information, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.[45]

---

[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Graham Greenleaf et al, 'Regulation of Digital Platforms as Part of Economy-Wide Reforms to Australia's Failed Privacy Laws (Australian Privacy Foundation Submission to the Australian Government on Implementation of the ACCC's Digital Platforms Inquiry—Final Report)' [2019] *SSRN Electronic Journal*; Mathews-Hunt (n 1).
[39] Ibid.
[40] Ibid.
[41] *Digital Platforms Inquiry Final Report* (n 32).
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.

According to the CDR, consumers must 'opt-in' to data collection, rather than 'opt-out', as is the current approach. The Australian Privacy Foundation agreed with this recommendation, and further suggested that protections could be strengthened by:

> specifically stat[ing] that the onus of proof of compliance with all consent conditions lies with the collector of the information; that separate consents should be required for each separate purpose (unbundling of bundled consents); and that information for which consent is required should be unbundled from any information for which consent is not required; that the related secondary purpose within reasonable expectations test must also be tightened; and that the take it or leave it approach to consent should be clearly interpreted as an unfair term.[46]

The ACCC also recommends that the current definition of 'consent' be updated in the *Privacy Act* to require a clear affirmative act that is freely given, specific, unambiguous and informed.[47] Suggestions for modifications centred on procedural change, in particular that a clear affirmative act should be required to establish consent. As acknowledged in the GDPR 'Silence, pre-ticked boxes or inactivity should not therefore constitute consent'.[48] Modifying the definition of consent to better align with the European GDPR in terms of the standard of data protection, would be a step in the right direction.

The ACCC advised that the application of the CDR to digital platforms would be considered during the process of determining which sectors the framework would apply to in the future.[49]

In December 2019, the federal government responded to the ACCC's Final Report. Of the 23 recommendations made, only six recommendations were supported in their entirety and 10 were supported 'in principle' (with plans for further reviews). The federal government 'noted' five others, and rejected two. A detailed implementation roadmap outlining the activities that will be undertaken over the next two years was included in their response. Unfortunately, this level of detail also highlighted the deficiencies in the Australian Government's approach and emphasised the fact that there is still a great deal of room for improvement. Unfortunately, even with the government's proposal for further legislative reviews across a number of areas, including the application of unfair contract terms to small business and consumer loyalty schemes, this plan offers only the mere possibility of improvement to consumer privacy protections. And even if these eventuate, they are still a long way away.

6.3 Limitations of the current regulatory regime in Australia

The failure of the current regulatory regime is evident through the fact that there are not, to the author's understanding, any public or private actions initiated by Australian consumers against companies for exploitation of data privacy rights, despite the fact that these breaches have been widely reported in the mainstream news. There are also very few cases referencing informed consent in the context of standard form agreements and even fewer references to online standard form agreements, even though it is a fundamental element of traditional contract law theory that is violated on almost every occasion an individual enters into an online standard form agreement. Despite the reality that consumers do not read standard form agreements and therefore, cannot have provided 'informed consent', online standard form agreements are routinely enforced, and consent is deemed to be valid.

Through the patchwork legislative framework described above, there are significant gaps and many contributing factors in the failure of Australia's current regime. Foremost among these gaps is the reality that there is no general law right to privacy for Australian citizens.

---

[46] Greenleaf et al (n 38).
[47] *Digital Platforms Inquiry Final Report* (n 32).
[48] Ibid.
[49] Ibid.

Even though Australia is a signatory to the International Convention on Civil and Political Rights, the rights afforded through this convention on topics have not been enacted in Australia's domestic law. Further, unlike Europe, where the focus is on the human rights perspective, Australia's regulatory regime is devised through an economic lens. Free and efficient markets are valued foremost, with human rights considerations being secondary considerations.

Sanctions and penalties under Australian information privacy laws are comparatively weak when compared to the European Union, particularly when compared to the sanctions available under the GDPR. For example, the maximum penalty for violations of the GDPR exceeds € 20 million. The enforcement of the GDPR is regulated by a supervisory authority in each member state. While in Australia, each of the information privacy regimes are overseen by a Commissioner. Privacy Commissioners are, in broad terms, given responsibility for resolving privacy complaints – typically through a conciliation process. At a Commonwealth level, the Information Commissioner has a role in initiating enforcement proceedings leading to fines of up to $A2.1 million.[50]

6.4 Solutions

Over the past 30 years, suggestions for amendment to Australia's current framework have typically focusing on providing consumers with more information and more notice,[51] others have also suggested that the process of deidentifying personal data may mitigate privacy concerns or that the provision of a cooling-off period could provide a non-drafting party with more time to reflect on their decision and change their mind.

In December 2019, the Australian Government published the 'Regulating in the Digital Age' report and implementation roadmap in response to the ACCC's Digital Platform Inquiry. The report addressed each of the 23 recommendations outline in the ACCC's report. However despite the recognition that there is a need for reform in order 'to better protect consumers, improve transparency, recognise power imbalances and ensure that substantial market power is not used to lessen competition in media and advertising services markets'[52] only 6 of ACCC's recommendations were categorically supported and 4 immediate commitments to change proposed. The immediate commitments include:

- the establishment of a special unit in the ACCC to monitor and report on the state of competition and consumer protection in digital platform markets, take enforcement action as necessary, and undertake inquiries as directed by the Treasurer, starting with the supply of online advertising and ad-tech services;
- address bargaining power concerns between digital platforms and media businesses by tasking the ACCC to facilitate the development of a voluntary code of conduct;
- commence a staged process to reform media regulation towards an end state of a platform-neutral regulatory framework covering both online and offline delivery of media content to Australian consumers; and
- ensure privacy settings empower consumers, protect their data and best serve the Australian economy.[53]

---

[50] Office of the Australian Information Commissioner, 'Mandatory Data Breach Notification Comes into Force This Thursday' (online at 19 February 2018) https://www.oaic.gov.au/updates/news-and-media/mandatory-data-breach-notification-comes-into-force-this-thursday/.
[51] Katharine Kemp and Ross P Buckley, 'Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model' (2017) 18(3) *Georgetown Journal of International Affairs* 35.
[52] Josh Frydenberg, Paul Fletcher and Christian Porter, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (2019).
[53] Ibid.

The Australian Government's undeniably pro-business approach is defended by the disclaimer included in their response to the Digital Platform Inquiry that states:

> The Governments role is not to protect domestic businesses from digital competition, but rather to ensure the proper functioning of markets and a fair approach to regulation that ensures the rules of the physical world apply equally to the digital world.[54]

The reliance on a voluntary code of ethics is evidence enough that the issue of consumer protection in online standard form agreements is not being taken seriously.

Therefore, I conclude that the Australian Government's response is not an adequate response nor set of suitable solutions to the problem. Instead, I propose a two-pronged approach that recognises the urgency of the issue through the suggestion of a series of 'quick policy wins' that will result in more meaningful and effective protection for consumers and further systemic, long-term recommendations for change that can be achieved through policy development, further consultation and integration with other existing legislation.

The quick policy wins are aligned against three categories of change, and include definitional updates, content and structure of online standard form agreements and enforcement, penalties and sanctions. Long term solutions are proposed to include regulation of website design, better integration of the laws, regulators and enforcement bodies, a reviewed pace of policy review and recognition of the societal benefit of informed consent to online standard form agreements. Each of these proposals are also discussed in light of the Australian Government's recent response to the Digital Platform Inquiry.

6.4.1 Quick wins

6.4.1.1 Definitions

It was made clear through the Digital Platform Inquiry and CDR final reports that there is an urgent need to update the definition of key privacy concepts in the context of online standard form agreements. As outlined in their response to the Digital Platform Inquiry, the Australian Government agree with this. It is of critical importance to the Australian privacy framework that the definition of 'personal information' and 'informed consent' are updated and standardised across all regulatory instruments. These two concepts are discussed in detail below. Other terms requiring updated or new definitions include sensitive data, free services, trackable information, collection necessity and related purpose.

Personal information

'Personal information' is defined in the *Privacy Act* as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable'.[55] In the context of digital platforms, it is unclear whether this definition encompasses metadata such as IP addresses, other location data, or other technical data.[56]

Unfortunately, neither the Digital Platform Inquiry nor the CDR attempted to redefine 'personal information'. While the ACCC welcomed the changes proposed under the Digital Platform Inquiry, including updating the definition of personal information to ensure that the current and likely future technological developments in technology impacting the collection of identifiable personal information can be covered, a revised definition was not provided.

---

[54] Ibid.
[55] *Privacy Act* (n 5).
[56] *Digital Platforms Inquiry Final Report* (n 32).

The Australian Government's response[57] supported the definitional update 'in principle', however acknowledged that:

> the Government will consult further on this recommendation to ensure that the definition of 'personal information' captures technical data and other online identifiers that raises privacy concerns and that any amendments to the definition do not impose an unreasonable regulatory burden on industry.

On the other hand, the CDR focuses on defining 'customer data' instead of 'personal information'. Accordingly, customer data includes 'other identifying information, including where that information assists to distinguish one consumer from another.' One key exemption is the specific exclusion of an individual's date of birth from the classification of 'customer data'.[58]

Two of the largest digital platforms, Google and Facebook, each have different approaches to defining personal information in their privacy policies. The breadth of the respective definitions of, and references to, personal information being manifestly drafted in a way that best suits each company's interests. For example, Google describes personal information as:

> information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account'.[59]

Facebook, on the other hand, does not specifically reference 'personal information'. Instead references to 'information that personally identifies you' is explained to encompass 'information such as your name or email address that by itself can be used to contact you or identifies who you are'.[60]

The European Union's Data Protection Directive 1995 (95/46/EC) refers to 'personal data' as 'any information relating to an identified or identifiable natural person ('data subject')'.[61] 'An identifiable natural person' is defined as 'one who can be identified, directly or indirectly'.[62] This broad definition ensures that the Directive covers data that does not directly identify an individual, but may assist in identifying them. Online and device identifiers such as IP addresses, cookies, or device IDs, location data, usernames, and pseudonymous data are also covered by this definition.[63]

Informed consent

The definition of informed consent varies between each jurisdiction and between each sector. In Australia, consent is defined in the *Privacy Act 1988* (Cth). Accordingly, consent can be 'express' or 'implied' consent.[64] The *Privacy Act* does not outline any criteria for valid or informed consent. While, according to the Australian Guidelines to the National Privacy Principles, express consent is given explicitly, either orally or in writing.[65] On the other hand,

---

[57] Frydenberg, Fletcher and Porter (n 55).
[58] *Digital Platforms Inquiry Final Report* (n 32).
[59] Ibid.
[60] Ibid.
[61] *Article 4 EU General Data Protection Regulation 2016*.
[62] Ibid.
[63] 'The EU General Data Protection Regulation', *Human Rights Watch* (2018) https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation.
[64] *Privacy Act* (n 5).
[65] Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2019) https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf.

implied consent arises where consent may be reasonably inferred in the circumstances from the conduct of the individual and the organisation.[66]

In the European Union, the focus of the definition outlined in Article 2(h) of Data Protection Directive 1995 (95/46/EC) is on freely given permission, the exercise of real choice and a lack of coercion:

> Consent is any freely given specific and informed indication of the data subjects wishes by which the data subject signifies his or her agreement to personal data relating to him/her being processed.

Further, according to the Article 29 Data Protection Working Party Opinion 15/2011 consent:

> [c]an only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation coercion or significant negative consequences if he or she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free.

The Australian definition of informed consent should be updated to require clear affirmative act that is freely given, specific, ambiguous and informed. This would amend Australian legislation to be in line with standards of GDPR. An updated approach to the ensuring informed consent was the basis of the ACCC's DPI recommendation 16(c). However, again in their response to the DPI, the Australian Government indicated that this recommendation was only supported in principle and would be subject to consultation to ensure that entities drafting standard form agreements are not subject to significant regulatory burden and ensuring individuals do not suffer from 'consent fatigue'.

6.4.1.2 Content of Online Standard Form Agreements

There are a series of simple and effective updates to the *Privacy Act* that would result in an improved consumer understanding and awareness of key terms and conditions included in online standard form agreements. These include:

- The unbundling of consent and an opt-in approach. The default setting for consumer data collection is the 'opt-out' approach, whereby consumers must explicitly indicate that they do not agree to their data being collected. Bundled consent refers an entity using a single document or single request process to ask an individual to consent to a wide range of collections, uses and disclosures of their personal information, without giving them the opportunity to choose which of those collections, uses and disclosures they are willing to consent to.[67] An unbundled approach would require consumers to explicitly click 'agree' or 'accept' next to every request to collect, store and use personal information.
- At present, the vast majority of online standard form agreements do not have an expiration date. Custers aptly named his article on this topic, 'Click here to consent forever'.[68] All online standard form agreements must either be renewed after a certain period of time or lapse at the conclusion of each period. The Explanatory Statement for the Proposed Competition and Consumer (Consumer Data Right) Rules 2019 – August 2022 mandates that a period over which CDR data will be collected and used, is up to a maximum of 12 months.
- A restructuring of online standard form agreements to a predictable format should also be actioned. Privacy information ought to be located in the very beginning of the agreement in a box or designed element that differentiates the content from the

---

[66] Ibid.
[67] Office of the Australian Information Commissioner (n 18).
[68] Bart Custers, 'Click Here to Consent Forever: Expiry Dates for Informed Consent' (2016) 3(1) *Big Data & Society* 2053951715624935.

hundreds of pages of mind-numbing text. This is to minimise the effect of consent fatigue and to increase the likelihood that the policies will be read.

- One final possibility, offered by Hillman, may be for the law to mandate protective terms that are most important to consumers.[69] Such an approach, however, would be at the expense of the consumer's freedom of contract and undoubtedly, there would be lengthy deliberations over which terms ought to be mandatory. Specific examples of terms that could be standardised include forum selection, warranties, expiration dates, unilateral modification and dispute resolution.

6.4.1.3 Enforcement, Penalties and Sanctions

Some scholars argue that market failures are the result of market concentration and monopoly power.[70] Online marketplaces and platforms are hubs of monopolistic behaviour and this has led to serious concerns about competition problems in the digital economy and how competition laws should be designed to deal with these issues. Uncompetitive markets, including social media (Facebook) and search engines (Google) result in consumers being taken advantage of. This exploitation can be prevented if courts begin to apply and enforce the unfair contract terms in the context of online standard form agreements. However, recent action by the Australian Government suggests that they will not be implementing the recommendation provided in the Digital Platform Inquiry to apply unfair contract terms provisions to digital platforms. Instead, the government has noted this, and promised there will be consultation on a range of policy options to strengthen unfair contract term protections.[71]

Divisively, Hillman proposes the abandonment of the requirement to disclose terms in their entirety.[72] Instead, he suggests a reliance on unconscionability to police exchanges for unfairness once a dispute arises.[73] However, Hillman also acknowledges that in the US, the unconscionability doctrine has been unsuccessful in corralling advantage-taking by unscrupulous vendors and that such an approach is a dramatic limitation on the notion of manifest assent.[74]

It is widely documented that the Office of the Australian Information Commissioner has been ineffective at policing and enforcing data breaches.[75] An alternative solution offered through the Digital Platform Inquiry is for the ACCC to take on enforcement responsibilities. Such an approach would make sense, especially if the consumer protections offered under the *Australian Consumer Law* were extended to digital platforms. The establishment of a special unit in the ACCC to monitor and report on the state of competition and consumer protection in digital platform markets was, however, a step in the right direction. This special unit will be responsible for undertaking enforcement action as necessary, and initiating inquiries as directed by the Treasurer, starting with the supply of online advertising and ad-tech services.[76]

---

[69] Robert A Hillman, 'Consumer Internet Standard Form Contracts in India: A Proposal' (2017) 29(1) *National Law School of India Review* 70.
[70] Aditi Bagchi, 'At the Limits of Adjudication: Standard Terms in Consumer Contracts' http://papers.ssrn.com/abstract=2772733.
[71] Katharine Kemp and Rob Nicholls, 'The Federal Government's Response to the ACCC's Digital Platforms Inquiry Is a Let down', (*The Conversation* online 12 December 2019) https://theconversation.com/the-federal-governments-response-to-the-acccs-digital-platforms-inquiry-is-a-let-down-128775.
[72] Hillman (n 69).
[73] Ibid.
[74] Ibid.
[75] Greenleaf et al (n 38).
[76] Frydenberg, Fletcher and Porter (n 52).

Greenleaf et al's argument for the extension of penalties to businesses relying on unfair contract terms should also be considered.[77] The usual practice is for unfair contract terms to be declared void, however, in the context of online standard form agreements this would have little significance, particularly because most online agreements have zero monetary price. According to Greenleaf et al, in these transactions 'the impact of declaring a term void is less likely to have immediate impacts on the parties' financial rights and obligations'.[78] The introduction of financial penalties could become an effective deterrent, especially given the volume of transactions online standard form agreements affect. The State, Territory and Federal consumer affairs Ministers' agreement in November 2020 to move forward with changes to the *ACL* making unfair contract terms unlawful, and introducing civil penalties for breach, is to be welcomed, although no draft legislation has yet been released.[79]

Finally, tort law should also be applied for serious invasions of privacy. The recommendation, included in the ACCC's Digital Platform Inquiry Final Report, has been supported by the federal government in their response to the final report and earlier, in 2014, by the government and the Australian Law Reform Commission. On 12 December 2019, the Australian Government announced a review of the *Privacy Act*, including 'whether a statutory tort for serious invasions of privacy should be introduced into Australian law'.[80]

6.4.2 Systemic Long-Term Change

These changes require further policy development and planning.

6.4.2.1 Website Design Regulation

Online environments are being designed to exploit consumers in ways that they may not even realise. The visual interface affords the drafting party considerable opportunities to shape how consumers interact with their platform. In the absence of specific regulation governing design interfaces, online platforms are created intentionally to deepen information asymmetries and to allow consumers to agree to terms with minimal thought and consideration. The introduction of website design regulation, that requires the developer to draw the user's attention to any instance where a contract is entered into or their legal rights are being impacted, offers another potential solution for increasing the likelihood of ensuring informed consent to online standard form agreements.

In the absence of a specific professional body, code of ethics, or any other successful form of regulation of web design worldwide, we are beginning to see web designers create their own set of professional practices. The web standards movement is one such example, and other initiates have centred around accessibility and cultural sensitivity. Some argue that the self-regulation of web design has been met with unprecedented success.[81]

6.4.2.2 Better Integration of the Laws, Regulators and Enforcement Bodies

While the incremental revision of legal obligations through the *Privacy Act* is a conventional regulatory response to the evolving needs and preferences of a society over time, the unprecedented pace of technological change in the context of digital platforms means that such a response is inadequate in this setting. It has been argued throughout this chapter

---

[77] Greenleaf et al (n 41).
[78] Ibid.
[79] Michael Sukkar MP, 'Penalties to be introduced for unfair contract terms', (*Media Release*, 10 November 2020) http://www.michaelsukkar.com.au/ministerial-media-releases/penalties-to-be-introduced-for-unfair-contract-terms/
[80] Attorney-General's Department, Commonwealth of Australia, 'Review of the *Privacy Act* 1988', https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.
[81] Helen Kennedy, 'The Successful Self-Regulation of Web Designers' (2010) 10(3) *Ephemera: Theory & Politics in Organization* 374.

that the broad, general protections bestowed on consumers through the *Australian Consumer Law* and CDR should be better integrated role to protect consumers entering into online standard form agreements. Informed consent in the context of online standard form agreements has foundations in competition, consumer, and data protection and privacy law, which is why any legal solution needs to be designed in a way that these legal specialities are included and that both the human rights considerations and economic foundations are considered.

As Kerber argues, 'it is not sufficient to look for policy solutions only in one field of the law, as, e.g. competition law or data protection law, rather an integrated approach from different regulatory perspectives is necessary.'[82] Further, as outlined in the Digital Platform Inquiry Final Report:

> data collection and privacy laws can enhance consumer protection by ensuring that consumers receive accurate, intelligible information about entities data practices. This can increase the transparency of digital platforms data practices, which then assists consumers to make rational and informed choices about which digital platform service to use. It can lead to increased incentives for digital platforms to improve the privacy dimension of their services to meet consumer demand.[83]

6.4.2.3 Pace of Policy Review

As outlined in the ACCC Digital Platforms Inquiry Final Report 'the pace of technological change needs to be matched by the pace of policy review.'[84] The failure of policymakers to understand this accounts for the current state in Australia. The digital platform sector ought to be reviewed every two to three years. There are lessons here to be learn from the Australian Government's approach to reviewing Australia's franchising sector over the past 50 years.

Unfortunately, the Australian Government's response to the Digital Platform Inquiry remained silent on the future of reviews, beyond those outlined in the short- to medium-term. In order to ensure that any new legislation or enforcement body remains current and up-to-date with the latest developments, a program for continual review needs to be identified and adhered to.

6.4.2.4 Recognition of Societal Benefit

Finally, privacy is a social good, with the value of privacy being subjective and determined through the perspective of privacy as a final good or privacy as an intermediate good (advantages of keeping things private).[85] Social values impact the significance of informed consent in online standard form agreements. Societal benefit should become a key argument in creating a legal framework that ensures informed consent to online standard form agreements.

6.5 Conclusion

This chapter has analysed each of the regulatory instruments that currently comprise and will soon impact on the Australian privacy framework. A significant focus has been directed towards the ACCC's Digital Platform Inquiry and recent Australian Government Response to this inquiry and the accompanying implementation roadmap.

---

[82] Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11(11) *Journal of Intellectual Property Law & Practice* 856.
[83] *Digital Platforms Inquiry Final Report* (n 32).
[84] Ibid.
[85] Kemp and Buckley (n 51).

Fundamentally, it is clear that an effective new privacy framework needs a sophisticated and integrated approach that draws on the rules and regulations as they are outlined in Australia's competition, consumer, privacy and intellectual property laws. For this approach to be truly effective, collaboration between enforcement agencies, competition authorities, information commissioners, and consumer protection agencies will also need to be coordinated.

In a more specific sense, a series of solutions, split into quick policy wins and longer-term changes, have been proposed, which together will serve to enhance the protection provided through Australia's privacy framework and the nation's reputation on the world stage as a country that values a human being's right to privacy and protection.

The reality is, privacy best practice standards are evolving rapidly around the world, while Australia continues to lag behind, with no satisfactory proposal for ensuring that standards are improved to international best practices, we will continue to suffer as a nation economically, professionally and personally. Our web and app-based businesses will have to design their services to comply with overseas legislation and our citizens will be left trying to apply legislation created before the advent of online contracting to their online contracts.

KATHARINE KEMP

KAYLEEN MANWARING

Appendix A: 'Stop press' - *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367

In October 2019, the Australian Competition and Consumer Commission (ACCC) instituted proceedings against Google LLC and Google Australia Pty Ltd (together, Google) alleging contraventions of the misleading or deceptive conduct and false or misleading representations sections of the *Australian Consumer Law* (*ACL*). These proceedings were filed in response to on-screen representations Google made concerning user control over location data and Google's use of that data collected from Android mobile phones and tablets.[1]

On 16 April 2021, the Federal Court handed down its liability judgment in these proceedings, *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367 (*ACCC v Google (No 2)*). It held that Google had breached ss 18, 29 and 34 of the ACL, in the way it presented its privacy policies and settings through Android devices for two years from January 2017 to December 2018. (Google has since changed the way these settings are presented to consumers.)

The Federal Court found that Google's previous 'Location History' settings would have led some reasonable consumers to believe that they could prevent their location data being saved to their Google account. In fact, selecting 'Don't save my Location History in my Google Account' (**Image 1**) alone could not achieve this outcome.

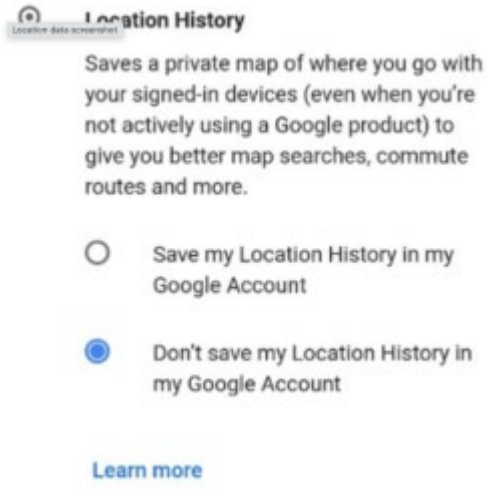


Image 1: Google's previous Location History setting[2]

[1] Concise statement, NSD1760/2019, *ACCC v Google LLC & Anor*, 29/10/2019, available at https://www.accc.gov.au/system/files/Concise%20Statement_ACCC%20v%20Google%20Australia%20Pty%20Ltd%20%26%20Anor_%2029.10.19.pdf

[2] *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367 (*ACCC v Google (No 2)*) [156].

Users needed to change an additional, separate setting to stop that location data from being saved to their Google account. In particular, they needed to navigate to 'Web & App Activity' and select 'Don't save my Web & App Activity to my Google Account' (**Image 2**), even if they had already selected the 'Don't save' option under 'Location History'.

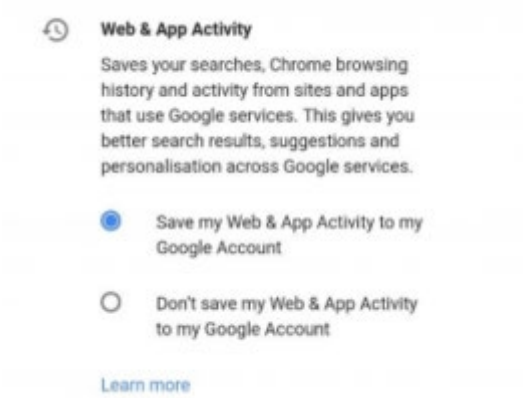


Image 2: Google's previous Web & App Activity settings[3]

The ACCC said that this decision is a 'world first' in relation to Google's location privacy settings. As sections 29 and 34 are designated civil penalty provisions in the *ACL*, the regulator has stated that it intends to seek pecuniary penalties against Google,[4] which could be up to $10 million, three times the value of the benefit received or 10 per cent of local turnover in the preceding 12 months.[5] The ACCC will also be seeking declarations, publication orders and compliance orders under the *ACL*. [6]

ACCC Chair Rod Sims responded to the Federal Court's findings, saying: '[t]his is an important victory for consumers, especially anyone concerned about their privacy online, as the Court's decision sends a strong message to Google and others that big businesses must not mislead their customers.' Indeed, it is clear that misleading or deceptive conduct, or false or misleading representations, connected to privacy policies and privacy settings could lead to similar liability under the *ACL*.

However, the ACCC was not wholly successful. The ACCC's action also alleged that statements made by Google concerning methods by which consumers could stop Google using their location data, and the purposes for which Google used the data, were misleading or deceptive, and false or misleading. Thawley J dismissed the ACCC's claim on the basis that 'reasonable users' would not have found the relevant statements misleading. It seems that the judge expected reasonable users to have a basic understanding of the business model of companies like Google in that 'they would have assumed that Google was obtaining as much commercial advantage as it could from use of the user's personal location data'.

Until a penalty decision is made by the Federal Court, and any appeals processes are exhausted, it is difficult to assess the deterrent effect the decision might have, especially against business entities with vast resources like Google. While the decision is a promising development under the *ACL*, for the reasons set out in the main body of this report, this

---

[3] *ACCC v Google (No 2)* n 2 [155].
[4] ACCC, 'Google misled consumers about the collection and use of location data', *Media Release* (16 April 2021) https://www.accc.gov.au/media-release/google-misled-consumers-about-the-collection-and-use-of-location-data
[5] *ACL* s 224.
[6] ACCC n 4.

judgment cannot provide a complete solution to the problem of harmful data practices[7] including the prolific sharing of consumers' personal information against their interests and the absence of free and informed consent.

Major changes to Australian privacy laws will also be required before companies are prevented from pervasively tracking consumers who do not wish to be tracked. The current review of the Federal Privacy Act[8] could be the beginning of a process to obtain fairer privacy practices for consumers, but any reforms from this review are likely to be a long-time coming.

[7] Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16(2-3) *European Competition Journal* 628.
[8] Australian Government, Attorney-General's Department, Review of the Privacy Act 1988, https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

UNSW
SYDNEY