The Senate

Economics References Committee

Influence of international digital platforms

November 2023

ISBN 978-1-76093-590-0 (Printed version)

ISBN 978-1-76093-590-0 (HTML version)

Printed by Printed by the Senate Printing Unit, Parliament House

Members

Chair
Senator Andrew Bragg — LP, NSW

Deputy Chair
Senator Jess Walsh — ALP, VIC

Members
Senator the Hon Matthew Canavan — NATS, QLD
Senator Jana Stewart — ALP, VIC
Senator Dean Smith — LP, WA

Substitute Members
Senator David Shoebridge — AG, NSW
(*for Senator McKim, 26 September 2022 to 28 November 2023)*

Secretariat
Alan Raine, Committee Secretary
Nicola Kosseck, Principal Research Officer
Adelaide Hutchins, Research Officer
Dr Andrew Gaczol, Principal Research Officer (*to 16 December 2022*)
Taryn Morton, Research Officer (*to 15 September 2023*)
Kieran Knox, Administrative Officer (*from 31 July 2023*)
Joti Saini, Legislative Research Officer (*to 17 August 2023*)

PO Box 6100
Parliament House
Canberra ACT 2600

Ph: (02) 6277 3540
Email: economics.sen@aph.gov.au

Contents

Terms of reference

The nature and extent of international digital platforms operated by large overseas-based multinational technology companies—so called 'Big Tech'—exerting power and influence over markets and public debate, to the detriment of Australian democracy and users, with particular reference to:

(a) the market shares of such international digital platforms across the provision of hardware and software services;
(b) vertical integration, or linking of multiple services, products and/or hardware, within such international digital platforms and resultant outcomes on users' ability to exercise choice;
(c) whether algorithms used by such international digital platforms lack transparency, manipulate users and user responses, and contribute to greater concentrations of market power and how regulating this behaviour could lead to better outcomes in the public interest;
(d) the collection and processing of children's data, particularly for the purposes of profiling, behavioural advertising, or other uses;
(e) the adequacy and effectiveness of recent attempts, in Australia and internationally, to regulate the activities of such international digital platforms;
(f) broader impacts of concentration of market power on consumers, competition and macro-economic performance, and potential solutions; and
(g) any other related matters.

Acronyms and abbreviations

ABC	Australian Broadcasting Corporation
ACCAN	Australian Communications Consumer Action Network
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications Media Authority
Adtech	Advertising technology
AI	Artificial intelligence
AICD	Australian Institute of Company Directors
AIIA	Australian Information Industry Association
ALIA	Australian Library and Information Association
ANU Tech	Australian National University's Tech Policy Design Centre
ARACY	Australian Research Alliance for Children and Youth
ASBFEO	Australian Small Business and Family Enterprise Ombudsman
AWS	Amazon Web Services
BOSE	Basic Online Safety Expectations
CBA	Commonwealth Bank Australia
CCA	*Competition and Consumer Act 2010*
CISO	Chief Information Security Officer
CMA	Children and Media Australia
COSBOA	Council of Small Business Organisations Australia
CPRC	Consumer Policy Research Centre
CRA	Commercial Radio & Audio
Criminal Code	*Criminal Code Act 1995*
CSEA	Child sexual exploitation and abuse
DIGI	Digital Industry Group Inc.
DITRDCA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
DMA	European Union Digital Markets Act
DP-REG	Digital Platforms Regulators Forum
DRW	Digital Rights Watch
DSA	European Union Digital Services Act
DSP	Demand side platform
DTA	Digital Transformation Agency
DV360	Display and Video 360
EU	European Union
FTC	United States Federal Trade Commission
FTC	Federal Trade Commission
GDPR	European Union General Data Protection Regulation

HCF	Hosting Certification Framework
HRLC	Human Rights Law Centre
IAP	In-app purchase
ISO/IEC	International Organization for Standardisation/International Electrotechnical Commission
LIV	Law Institute of Victoria
NCMEC	United States National Center for Missing and Exploited Children
NFC	Near-field communication
NFP	Not for profit
NIST	United States National Institute of Standards and Technology
NMBC	News Media and Digital Platforms Mandatory Bargaining Code
NSLA	National and State Libraries Australasia
OAIC	Office of the Australian Information Commissioner
OFCOM	United Kingdom Office of Communications
OPC	Obesity Policy Coalition
OSA	*Online Safety Act 2021*
Privacy Act	*Privacy Act 1988*
RBA	Reserve Bank of Australia
SBS	Special Broadcasting Service Corporation
SDKs	Software Development Kits
SME	Small to medium enterprise
SOCI	Security of Critical Infrastructure
SPA	Screen Producers Australia
SSP	Supply side platform
SVOD	Streaming video on demand
TCA	Tech Council of Australia
The committee	Senate Economics References Committee
TISN	Trusted Information Sharing Network
UK	United Kingdom
US	United States of America

Chapter 1
Introduction

Referral of the inquiry

1.1 On 26 September 2022, the Senate referred the following matter to the Economics References Committee (the committee) for inquiry and report by the last sitting day in 2023:

> The nature and extent of international digital platforms operated by large overseas-based multinational technology companies—so called 'Big Tech'—exerting power and influence over markets and public debate, to the detriment of Australian democracy and users, with particular reference to:
>
> (a) the market shares of such international digital platforms across the provision of hardware and software services;
> (b) vertical integration, or linking of multiple services, products and/or hardware, within such international digital platforms and resultant outcomes on users' ability to exercise choice;
> (c) whether algorithms used by such international digital platforms lack transparency, manipulate users and user responses, and contribute to greater concentrations of market power and how regulating this behaviour could lead to better outcomes in the public interest;
> (d) the collection and processing of children's data, particularly for the purposes of profiling, behavioural advertising, or other uses;
> (e) the adequacy and effectiveness of recent attempts, in Australia and internationally, to regulate the activities of such international digital platforms;
> (f) broader impacts of concentration of market power on consumers, competition and macro-economic performance, and potential solutions; and
> (g) any other related matters.

Conduct of the inquiry

1.2 The committee advertised the inquiry on its website and released an issues paper to guide submitters.

1.3 It also wrote to relevant stakeholders and interested parties inviting submissions by 28 February 2023. The committee published 77 submissions, which are listed at Appendix 1.

1.4 The committee held three public hearings:

- 26 July 2023 – Sydney in person and by teleconference.
- 22 August 2023 – Canberra in person and by videoconference.
- 03 October 2023 – Canberra by videoconference.

1.5 A list of witnesses who gave evidence at the hearings is available at Appendix 2.

1.6 Links to public submissions, Hansard transcripts of evidence and other information published by the committee for this inquiry are available on the committee's website.

Acknowledgements

1.7 The committee thanks all individuals and organisations who assisted with the inquiry, in particular those who made submissions or gave evidence at public hearings.

Structure of the report

1.8 This chapter provides details on the referral and administration of the inquiry.

1.9 Chapter 2 examines economic benefits from the rise of technology, respective market shares of Big Tech firms and the risks of concentrated market power of Big Tech.

1.10 Chapter 3 details a range of competition concerns arising from the power of Big Tech and proposed solutions in relation to vertical integration, mergers and acquisitions, self-preferencing, tying and interoperability.

1.11 Chapter 4 describes bargaining imbalances that arise between consumers and Big Tech companies. It considers issues relating to this imbalance including unfair contract terms, unfair trading practices and inadequate dispute resolution, and proposals to address these concerns.

1.12 Chapter 5 explores privacy and competition concerns in relation to the data collection practices of Big Tech. It considers concerns with profiling, data brokers and cloud storage, and potential solutions to these concerns.

1.13 Chapter 6 considers the risks of Big Tech algorithms and automated decision-making including filter bubbles, bias and discrimination, dis- and misinformation and lack of Australian content discoverability. It then considers the role of transparency in mitigating these harms.

1.14 Chapter 7 looks at the consumer harms of scams, harmful apps and fake reviews, and possible mechanisms to address these concerns.

1.15 Chapter 8 examines the risks arising from collection, collation and use of children's online data. It discusses unethical and criminal behaviours, as well as potential solutions for protecting children online.

1.16 Chapter 9 explains the potential risks and opportunities for reform of emerging technologies, with a focus on the metaverse and artificial intelligence.

1.17 Chapter 10 provides the committee's view and provides several recommendations to promote better consumer and competitive outcomes in digital platforms markets.

Chapter 2
Background

Overview

2.1 The term 'Big Tech' refers to large digital platforms, in particular, the five largest platforms: Alphabet (Google), Amazon, Apple, Meta and Microsoft.

2.2 These companies in many instances have acquired other popular platforms—for example, Google owns YouTube, while Meta owns Instagram and WhatsApp. The term may also encapsulate other smaller companies with dominance in a particular segment of the market or high valuations such as Adobe, Netflix, Nvidia, Oracle, Salesforce, Snap, Twitter (X Corp.) and Uber.

2.3 This chapter details:

- economic benefits from the rise of digital technology;
- respective market shares of Big Tech firms; and
- risks of concentrated market power of Big Tech.

Technology is important

2.4 Digital platforms are important to Australia as they provide pivotal business and consumer services and drive economic growth. Consumers rely on digital platforms for various services, such as connecting with others, accessing information and entertainment, conducting business, and purchasing goods and services. The significance of digital platforms means ensuring competition and consumer protections is integral to the economy.

Economic growth

2.5 Big Tech has contributed to a thriving technology sector, stimulating innovation and opportunities for emerging companies to grow.

2.6 The digital technology sector, of which digital platforms play a large role, contributed an estimated $167 billion to the Australian economy in the 2021 financial year, equivalent to 8.5 per cent of gross domestic product.[1] It is Australia's third largest industry, with over 100 tech companies originating from Australia valued at $100 million or more, including over 20 unicorn[2] companies.[3]

---

1 Australian Competition and Consumer Commission (ACCC), *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 29; Australian Information Industry Association (AIIA), *Submission 16*, [pp. 1–2]; Microsoft, *Submission 47*, p. 3.

2 Companies that reach a valuation of $1 billion without being listed on the stock market.

3 Tech Council of Australia, *Submission 63*, p. 2.

2.7 Ms Belinda Dennett, Corporate Affairs Director, Microsoft, commented:

> … foundational investments in cloud infrastructure by global tech companies have contributed to Australia's strong track record by launching globally successful tech companies, with 2.3 per cent of the world's tech unicorns having come from Australia despite our much smaller 1.6 per cent share of global GDP [gross domestic product].[4]

2.8 The Tech Council of Australia commented on the economic contribution of Big Tech and the potential for the future:

> Our research highlights that both Australian starts-ups and scales-ups, and large global tech companies, will play an important role in helping grow the economic contribution of the tech sector in the future to meet the targets of delivering $250 billion per annum to Australia's GDP, and seeing 1.2 million people in tech jobs by 2030 … While Australia has shown its potential in the tech sector, we still have significant room to grow. Our research shows the direct tech sector in Australia is only 3.8% of GDP. In Canada it is 6.8%, in the UK 8.1% and in the US 10.2%.[5]

2.9 Submitters provided several examples of investments by Big Tech firms:

- Google, through its Digital Future Initiative, announced a $1 billion investment in research, infrastructure and partnerships, including in Quantum and artificial intelligence (AI) technologies in Australia.[6]
- Apple invests in clean energy in Australia, developing new sources of renewable energy, expanding coding education programs, and forging partnerships with Indigenous-led non-profits.[7] In 2022, Apple invested more than $20 billion in research and development.[8]
- Amazon Web Services (AWS) plans to invest $6.8 billion in the Asia Pacific Region from 2022 to 2037, contributing an estimated $15.9 billion to Australia's GDP from 2022 to 2037. AWS investment from 2022 to 2037 will support an estimated annual average of more than 2 500 full-time equivalent jobs at local vendors in the data centre supply chain.[9]
- Amazon's Prime Video service has commissioned 27 Amazon Original series in Australia since its launch, investing well over $150 million in local productions, and resulting in more than 2 500 jobs across Australia.[10]

---

4 *Proof Committee Hansard*, 22 August 2023, p. 8.

5 Tech Council of Australia, *Submission 63*, p. 2.

6 Google, *Submission 49*, p. 1.

7 AIIA, *Submission 16*, [p. 2].

8 Mr Kyle Andeer, Vice President, Products and Regulatory Law, Apple Inc., *Proof Committee Hansard*, 3 October 2023, p. 6.

9 AIIA, *Submission 16*, [p. 2].

10 Amazon Australia, *Submission 48*, p. 2.

Small businesses and employment

2.10 Many Australian businesses benefit from tech services, including search and advertising services that allow them to reach larger audiences. The global availability of tech makes it possible for businesses of all sizes to reach international customers.

2.11 Meta commented on the benefit of digital platforms to small businesses:

> A recent report by Deloitte found that 82 per cent of Australian small businesses reported using free, ad-supported Meta apps to help them start their business, and 71 per cent of Australian small businesses that use personalised advertising reported that it is important for the success of their business.[11]

2.12 DoorDash submitted that digital platforms provide not only economic benefits for businesses, but support job growth and help consumers:

> Since our launch in Australia, merchants have earned over $1 billion AUD in sales from orders placed on DoorDash Marketplace, including over $100 million AUD for non-restaurant merchants. In addition from 2021 to 2022, sales on DoorDash Marketplace grew by 94% for merchants and by 570% for non-restaurant merchants.[12]

2.13 The Australian Computer Society's *Digital Pulse 2022 Report* found that by 2024 there will be more than 1 million technology workers in Australia, growing to 1.2 million by 2027. This will mean the proportion of the Australian workforce in technology roles will rise to 8.5 per cent by 2027, outpacing broader employment growth.[13]

2.14 Mr Michael Cooley, Director, Public Policy Australia, Amazon Australia, highlighted how Amazon's expansion into Australia has resulted in job growth and allowed small businesses access to more consumers. Mr Cooley estimated Amazon has:

> … created more than 20,000 Australian jobs to support their Amazon related business activities … Just two weeks ago, we announced our seventh fulfilment centre has commenced construction in Craigieburn, north-east Melbourne. Targeting completion in 2025, the new site will create around 2,000 local jobs once fully operational and an additional 2,000 local jobs during the construction and fit-out.[14]

2.15 Ms Dennett indicated that Microsoft partners with emerging technology companies, supporting business growth and creating jobs:

> In Australia we have over 9,000 partners. Seventy per cent of those are Australian small and medium-sized businesses, employing over 200,000

---

11 Meta, *Submission 69*, p. 4.

12 DoorDash, *Submission 64*, p. 2.

13 AIIA, *Submission 16*, [pp. 1–2].

14 *Proof Committee Hansard*, 22 August 2023, p. 1.

> Australians in every corner of the country. In 2020 those partners contributed over $55 billion to the economy, of which 48 per cent was directly attributable to Microsoft. Those partners created $1.5 billion of new and repeatable IP built on the Microsoft platform.[15]

2.16 Mr Kyle Andeer, Vice President, Products and Regulatory Law, Apple Inc., stated that the Apple app store supported more than 150 000 Australian jobs and facilitated $14 billion in commerce in Australia and New Zealand in 2022.[16]

2.17 Large technology firms also contribute to education and reskilling opportunities for students and workers. Many companies partner with Australian educational institutions to strengthen science, technology, engineering, and mathematics education or provide alternate courses to incentivise workers to transition into tech roles.[17] For example, Google has provided free digital skills training to over 600 000 Australian small businesses and individuals under the Grow with Google program.[18]

Benefits for consumers

2.18 Benefits of technology growth for consumers include convenience, affordability and efficiency of services. Many of these improvements are made possible due to market power of Big Tech, as when many people use the same platform, the platform can aggregate data and improve services.

2.19 The Australian Competition and Consumer Commission (ACCC) noted it has been estimated that digital platforms generate a consumer surplus of approximately $5 000 per Australian household per year through free or cheaper and more convenient goods and services. Google's services alone are estimated to create over $50 billion of annual economic value that flows to Australian businesses and consumers.[19]

2.20 Ms Dennett commented on the benefits of widespread technology to consumers during the COVID-19 pandemic. Technology was:

> … critical in enabling many Australians to work from home, learn from home and stay connected to their families and friends, and critical for the parliament to continue to sit, for government to continue to deliver services and for most of us to continue to buy the things we needed.

---

15 Ms Belinda Dennett, Corporate Affairs Director, Microsoft, *Proof Committee Hansard*, 22 August 2023, p. 8.

16 *Proof Committee Hansard*, 3 October 2023, p. 6.

17 BSA – The Software Alliance, *Submission 32*, p. 8.

18 Google, *Submission 49*, p. 2.

19 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 29.

> … [B]y enabling remote working, collaboration technologies … helped to keep employed 3.2 million Australians who would otherwise have been unable to keep working.[20]

2.21 Meta stated that personalised advertising provided by digital platforms is beneficial to consumers as it provides them access to products and services relevant to their interests.[21]

2.22 Similarly, Amazon Australia highlighted that access to information through digital platforms gives consumers greater choice as they can research prices, product information and retailers.[22]

Climate change

2.23 Submitters also highlighted how digital platforms are working to combat climate change. For example, Google is enabling the use of AI for natural disaster detection and post-disaster rebuilding applications to strengthen Australia's resilience against the impacts of climate change.[23]

Market power

2.24 Many digital platform markets are dominated by one or two large providers that face limited competitive constraint.

2.25 Together, Alphabet, Apple, Meta, Amazon and Microsoft have a joint market capitalisation of around US$4.5 trillion.[24] Each company holds dominant market power in various sectors: app stores (Google and Apple), search (Google), ad tech[25] (Google), social media (Meta), e-commerce (Amazon), desktop operating systems (Microsoft) and cloud (Amazon and Microsoft). While they have market strengths, they compete for market share across various areas, such as hardware, PC and mobile operating systems and entertainment.

2.26 An analysis of the time Australians spend on particular apps and websites reveals the market share that Google, Apple, Meta and Microsoft command of time spent online in Australia, with Australians spending the most time on Google (including YouTube and search engines) and Meta-owned platforms (Facebook, Messenger, Instagram and Whatsapp) (see Figure 2.1 below).

---

20 Ms Belinda Dennett, Corporate Affairs Director, Microsoft, *Proof Committee Hansard*, 22 August 2023, p. 8.

21 Meta, *Submission 69*, p. 4.

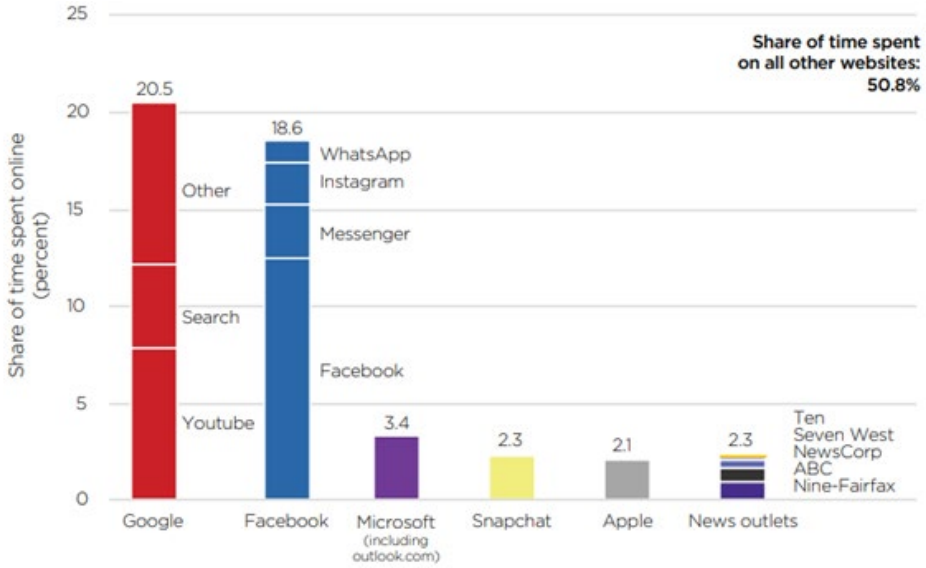
22 Amazon Australia, *Submission 48*, p. 4.

23 Google, *Submission 49*, p. 2.

24 Cory Mitchel, *GAFAM stocks*, 7 October 2020, www.investopedia.com/terms/g/gafam-stocks.asp (accessed 2 September 2022).

25 Advertisement technology.

Figure 2.1 Apps and websites Australians spent the most time on, as of 2019, by platform



Source: Australian Competition and Consumer Commission, Digital Platforms Inquiry – Final Report, July 2019, p. 6, citing Nielsen Digital Panel, February 2019.

2.27 The ACCC's *Digital platform services inquiry, Interim report No. 5 – Regulatory reform* found globally dominant digital platforms are also the most widely used digital platforms in Australia:

> Among search engines, in 2018 Google Search accounted for 90 per cent of search traffic originating from Australian desktop computer users and over 98 per cent of search traffic from Australian mobile users.
>
> Among social media platforms, Facebook has by far the largest user base in Australia, with approximately 17 million users accessing its platform on a monthly basis in 2019. Assuming the users are all adults, this equates to approximately 84 per cent of Australian adults accessing the Facebook platform at least monthly.
>
> Instagram (owned by Facebook) is the next most popular social media platform with approximately 11 million monthly users … equating to approximately 54 per cent of Australian adults.[26]

Competition and consumer risks

2.28 There is growing international consensus that reform is needed to control the market power of Big Tech.

2.29 Because of the significance of technology in our lives, the potential for harm in digital platform markets is high. The importance and widespread use of digital platforms creates more opportunities and incentives for these platforms to engage in conduct that is anti-competitive or may harm consumers.

---

[26] ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 42.

2.30 Companies with dominant market power may take advantage of inadequate protections and exploit power imbalances to the detriment of consumers and small businesses. This directly harms platform users, as well as reducing trust in digital services and inhibiting economic growth.

2.31 Further, limited competitive constraints reduce incentives to innovate and improve. This could result in higher prices, greater exposure to advertising or increased harvesting of personal data. Lack of competition can also result in reduced consumer choice.

2.32 Digital platform markets in Australia have high levels of concentrated market power, with markets such as app stores, search services, and ad tech dominated by a small number of platforms with principal market power. The lack of competition in the digital platforms sector gives Big Tech the opportunity to engage in anti-competitive conduct that benefits themselves, to the detriment of consumers and competitors.[27]

2.33 Some submissions argued many of these issues arise in other industries across the economy. For instance, Meta commented:

> Many of the characteristics of digital markets identified by Australian policymakers (such as economies of scale, use of data, self-preferencing, optimising the user experience, and M&A [merger & acquisition] activity) are not unique to digital platforms. They occur in industries right across the economy and can either deliver significant benefits or result in certain harms, depending on a range of factors. Regulating specific services or segments too narrowly will create market distortions between digital platforms and other competitors (such as print and broadcasting advertisers) and inhibit innovation and investment.[28]

2.34 However, these issues raise particular challenges when they occur on digital platform services. The ACCC summarised the unique economic and commercial characteristics of digital platforms that contribute to high barriers to entry and expansion and support market concentration. These include:

- **Strong network effects:** where the value of a service depends on the number of users with whom other users can interact. In markets with strong positive network effects, users will be drawn to the platform with the largest number of users.
- **Significant economies of scale and sunk costs:** where the average cost of providing services decreases with increased use. In markets where these dynamics are present, larger platforms have a cost advantage, while high fixed costs of entering can dissuade new entry and put smaller rivals at a cost disadvantage.

---

[27] See, for example, ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 42; Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

[28] Meta, *Submission 69*, p. 10.

- **Advantages of scope and expansive ecosystems:** where supplying multiple related services advantages a large platform through the ability to share and combine data, the ability to leverage existing user-bases across services, or lower average costs. This can raise barriers to entry and expansion, which may be reinforced when platforms make their services incompatible with other services outside their ecosystem.
- **Barriers to switching:** where consumer inertia, switching costs and a platform's interface design can increase consumer lock-in, often to the incumbent's advantage.
- **Access to high-quality user data:** where vast amounts of individual-level data are required to train algorithms and offer higher-quality and personalised services (including targeted advertising). Access to such data provides a considerable competitive advantage to established digital platforms.

These characteristics also provide large incumbent digital platforms with the ability and incentive to engage in strategic conduct to entrench and expand their market power.[29]

2.35 The substantial market power held by digital platforms gives them the ability and incentive to engage in anti-competitive conduct that entrenches and expands their market power.

2.36 Anti-competitive conduct may reduce incentives for smaller businesses to enter digital platform markets, innovate and improve services. Ultimately, for consumers, this leads to limited choice, lower quality services and higher costs.[30]

2.37 Ms Kate Reader, General Manager, Digital Platforms Branch, ACCC, explained these harms:

> I think we're seeing a lack of choice, especially lock-in effects. We're seeing a lack of innovation compared to a market—if you had more players and more competition, there'd probably be a lot more innovation. We're seeing prices go up or be higher than they would be in the competitive market, so, when you pay for apps, a large chunk of your payment is going to the digital platforms. Even when things seem free, you're paying in terms of looking at all the advertising. If the market were more competitive, there would be quite a good chance that there would be less advertising exposure.[31]

2.38 Competition and consumer risks are discussed in greater depth in the following chapters.

Digital platform regulators

2.39 Primary responsibility for regulating digital platforms is shared between the Australian Communications and Media Authority (ACMA), the ACCC, the

---

29 ACCC, *Submission 8*, pp. 7–8.

30 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 43.

31 *Proof Committee Hansard*, 22 August 2023, p. 34.

Office of the Australian Information Commissioner (OAIC), and the Office of the eSafety Commissioner (eSafety).

2.40 Together, these bodies share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms in an informal body called the Digital Platforms Regulators Forum (DP-REG).[32] See Figure 2.2 for a summary of each agency's responsibilities.

2.41 The ACMA oversees content regulation in Australia, including matters related to some online content, broadcasting standards and classification, radiocommunications and telecommunications. Digital platforms may be subject to obligations regarding harmful or illegal content, such as child exploitation material, violence, or hate speech. The ACMA also oversees the *Australian Code of Practice on Disinformation and Misinformation* relating to targeting of a person with dis- and misinformation.[33]

2.42 The ACCC conducts inquiries and law enforcement cases in relation to Australian Consumer Law and anti-competitive behaviour by digital platforms. Recent inquiries have focused on issues relating to market dominance, mergers and acquisitions, and the impact on competition in the digital advertising market.[34]

2.43 The OAIC has three main functions:

- Privacy functions: protecting the privacy of individuals under the *Privacy Act 1988* and other legislation;
- Freedom of information functions: access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982*; and
- Information management functions as set out in the *Australian Information Commissioner Act 2010*.[35]

2.44 eSafety is the primary agency tasked with regulating online safety. Its enabling legislation is the *Online Safety Act 2021* (OSA). eSafety's role includes administering complaints and investigation schemes for four types of online harms:

- cyberbullying of children,
- cyber abuse of adults,
- the non-consensual sharing of intimate images, and

---

32 Digital Platforms Regulators Forum, *Submission 34*, p. 4.

33 Australian Communications and Media Authority (ACMA), *Submission 24*, p. 1.

34 ACCC, *Inquiries and consultations*, www.accc.gov.au/inquiries-and-consultations (accessed 22 November 2023).

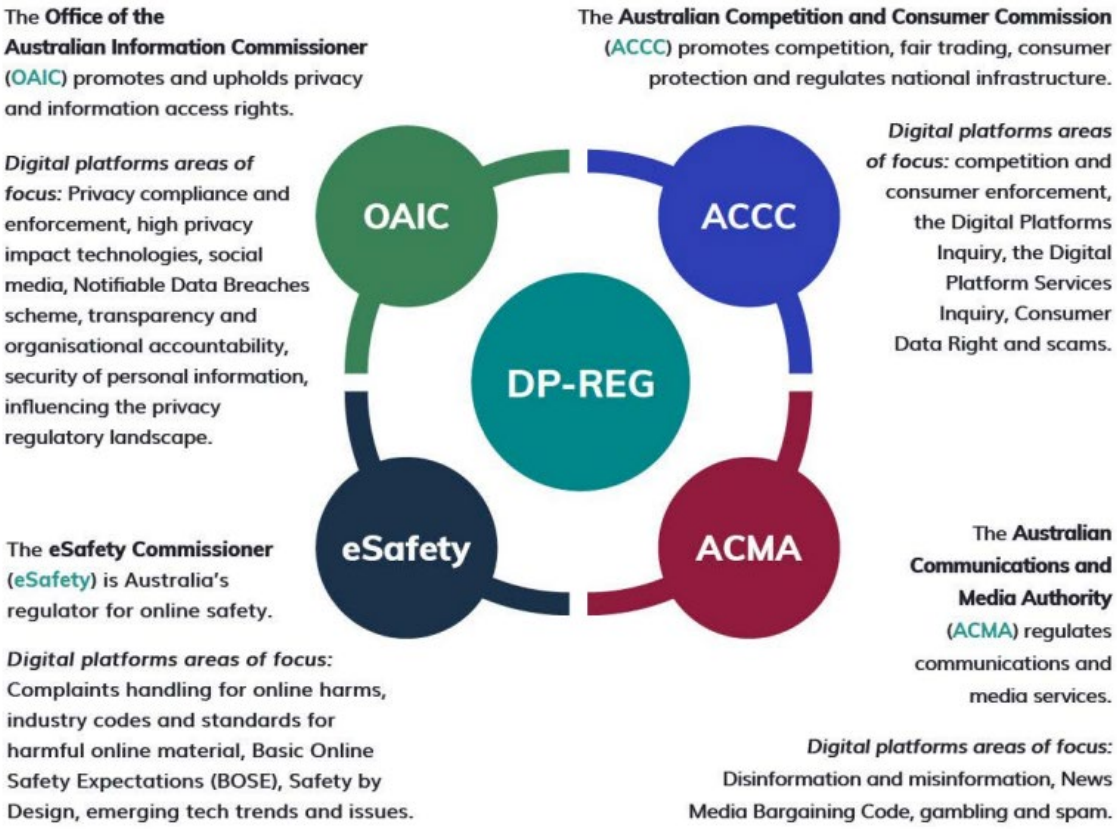
35 Office of the Australian Information Commissioner, *Submission 61*, p. 1.

- illegal or restricted online content.[36]

2.45 The OSA also provides eSafety with 'powers to regulate digital platforms' broader systems and processes'.[37] eSafety advised that it:

> … closely monitors new and emerging tech trends and challenges, including those occurring on major international digital platforms, and advocates for greater transparency and accountability in their efforts to address online safety issues. We also work with local and international stakeholders to examine new research, policy and legislative developments, and provide resources and tools for industry's use.[38]

Figure 2.2 DP-REG member's remits and perspectives



Source: Digital Platforms Regulators Forum, Submission 34, p. 4.

[36] Office of the eSafety Commissioner, *Submission 2*, p. 1.

[37] Office of the eSafety Commissioner, *Submission 2*, p. 1.

[38] Office of the eSafety Commissioner, *Submission 2*, p. 1.

Chapter 3
Competition

Overview

3.1 Market dominance of Big Tech has raised several concerns for competition. Submitters suggested that Big Tech firms have substantial market power that makes it difficult for other businesses to compete, resulting in less innovation and limited choices for consumers.

3.2 This chapter discusses a range of concerns raised by submitters in relation to:

- vertical integration, mergers and acquisitions;
- self-preferencing;
- tying; and
- interoperability.

3.3 This chapter will then discuss proposed solutions to digital platform competition issues, including the adoption of principles-based legislation or industry codes.

Vertical integration, mergers and acquisitions

Vertical integration

3.4 As tech companies have grown to become some of the largest firms in the world, they have increasingly engaged in a practice called 'vertical integration'.

3.5 Vertical integration is a business expansion strategy where companies acquire additional levels of the supply chain. Companies can integrate vertically by building additional operations, or through mergers and acquisitions.[1]

3.6 Vertical integration allows companies to limit reliance on competitors for other services and gives companies the opportunity to have full control of the processes related to their operations. It also grants competitive advantages such as allowing firms to gather larger suites of data and improved customer insights, which can lead to higher quality products and services, and increased profits.[2]

3.7 An example of a vertically integrated company is shown in Figure 3.1 below. In the case of Apple, it controls multiple levels of the phone supply chain, including design and sales of devices, the iOS operating system on those

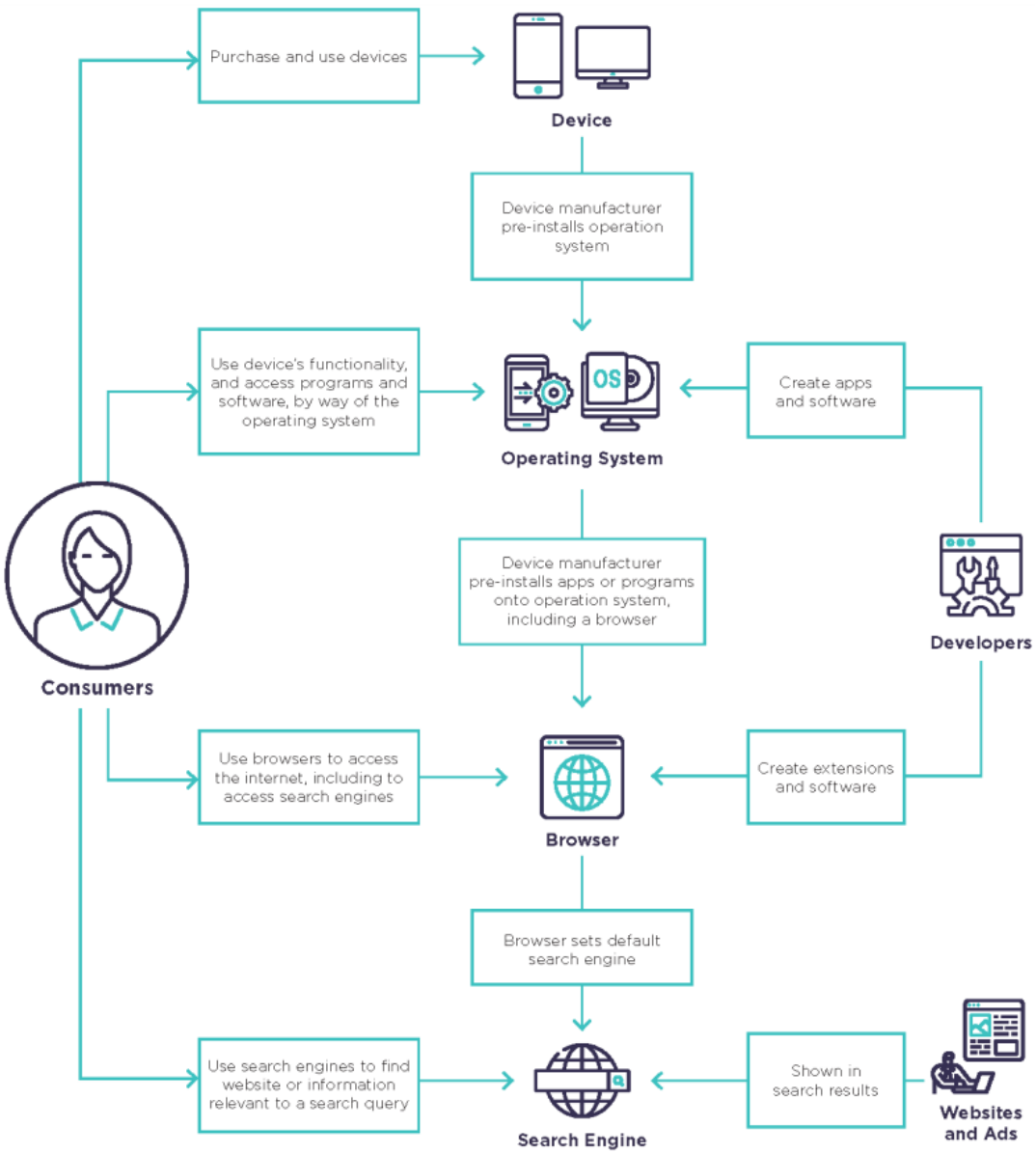
---

1 Abby Jenkins, *How Does Vertical Integration Work? Pros, Cons and Examples*, 5 January 2023, www.netsuite.com/portal/resource/articles/erp/vertical-integration.shtml (accessed 6 November 2023).

2 Abby Jenkins, *How Does Vertical Integration Work? Pros, Cons and Examples*, 5 January 2023, (accessed 6 November 2023).

devices, the Apple App Store, and apps such as the Safari browser.[3] Google pays Apple around US$7 billion annually to be the default search engine for Safari.[4]

Figure 3.1 Example of the platform ecosystem surrounding a vertically integrated digital platform



Source: Australian Competition and Consumer Commission, Digital Platform Services Inquiry, Third Interim Report, 28 October 2021, p. 26.

---

[3] Paul Cole-Ingait, *Vertical Integration Examples in the Smartphone Industry*, https://smallbusiness.chron.com/vertical-integration-examples-smartphone-industry-79551.html (accessed 6 November 2023).

[4] Elijah Ajuwon, *Apple Silicon: Why tech giants engage in vertical integration*, 8 September 2020, www.tcsnetwork.co.uk/apple-silicon-why-tech-giants-engage-in-vertical-integration (accessed 6 October 2023).

3.8 Submitters raised concerns that vertical integration increases companies' market power, leading to monopolisation of markets, limited competition, higher prices, and reduced customer choices.[5]

Conflict of interest

3.9 Submitters argued vertical integration creates a conflict of interest that incentivises and allows companies to engage in anti-competitive conduct.[6]

3.10 Vault Cloud submitted that vertical integration:

> … may harm consumers ability to choose alternatives or switch to competitors. This could create conflicts of interest in the different stages of the supply chain, which makes not only ensuring the use of personal data in an ethical and transparent manner more difficult but potentially enable Big Tech companies to use its dominant market position to raise prices and drive small local companies out of business or create barriers to entry for new businesses.[7]

3.11 Professor Toby Walsh, Chief Scientist, AI Institute, University New South Wales, acknowledged centralised markets may have advantages for consumers, such as easy accessibility. However, he noted vertically integrated companies create a conflict:

> A fundamental principle for the fair and efficient operation of any market, physical or digital, is independence of the market maker from the market participants. A bank, for example, must have Chinese walls between its brokerage operations and the other parts of its business. Digital markets largely lack such safeguards. Amazon, for example, is both the market place for much e-commerce and a trader in that market place. It can therefore, if it chooses, use pricing and sales information from running the market place to out compete other traders. It also gets to choose which traders to highlight, which also creates problematic issues of conflict.[8]

3.12 An example of the conflict of interest caused by vertical integration is seen in Google's practice of bundling exclusive access to Google data and YouTube video inventory with Display and Video 360 (DV360). DV360 is a demand side platform (DSP) technology that allows buyers to buy advertising inventory. A conflict arises because Google is a seller of inventory and determines where

---

5 See, for example, Free TV Australia, *Submission 17*, p. 9; Dr Janine Arantes, *Submission 40*, p. 2; Australian Competition and Consumer Commission (ACCC), *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 7.

6 See, for example, Professor Toby Walsh, *Submission 42*, [p. 1]; Vault Cloud, *Submission 38*, [p. 1]; Commercial Radio & Audio, *Submission 43*, pp. 6–7.

7 Vault Cloud, *Submission 38*, [pp. 1–2].

8 Professor Toby Walsh, *Submission 42*, [p. 1].

advertiser budgets are allocated, giving it the ability to preference its own services.[9]

3.13 Mr Ben Campbell, Director, Digital Advertising and Data Products, Nine Entertainment (Nine), clarified this practice, providing a specific example of when an advertiser wants to run a digital video campaign:

> The advertiser might say, 'Well, I want to access some of that rich targeting that Google has. I also said from the outset that I need to run my campaign on YouTube, so my only option is to run that campaign in DV360 as a DSP.' It would set up the campaign for 100,000 impressions and select those sites that it wants to run across. The DSP would choose the allocation of where that budget gets delivered. That is the issue. Google owns the DSP. It also owns some of that inventory in the form of YouTube inventory. Google is essentially deciding where that budget is being spent on behalf of the advertiser when it is running that campaign programmatically.[10]

3.14 Blockchain Australia stated that even threats of Big Tech expanding its offerings can stifle innovation:

> An example of this is the threats by Apple over a year ago to add a buy now pay later capability to Apple Pay. This has greatly impacted the development of an industry that started in Australia and had potential to grow internationally. Apple has still not gone live, but the threats have had the desired impact.[11]

Mergers and acquisitions

3.15 A merger is an agreement that unites two existing companies into a new company.[12]

3.16 A business acquisition is where a company purchases most or all of another company's shares to gain control of that company. Acquisitions are typically agreed between the two companies, but the term can be used interchangeably with 'takeover', in which one company takes control of another against the wishes of its management team.[13]

3.17 Mergers and acquisitions allow companies to expand and provide additional products and services, which may be beneficial to consumers. However, they may eliminate competition and entrench market power of large companies.

---

9 Free TV Australia, *Submission 17*, p. 8; Mr Ben Campbell, Director, Digital Advertising and Data Products, Nine Entertainment, *Proof Committee Hansard*, 3 October 2023, p. 25.

10 *Proof Committee Hansard*, 3 October 2023, p. 25.

11 Blockchain Australia, *Submission 45*, [p. 5].

12 Marshall Hargrave, *Merger: Definition, How It Works With Types and Examples*, 8 May 2022, https://www.investopedia.com/terms/m/merger.asp (accessed 6 November 2023).

13 Will Kenton, *What Is an Acquisition? Definition, Meaning, Types, and Examples*, 10 October 2023, https://www.investopedia.com/terms/a/acquisition.asp (accessed 6 November 2023).

3.18 Between 2008 and 2018, Amazon, Facebook (now Meta) and Google made approximately 300 acquisitions, 60 per cent of which involved firms that were less than 4 years old.[14]

3.19 Submitters raised concerns that large tech companies may adopt a strategy of acquiring rivals to eliminate or take control of other companies that threaten a platform's dominance. This undermines competition and allows Big Tech to gain additional advantages such as economies of scale, larger data sets and network effects that entrench their market power.[15]

3.20 The Centre for AI and Digital Ethics explained how Big Tech seeks to take out rivals that threaten their power:

> Killer acquisitions refer to the practice of acquiring competitors to shut down or take control of projects that threaten a platform's dominance or market share-a well-known phenomenon on [sic] the pharmaceutical industry. The most well-known instance of this conduct in the digital platforms context is Facebook's acquisition of lnstagram in 2012, which Facebook considered a 'threat'. This has a deleterious effect on competition and obviates the potential benefits of innovative new services.[16]

Self-preferencing

3.21 Vertical integration incentivises companies to engage in self-preferencing behaviours that may be anti-competitive.

3.22 Free TV Australia (Free TV) provided an explanation of self-preferencing behaviours:

> Self-preferencing refers to the practice of a platform using a dominant or gateway position in one market to provide an advantage to products and services the same company offers in related markets … Self-preferencing also occurs when a digital platform service forces businesses and consumers to use particular products or services of that platform in order to use the platform's products or services in a related market. This bundling and tying of products and services can occur, for example, through digital platform services only being available through one of its own offerings, or the imposition of interoperability restrictions.[17]

3.23 Examples of self-preferencing raised in submissions include:

- Apple and Google using data collected in the provision of app store services to inform the development of their own apps.

---

14 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 36.

15 See, for example, ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 31; Centre for AI and Digital Ethics, *Submission 23*, [p. 11]; Law Institute of Victoria (LIV), *Submission 12*, [p. 2]; Consumer Policy Research Centre, *Submission 60*, p. 3.

16 Centre for AI and Digital Ethics, *Submission 23*, [p. 11].

17 Free TV Australia, *Submission 17*, p. 7.

- Apple ranking its own apps more favourably than third-party apps in its App Store search results.
- Google promoting its own services in search results on Google Search.
- Google giving its own ad tech services favourable treatment compared to ad tech services provided by third parties.
- pre-installed web browsers such as Safari on iOS, or Google demoting rival shopping aggregator search results in favour of its own service.

3.24 The committee received evidence that self-preferencing behaviour by Big Tech platforms entrenches their market power and stifles competition.[18]

3.25 Self-preferencing may affect the ability of rivals to compete by reducing the discoverability of their products, raising costs through discriminatory terms and conditions of access, reducing innovation by limiting or denying interoperability, and utilising non-public data to 'free ride' off the innovation efforts of their rivals. It may also reduce incentives for competitors to enter and compete in digital platform markets, leading to reduced innovation and consumer choice, increased prices, and steering consumers to products that do not align with their preferences.[19]

3.26 Commercial Radio & Audio argued platforms are incentivised to preference their own products and discriminate against other companies due to vertical integration.[20]

3.27 However, the Australian Competition and Consumer Commission (ACCC) noted some forms of self-preferencing may be harmless or pro-competitive, for example, if it makes platforms more beneficial to consumers or leads consumers to more suited products.[21]

Self preferencing in search services

3.28 The ACCC's digital platforms inquiry highlighted the significant market power of Google in search and advertising services:

- Google has substantial market power in the supply of online search in Australia with approximately 94 per cent of online searches in Australia currently performed through Google.

---

[18] See, for example, Commercial Radio & Audio, *Submission 43*, p. 6; Commonwealth Bank of Australia (CBA), *Submission 71*, p. 3; Consumer Policy Research Centre, *Submission 60*, p. 3; Special Broadcasting Service, *Submission 3*, p. 8; Free TV Australia, *Submission 17*, p. 7; Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

[19] See, for example, ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, pp. 124-125; Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

[20] Commercial Radio & Audio, *Submission 43*, pp 6–7.

[21] ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, pp. 124–125.

- Google has substantial market power in the supply of online search advertising. This flows directly from its substantial market power in the consumer facing market for online search.[22]

3.29 Self-preferencing may give Google an unfair advantage, rather than services competing on merit. The ACCC identified 'many examples of Google favouring its own related services at the expense of third-party ad tech services' of which 'the cumulative effect … had been to lessen competition in the supply of a range of ad tech services'. The ACCC found Google had:

- restricted purchase of YouTube inventory to its demand-side platforms
- directed demand from its demand-side platforms (particularly Google Ads) to its own supply-side platform
- used its publisher ad server to preference its supply-side platform over time
- restricted how its supply-side platform works with third-party ad servers
- used its control over auction rules in its publisher ad server to advantage its other services
- announced plans which could allow it to use its position in providing the Chrome browser to preference its ad tech services.[23]

3.30 Self-preferencing of search services could affect multiple other related markets by preferencing services such as YouTube, Google Hotels and Google Flights. Increased competition from Google in these services could benefit consumers, but does not always do so. For example, Google Search displayed its own paid Google Play and YouTube services first, for a television show that could be viewed for free elsewhere.[24]

3.31 Dr Janine Arantes argued Google's dominance in the search engine market has allowed Google to bundle search services with email and cloud storage, creating a barrier to entry for competitors and limiting the choice available to educators and students.[25]

Default search engine settings

3.32 Submissions highlighted that one method Google has used to gain and maintain dominance is by being a default search engine.

3.33 DuckDuckGo, an internet search engine provider, stated that setting a default service is one of the most effective forms of self-preferencing, as users rarely switch to an alternative. It noted that, in 2018, Google observed users are

---

22 ACCC, *Digital Platforms Inquiry: Preliminary report*, 10 December 2018, p. 4.

23 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, pp. 129–130.

24 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 129.

25 Dr Janine Arantes, *Submission 40*, p. 2.

unlikely to change the default search engine on a mobile. DuckDuckGo explained:

> This strategy translated into Google securing the search default on its own operating system Android through licensing agreements, establishing the Google default on its own devices (Pixel phones or Chromebooks), and acquiring default positions elsewhere. According to the DOJ [United States Department of Justice], Google pays Apple between $8-12 billion annually in order to secure the search default across the Apple ecosystem. As a result, the DOJ estimates in its lawsuit against Google that "over 85 percent of all browser usage in the United States occurs on Google's own Chrome browser or on one of the browsers covered by these revenue sharing agreements."[26]

Self-preferencing in app markets

3.34 Apple and Google benefit from self-preferencing as they each have their own first-party app store that is pre-installed on Apple or Android devices. In 2021, Apple iOS and Google Android accounted for close to 100 per cent of mobile operating system use in Australia.[27]

3.35 Apple devices specifically restrict downloading of alternate app stores and thereby Apple 'faces no constraints on its market power in relation to iOS app distribution or in-app payment processing'.[28]

3.36 Google is 'by far the largest mobile app distribution platform on Android OS'.[29] Google allows other stores to be downloaded, though 90 per cent of purchases occur through the Google Play.[30] Submissions suggested other stores are rarely used because Google Play is pre-installed, displayed on the home screen of Android devices, and other stores have a smaller user base.[31] Match Group (Match) elaborated:

> Google has taken steps to quash competing app stores, including by erecting barriers to prevent users from downloading or using alternate stores, imposing restrictions on competing app stores that do not apply to the Google Play Store and by reaching anticompetitive agreements with other companies to not start alternative stores.[32]

3.37 Many Apple and Google apps enjoy the benefit of pre-installation, being set as defaults or having superior integration. Apple phones come pre-installed with

---

26 DuckDuckGo, *DuckDuckGo comments in response to [ACCC] Discussion Paper for Interim report No. 5, Updating competition and consumer law for digital platforms services inquiry*, April 2022, p. 4.

27 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 37.

28 Epic Games, *Submission 77*, [p. 1].

29 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 37.

30 Match Group, *Submission 73*, p. 3.

31 See, for example, Match Group, *Submission 73*, pp. 3-4; Epic Games, *Submission 77*, [p. 1].

32 Match Group, *Submission 73*, pp. 3–4.

Apple apps such as Apple Music, Apple TV, and Apple News. Google requires device manufacturers that pre-install the Google Play Store to also install other Google services. These services enable Apple and Google to attract and retain consumers within their platform ecosystems.[33]

3.38 Submitters raised concerns that the market power of Apple and Google gives them the ability and incentive to favour first-party apps at the expense of rival apps.[34] App stores may treat first-party apps more favourably than third-party apps by:

- ranking first-party apps more favourably in app store search results
- removing consumers' ability to rate and review first-party apps, which may result in a more positive ranking of first-party apps than otherwise
- providing first-party app developers with superior access to data, including information about rival apps. This includes information collected through app review processes, the operation of the app stores, and app developers' use of in-app payment systems
- delaying or blocking competing third-party apps' access to their app stores.[35]

3.39 The Centre for AI and Digital Ethics commented on how Apple preferences its own web browser, Safari, by using it as the default:

> For example, using its dominance in the mobile device market, Apple may set Safari as a default and give it unique access to system functionality within iOS. Such behaviour by Apple likely drives traffic away from competitors such as Firefox and towards Apple's own offering, reducing market competition.[36]

3.40 Epic Games, with regard to its attempt to introduce its own in-app payment system and subsequent litigation with Apple, commented:

> Developers are barred from reaching billions of iOS and Android users unless they go through the Apple and Google app stores and submit to whatever terms they impose. Opening mobile devices to alternate means of downloading applications and software is foundational to the creation of a more open ecosystem, whether it be alternative app stores or direct downloading of applications from the web. These solutions already exist and are regularly and safely used by consumers every day when they use

---

33 See, for example, Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy, Match Group, *Proof Committee Hansard*, 26 July 2023, p. 2; ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 133.

34 Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy, Match Group, *Proof Committee Hansard*, 26 July 2023, p. 2; ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 129.

35 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 127.

36 Centre for AI and Digital Ethics and Melbourne Law School, *Submission to the ACCC Digital Platforms Services Inquiry Discussion Paper [September 2022 interim report]*, April 2022, p. 2.

> their laptop or desktop computers, including PCs, [M]acs and Chromebooks. It is only when consumers shift from the computer on their desk to the computer in their pocket that they are limited to software installation through the App Store and Play Store. These limits are the product of commercial decisions by Apple and Google – not of safety or technical necessity.[37]

3.41 The Coalition for App Fairness stated that Apple has affected app developers and preferences its own digital well-being and parental control apps by restricting other developers from accessing certain device features. It argued Apple's preferencing 'undermines the ability of app developers to compete, innovate and solve issues of concern to consumers'. It gave an example:

> … following a change to its operating system, Apple made it very hard for third-party apps to ask users for permission to track their location when the app is not being used (functionality that is necessary for the operation of certain apps), while Apple tracks by default users' location at all times and users cannot opt out unless they go deep into Apple's settings.[38]

Tying

3.42 Tying conduct is a form of self-preferencing where a supplier provides one product or service on the condition that the purchaser buys another product or service from the same supplier.

3.43 A digital platform with market power may exclude or hinder its competitors by tying a service in which it has market power to a product or service it provides in a related market. This can damage competition in the related market by limiting access to users or reducing the ability of rivals to gain sufficient scale to profitably and effectively compete in that market.

3.44 Submissions raised concerns that tying of products and services limits competition and reduces consumer choice.[39]

3.45 Gumtree Australia explained:

> Gatekeepers often gain and maintain unfair market advantage by tying other (ancillary) services with their core platforms, nudging users to access and use the broader service offering within their ecosystem which have the effect of discriminating against or excluding competing solutions against the service owned by the platform. Examples are adjacent services (like a marketplace, a payment solution or distribution service) that are pre-installed, tied, embedded and/or integrated with their core platform service. Users are exposed to these services regardless of whether they choose to or not, thereby locking-in users while foreclosing competitors.[40]

---

37 Epic Games, *Submission to ACCC September 2022 interim report*, p. 7.

38 Coalition for App Fairness, *Submission to ACCC September 2022 interim report*, pp. 9–10.

39 See, for example, Free TV Australia, *Submission 17*, p. 7; Match Group, *Submission 73*, p. 1.

40 Gumtree Australia, *Submission to ACCC September 2022 interim report*, p. 3.

In-app payment tying in app markets

3.46 The Google Play Store and the Apple App Store require developers to pay commission fees on in app purchases (IAP) of 15 to 30 per cent. Further, each app store bans developers from informing consumers about opportunities to make purchases outside of the app.

3.47 Submissions stated that forced IAPs limit competition as they make it difficult for developers to compete with Apple and Google.[41]

3.48 The ACCC concluded:

> Tying of app store services to in-app payment systems leads to a loss of consumer choice as consumers are unable to use (and developers are unable to offer) any other payment option when making payments in apps. This could negatively impact the quality and functionality of the apps and services that app developers wish to provide their users, such as by limiting their ability to issue refunds or cancel subscriptions. It could also affect:
>
> - app developers' ability to make changes to the prices of in-app purchases
> - competition between apps that are subject to the requirement and apps that are not the choice of business model for app developers.[42]

Uneven playing field

3.49 Submissions stated the circumstances that determine which apps need to pay commission fees are arbitrary and lead app developers to compete on an uneven playing field.[43] Match described:

> … only 3% of developers [are] required to pay this fee to Google, and 16% required to pay this fee to Apple. There does not appear to be a justifiable rationale for Apple or Google to require some apps (offering digital services), and not others (offering physical services), to use their proprietary in-app purchase systems and pay a 30% commission.
>
> For example, Uber provides a similar type of service to Tinder: Uber connects a rider to a driver to meet and take a ride, while Tinder connects two people together so they can meet and go on a date. Yet, Uber is not required to use Apple's IAP because Apple considers it involves services consumed outside the Uber app. Similarly, Facebook, which since September 2019 has been providing a dating service, does not have to pay Apple for any services relating to its app (ie. distribution of its app to iOS users), save for an annual USD [US dollar] $99 fee.[44]

---

41 See, for example, Match Group, *Submission 73*, p. 1; Free TV Australia, *Submission 17*, p. 13; Epic Games, *Submission 77*, Appendix A, [p. 5].

42 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 133.

43 See, for example, Epic Games, *Submission 77*, Appendix A, [pp. 5–6]; Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy, Match Group, *Proof Committee Hansard*, 26 July 2023, p. 2.

44 Match Group, *Submission 73*, p. 6.

3.50 Free TV stated IAP tying leads to 'substantially different revenue outcomes for app developers/providers'.[45] Match explained that one reason this occurs is because:

> … subscription funded apps that are subject to the in-app tying condition must pay differential rates compared to those which are ad-powered. This results in the former paying hundreds of millions in commission fees to Apple and Google, while their rivals pay only USD$99 per annum to Apple or USD$25 registration fee to Google (which subscription-funded apps must also pay). This results in ad-powered apps having an enormous advantage over subscription-based apps, even if users would generally prefer a subscription-based service.[46]

3.51 Evidence to the committee suggested the 30 per cent fee is 'exorbitant' and limits developer profits.[47] For example, Epic Games stated the fee 'is around 10 times higher than fees charged by analogous electronic payment processors in competitive contexts, such as PayPal, Stripe, Square or Braintree, which typically charge payment processing rates of around 3%'.[48] It commented:

> … Apple and Google necessarily force developers to (i) suffer lower profits (rendering some apps financially unviable altogether), (ii) reduce the quantity or quality of their apps, (iii) raise prices for consumers, or some combination of the three … Opening the mobile ecosystem to the same level of competition and openness that consumers and developers experience on desktop computers will help ensure that self-determination and market forces – rather than the unilateral preferences of two companies – set the terms by which these products, services and industries evolve to meet consumer needs and demands.[49]

3.52 Match argued IAPs may be used by Apple and Google to plan their own prospective entry into developers' app categories using the sensitive customer data and other insights obtained. Apple may have already done this in relation to music streaming services (Apple Music), 'e-readers' (Apple Books), video streaming services (Apple TV), news (Apple News) and gaming (Apple Arcade).[50]

---

45 Free TV Australia, *Submission 17*, p. 13.

46 Match Group, *Submission 73*, p. 6.

47 See, for example, Epic Games, *Submission 77*, [p. 1]; Match Group, *Submission 73*, p. 7; Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy, Match Group, *Proof Committee Hansard*, 26 July 2023, p. 2.

48 Epic Games, *Submission 77*, Appendix A, [p. 5].

49 Epic Games, *Submission to ACCC September 2022 interim report*, pp. 8–9.

50 Match Group, *Submission 73*, p. 6.

Security concerns

3.53 Epic Games highlighted Apple's argument to the United Kingdom (UK) Competition and Markets Authority that:

> … if third-party app stores were able to operate on iOS devices, the level of protection against malware would move from Apple's high standard of review to the lowest standard offered by a third-party app store, creating a risk for the individual device and the overall ecosystem.[51]

3.54 However, Epic Games disagreed with Apple's statement:

> Apple self-servingly mischaracterises the risk and the function of the App Store app review process and its impact on device security. It also makes the baseless assertion that competition in app distribution would be a security "race to the bottom," rather than a "race to the top" where rivals with more innovative and secure app stores challenge Apple to do better. To the contrary, Apple's app review protections could be replicated—and even improved—by third parties. Anticompetitive app store policies should not get a free pass from scrutiny just because Apple or Google invoke privacy and security justifications … The choice between promoting competition and promoting security is not a binary one. Competition is likely to drive innovation and improvement in security and consumer privacy.[52]

IAPs limit app personalisation

3.55 Evidence to the committee suggested IAP tying may also hinder apps from catering to consumer needs by limiting the data developers can collect and by hindering communication.

3.56 Match contended that by not giving apps access to the IAP data, developers cannot address user needs influenced by geographical borders or historical context.[53] Match argued:

> By mandating the use of IAP tying, Apple and Google insert themselves as intermediaries between app developers and their customers, effectively usurping the customer relationship and impacting app developers' ability to service their customers. For example, when an iOS (Apple) user contacts Tinder to obtain a refund of their Tinder subscription, Tinder has no visibility or control over the user's purchase. Apple's process is opaque, inefficient and insufficiently staffed to keep developers informed about the status of a refund or request. Tinder has received negative user feedback regarding this process. In addition to harming developers, this intermediation increases users' reliance on Apple and Google, thereby

---

51 United Kingdom (UK) Competition and Markets Authority, *Mobile ecosystems market study interim report*, December 2021, pp. 373–374, cited by Epic Games, *Submission to ACCC September 2022 interim report*, p. 6.

52 Epic Games, *Submission to ACCC September 2022 interim report*, p. 6.

53 Match Group, *Submission 73*, p. 7.

> increasing the "stickiness" (and market power) of their respective platforms.[54]

3.57 Nine stated that IAP tying limits communication between developers and app users, meaning app users receive an inferior experience. Nine was concerned about the effect of this on the sustainability of its business:

> It is not always possible to communicate with these customers or understand if they are using the app, resulting in a worse customer experience and risking Nine's business relationship with app users. This could result in a premature churn of a subscriber due to the inability to showcase the breadth of value from our subscriptions. Even as more information was made available (through development effort and significant time spent working with Apple), Apple's App Store rules limit direct contact with these customers.[55]

3.58 Mr Luc Delany, Chief Executive Officer, International Social Games Association, commented that tying:

> … also creates a bottleneck on data. It means that we don't necessarily know how our customers are using the service. It gets further complicated when we, as the game being sold through the app store, we are increasingly obliged under data protection rules to know more about our customers to ensure we protect their data better. One of the best ways to do that would be to have a payment relationship with the customer. We can't have that relationship because we are blocked from doing so by the app stores.[56]

3.59 As noted in Chapter 7: Consumer harms, IAP tying also frustrates developer efforts to detect and respond to scams and identify bad actors as they have limited data to cross reference and verify user authentication.[57]

Interoperability

3.60 Consumers tend to use services and products that are defaults or with which they are familiar. This may reflect brand loyalty, 'learning costs' involved with new systems, or behavioural bias. These factors can be overcome more easily if barriers to switching, such as costs, are limited.[58]

3.61 Interoperability refers to the ability for systems or devices to work with other systems or devices. Interoperability allows consumers to move to new services or devices that better fit their needs. Features that lock consumers into a

---

54 Match Group, *Submission 73*, p. 4.

55 Nine Entertainment, *Submission to ACCC September 2022 interim report*, pp. 2–3.

56 *Proof Committee Hansard*, 3 October 2023, pp. 36–37.

57 Match Group, *Submission 73*, Appendix 2 (Match Group, 'Response to the Government consultation on the ACCC's regulatory reform recommendations for digital platforms', *Submission by Match Group Inc. to Treasury*), p. 3.

58 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 35.

particular system or platform by making it difficult for consumers to change are not interoperable.

3.62 Companies may impede consumers from switching products or services through bundling and tying practices that lock consumers in to one provider.[59] Features that lock consumers into a particular service may include:

- high switching costs
- challenges in coordinating a network of users to switch
- lack of transparency
- restrictions of accessing device functionality
- the inability to delete certain apps
- exclusive pre-installation and default settings such as for a browser or search engine.

3.63 Many submissions suggested services or features that are not interoperable are likely to limit competition, reduce consumer choice, and hinder innovation and quality of services.[60]

3.64 Free TV provided an example of how Google reduces interoperability to preference its own products at the detriment of supply-side platforms (SSPs):

> … Google imposes restrictions on how its products integrate with ad tech services such as header bidding (an ad tech service that enables a number of SSPs to bid against each other in real time) … The ACCC has found that Google's refusal to participate in industry-developed header bidding preferences its own SSP product. While there are workarounds available to include Google's SSP at the final stage of a heading bidding process, this process is sub-optimal and still places the Google SSP at a structural competitive advantage to those SSPs limited to inclusion in the initial header bid auction. Google's proprietary service, Exchange Bidding, itself is characterised by self-preferencing with non-Google SSPs subject to an extra fee if they win the auction process.[61]

3.65 Mr Mark Nottingham, expert advisor to the UK Competition and Markets Authority's Digital Markets Unit, suggested mandating interoperability would promote competition:

> While requiring companies with undue power to 'open up' interfaces is not a panacea, it does show great promise: not only would doing so open up opportunities for competing companies, but (if correctly applied) it would allow users to manage their data directly, without a commercial intermediary. This approach is in keeping with the architecture and historical examples of the Internet and the Web themselves. Openly

---

59 See, for example, Digital Transformation Agency, *Submission 7*, p. 5; Mr Rob James, Principal Consultant and Chief Executive Officer, Rob James Consulting Pty Ltd, *Proof Committee Hansard*, 26 July 2023, p. 32.

60 See, for example, Digital Transformation Agency, *Submission 7*, p. 5; Google, *Submission 49*, p. 19.

61 Free TV Australia, *Submission 17*, p. 11.

> specified, interoperable protocols and formats brought us these public goods and helped to assure that no single party had control over them. Legal pressure to provide interoperable interfaces to specific functions identified as 'chokepoints' for power — e.g., when there is an imbalance in power due to network effects — has the potential to do the same for social networking, shopping, chat, and other proprietary functions that have been built on top of the open Internet.[62]

Innovation

3.66 Mozilla stated that dealing with issues stemming from interoperability failure or self-preferencing by other platforms is a significant cost which could be otherwise spent on innovation:

> For example, Apple and Microsoft require their respective browser engines to be used in any browser product listed in their app stores. However, rebuilding a browser for a separate browser engine is a significant technical challenge that requires financial and human capital. This increases development costs and can prevent or delay market entry. For example, as of April 2021, Mozilla has no listing in the Microsoft App Store because development on Microsoft's browser engine (which is currently Google's Blink/Chromium) is impractical when the value of Firefox is in its unique Gecko browser engine. This impedes download and use of Firefox on Windows because it is not considered a "verified app" by Microsoft.[63]

Inability to exercise consumer choice

3.67 Submissions suggested locking features may limit the ability for consumers to make fully informed choices or exercise preferences, therefore reinforcing barriers to entry and expansion for competitors.[64]

3.68 The Australian Communications Consumer Action Network argued that messaging services lock consumers into one platform, which forces users to choose platforms based on social networks rather than the merits of each app. Further, it stated:

> Platforms often cite privacy and security as excuses for the lack of initiative in interoperability, but their lack of progress in finalising standards leads some critics to find this argument unconvincing. For example, the open-source Signal protocol already underpins many messaging apps and could serve as a preliminary cryptographic standard. The lack of messaging interoperability risks making communications worse for Australian consumers. SMS is a fundamental means of communication for many Australians. As Australians expect more from their messaging services, such as multimedia and reactions, standards will need to evolve to meet those expectations. However, Apple's iMessage, one of the most popular apps for SMS and messaging, limits interoperability with other apps. According to

---

62 Mr Mark Nottingham, *Submission 37*, p. 2.

63 Mozilla, *Submission to ACCC September 2022 interim report*, p. 10.

64 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 35; Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

> court documents, the lack of interoperability may be intentional to protect Apple's market share.[65]

3.69 The Australian Publisher's Association stated that digital platforms lock consumers to their platforms when purchasing books online. For example, eBooks purchased through Amazon can only be read on Amazon Kindle devices.[66]

Interoperability of mobile services

3.70 The committee was advised that interoperability for Apple and Android phones is limited.

3.71 The Centre for AI and Digital Ethics stated that Apple makes interoperability with other services such as Android difficult, 'allowing Apple to charge higher prices than they would if they had to compete on quality of product and service alone'.[67]

Downloading on Apple and Google devices

3.72 Apple has banned direct downloading on iOS devices. Google allows direct downloads but makes it difficult to download via alternative app stores or browsers. Google also 'imposes technical impediments, including multiple warning screens and requires settings adjustments, which discourage users from directly downloading applications onto their mobile devices'.[68]

3.73 Epic Games stated that these are unnecessary barriers:

> Apple and Google have argued that a closed ecosystem, which limits or bans direct downloads or competing App Stores while limiting interoperability, is the only guarantee of safety and privacy. Contrary to Apple and Google's claims, the choice between competition and security is not binary. Rather, greater competition in the distribution of applications on mobile devices will not only open the market to greater price competition, it will also spur innovation and improvements in security and privacy offerings. Many competition authorities around the world are grappling with these issues, including how to encourage meaningful competition in mobile ecosystems.[69]

Access to technology components

3.74 Apple prevents third parties from accessing the near-field communication (NFC) components that allow contactless payments on Apple mobile devices.

---

65 Australian Communications Consumer Action Network, *Submission to ACCC September 2022 interim report*, p. 10.

66 Australian Publisher's Association, *Submission 56*, p. 3.

67 Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

68 Epic Games, *Submission 77*, [p. 1].

69 Epic Games, *Submission to ACCC September 2022 interim report*, p. 5.

This means that any contactless payments on Apple mobile devices must be made using 'Apple Wallet' or 'Apple Pay'.

3.75 The ACCC raised concerns 'that this conduct may reduce competition in the supply of alternative payment apps and services, including preventing third parties from providing mobile wallet services that effectively compete with Apple's on its devices.' It also recommended regulations that allow parties access to the NFC functionality.[70]

3.76 The Commonwealth Bank of Australia agreed with this recommendation and added:

> … this needs to go further with any regulation of NFC chips and mobile wallets also needing to ensure that consumers have the same rights against the mobile wallet provider that they have against regulated financial institutions that provide payment services. The Government's announcement that digital wallets would be part of any new payments regulatory framework was encouraging and could go a long way to achieving this outcome.[71]

Interoperability of cloud services

3.77 Many submissions raised the lack of interoperability as limiting competition in cloud markets.[72]

3.78 Many cloud providers use proprietary systems or bundle costs that make it difficult for consumers to switch providers. Mr Rupert Taylor-Price, Chief Executive Officer, Vault Cloud, gave an example:

> … if you migrate from a government facility to ours, and back and forward, it's very free and easy. If you go onto a proprietary platform, where at deep layers of the technology they've potentially put hooks in that hold you into that environment, these are not things that benefit the consumer. These are there purely for the benefit of the provider.[73]

3.79 Google stated the lack of interoperability could result in reduced user-choice, higher consumer costs, lower quality of services, reduced security and stunted innovation.[74]

3.80 The Digital Transformation Agency argued:

> … one of the impediments to cloud competition is the cost and complexity of the supporting management and reporting tools that have been developed by large providers over time. These are often proprietary in

---

70 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 159.

71 CBA, *Submission 71*, p. 2.

72 See, for example, Digital Transformation Agency, *Submission 7*, p. 5; Google, *Submission 49*, p. 19.

73 *Proof Committee Hansard*, 26 July 2023, p. 21.

74 Google, *Submission 49*, p. 19.

> nature, and they are often critical in the cost-effective deployment of data and systems to the cloud. In most cases these tools are bundled with the cloud subscription costs and their use can create "lock-in" positions …[75]

3.81 Mr Rob James, Principal Consultant and Chief Executive Officer, Rob James Consulting Pty Ltd, echoed these concerns, stating:

> … a lot of these cloud providers are bringing proprietary technologies for organisations to use now. This is a double-edged sword. Some of these proprietary technologies actually help and encourage innovation in the ability to develop digital solutions rapidly, but it also provides a lock into that particular vendor. Again, if we look at larger organisations, they have the potential to have resources and capabilities to manage that and to be able to plan around that, but, for a lot of smaller organisations, that is close to impossible. The fact that you're leveraging the proprietary technologies to accelerate your digital solutions also means that you're potentially painting yourself into the corner and locking into that vendor, unless you intend to place some significant investments to orchestrate your way out of that if you need to.[76]

3.82 However, this view was not universally shared, with Amazon Web Services and Mr Nottingham commenting that interoperability is not an issue in the cloud sector.[77] Mr Nottingham stated:

> There is already significant competition in the largest cloud markets (especially infrastructure-as-a-service); consumers have many choices for services like virtual CPUs and block storage. In most cases, switching costs are reasonable; an adapter or library might be needed, but because many services share base concepts, it's hard to argue that there isn't a competitive market.[78]

Problems with the current regulatory framework

3.83 Competition in digital platform markets is primarily regulated by the ACCC under the *Competition and Consumer Act 2010* (CCA).

3.84 Many submitters stated enforcement of the current competition laws is insufficient to effectively address harms arising from entrenched market power of some digital platforms and promote competition.[79]

---

75 Digital Transformation Agency, *Submission 7*, p. 5.

76 *Proof Committee Hansard*, 26 July 2023, pp. 32–33.

77 Mr Mark Nottingham, *Submission 37*, p. 3; Amazon Web Services, *Submission 46*, p. 5.

78 Mr Mark Nottingham, *Submission 37*, p. 3.

79 See, for example, ACCC, *Submission 8*, p. 4; Free TV Australia, *Submission 17*, p. 14; Match Group, *Submission 73*, p. 7; CBA, *Submission 71*, p. 1.

3.85 The nature of the technology industry is fast-moving, opaque and complex, and new forms of conduct and harm can emerge rapidly. Anti-competitive conduct may be systemic and widespread, with the potential for significant harm.[80]

3.86 Under the CCA, enforcement is retrospective, addressing specific conduct on a case-by-case basis.[81] This approach is only capable of addressing discrete categories of conduct through a lengthy and costly process, and as a result is not effective or efficient. The immense scale and financial resources of digital platforms further impede traditional court enforcement and result in protracted litigation outcomes (as shown in Box 3.1).

3.87 Match elaborated on its perspective of the current regulatory framework:

> Markets for digital platforms services tend to be dynamic and fast paced, due to frequent innovations in terms of products and services offered by digital platforms. Given the length of typical enforcement cases (not to mention the uncertainty of the outcomes), there is a risk that the conduct of a digital platform may result in further harm while any enforcement proceedings are on foot. Further, it would be impossible for the ACCC to take enforcement action against all the different competition issues arising in different digital platforms markets one by one. This difficulty of ex post enforcement is heightened by the need to gather evidence in a litigious action, particularly if the necessary evidence is not preserved by digital platforms.[82]

3.88 Ms Kate Reader, General Manager, Digital Platforms Branch, ACCC, also shared her concerns:

> The current method of dealing with competition concerns in terms of bringing litigation in relation to individual, specific sets of actions is probably not the most effective way to deal with these large global platforms, particularly with things like self-preferencing, where particular digital platforms preference their own products over the products of third parties who may be smaller or unable to offer the suite of services that are offered by large digital platforms.[83]

3.89 Epic Games stated litigation cannot address systemic market issues. Further, the costs of litigation make it difficult for businesses to pursue issues:

> … litigation is costly – prohibitively so for many innovators, particularly small businesses, and new entrants. While Epic has brought legal proceedings against Apple and Google, few developers have the resources

---

80 See, for example, ACCC, *Submission 8*, p. 4; Free TV Australia, *Submission 17*, p. 14; Match Group, *Submission 73*, p. 7; CBA, *Submission 71*, p. 1.

81 ACCC, *Submission 8*, p. 4

82 Match Group, *Submission 73*, p. 7.

83 *Proof Committee Hansard*, 22 August 2023, p. 34.

to endure protracted litigation against two of the world's wealthiest companies.[84]

3.90 Where cases are not addressed in a timely manner, it can have significant costs for economic and consumer welfare. Factors like high barriers to entry and strong market power are often difficult to reverse, even if a platform ceases its conduct.[85]

3.91 Free TV argued enforcement action under the ACCC's existing powers is inadequate and 'unlikely to have broad deterrent value in the Digital Platform sector, where there are a small number of dominant providers engaging in a broad range of different types of anti-competitive conduct'.[86]

3.92 Free TV noted that for these reasons the ACCC has not taken enforcement action to comprehensively address competition or consumer issues in this sector.[87]

3.93 The ACCC also argued available remedies are not sufficient to adequately address harms, as digital platforms may simply change their conduct to achieve a similar outcome.[88]

Box 3.1 Examples of lengthy litigation

Australian examples

- In 2008, the ACCC first brought proceedings against Cement Australia Pty Ltd. After the liability judgment, relief judgment and an appeal, the Federal Court handed down judgment in 2017 upholding the ACCC's appeal.
- Between 2008 and 2010, the ACCC commenced proceedings against 15 international airlines for price fixing agreements. One proceeding (against PT Garuda Indonesia Ltd) was not finalised until 2021, when the airline withdrew its appeal against the penalty judgement.
- The ACCC initiated proceedings against Flight Centre in March 2012 for attempting to induce 3 international airlines into price fixing arrangements. Final penalties were ordered by the Full Court of the Federal Court in April 2018.

A private litigant, Epic Games, initiated legal proceedings in Australia against Apple in 2020 and Google in 2021 over Apple and Google's in-app payment requirements, including the level of their commissions. The cases won't go to trial until March 2024.

84 Epic Games, *Submission 77*, Appendix A, [p. 4].

85 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 51.

86 Free TV Australia, *Submission 17*, p. 15.

87 Free TV Australia, *Submission 17*, p. 15.

88 ACCC, *Submission 8*, p. 4.

International examples

- The Google Shopping case, which led to Google being fined EUR2.4 billion in 2017, took more than 7 years after the European Commission opened a formal investigation, with a decision on Google's appeal to the General Court in November 2021.
- The Google Android investigation, which led to Google being fined EUR4.125 billion in2022 took more than 7 years after the European Commission opened a formal investigation in 2015, and a decision on Google's appeal to the General Court in September 2022.
- The Google AdSense case, in which Google was fined EUR1.49 billion in 2019, took 9 years after the European Commission opened a formal investigation in 2010.
- In the US, a Department of Justice case alleging Google unlawfully maintained monopolies in search and search advertising is scheduled to go to trial in September 2023, 3 years after the agency filed a complaint.

Source: ACCC, Digital platform services inquiry, Interim report No. 5 – Regulatory reform, September 2022, pp. 48–49.

The case for reform

3.94 Evidence to the committee supporting implementation of new competition measures specific to digital platforms was mixed.

3.95 Many submissions supported greater regulatory oversight.[89] For example, Vault Cloud argued '[t]he current amount of regulation in the technology sector is disproportionately small relative to the risks that the sector poses to Australia's security' and supported increased regulation of IT to ensure the welfare of Australians. It stated that resistance to regulation is not unique to the digital platforms sector:

> … there have been many instances where industries have resisted regulation, often to the detriment of consumers. The examples of smoking, driving, aviation, food, pharmaceuticals, oil and gas, and firearms are just a few of the many instances where this has occurred. The current conduct of foreign technology companies is in line with these past behaviours. It is essential that regulations are put in place to protect public health, safety, and well being, even when the industry resists such measures.[90]

[89] See, for example, Match Group, *Submission 73*, p. 2; Free TV Australia, *Submission 17*, p. 3; ACCC, *Submission 8*, p. 1; Consumer Policy Research Centre, *Submission 60*, p. 7; CBA, *Submission 71*, p. 1; Centre for AI and Digital Ethics, *Submission 23*, [p. 11]; Commercial Radio & Audio, *Submission 43*, p. 2.

[90] Vault Cloud, *Submission 38*, [p. 4].

3.96 Epic Games argued:

> Regulatory action inherently is directed at remedying broader systemic failure and providing guidance and relief to all those impacted in a market … The Australian Government does not – and should not – need to await the outcome of private or ACCC proceedings instituted against Apple and Google to implement legislative reform.[91]

3.97 Other submitters did not support reform. They suggested that the digital platforms sector is highly competitive and that the characteristics identified (such as economies of scale, self-preferencing, optimising user experience, and mergers and acquisitions) are not unique to digital platform markets.[92]

3.98 Some submissions stressed that there are multiple ongoing initiatives seeking to address digital platform issues, and no further changes should be proposed until these current initiatives have been reviewed to avoid overlap.[93]

Proposed solutions

3.99 This section discusses proposed solutions to the competition issues raised in submissions. Submitters suggested aligning Australia with international regulations, implementing principles-based legislation and implementing industry codes. Submissions also proposed more specific solutions to limit anti-competitive effects of vertical integration, self-preferencing and tying, and to promote interoperability.

International alignment

3.100 Multiple submissions advised the committee that alignment with international regulations is important.[94]

3.101 The Tech Council of Australia considered Australia should avoid international regulatory conflicts:

> This is important because tech companies are born with the intention of becoming global – operating in multiple regions and nations, having a diversified workforce and tapping into a global market of customers. Many tech companies operating in Australia already 'benchmark' themselves by reference to global regulations including the EU's GDPR [General Data Protection Regulation] and those from ISO/IEC [International Organization for Standardisation/International Electrotechnical Commission] standards.

---

91 Epic Games, *Submission 77*, Appendix A, [p. 5].

92 See, for example, Developers Alliance, *Submission 35*, [p. 2]; Meta, *Submission 69*, p. 10.

93 See, for example, Communications Alliance, *Submission 58*, p. 7; BSA – The Software Alliance, *Submission 32*, p. 3; Amazon Web Services, *Submission 46*, p 6; Australian Institute of Company Directors, *Submission 28*, [p. 2].

94 See, for example, Tech Council of Australia, *Submission 63*, p. 5; Developers Alliance, *Submission 35*, [p. 5]; Epic Games, *Submission 77*, Appendix A, [p. 6].

> It is important for any outcomes from this inquiry acknowledges the need for international interoperability.[95]

3.102 Mr Delany commented positively about the EU Digital Markets Act[96], stating:

> We are optimistic that when it does come into effect it will create greater consumer choice and greater choice for developers as well in how they get their services in front of the consumer.[97]

Principles-based legislation

3.103 Various submitters recommended the introduction of principles-based legislation to address the competition issues raised throughout the inquiry.[98]

3.104 Evidence highlighted that principles-based legislation is flexible and can therefore capture emerging technologies.[99]

3.105 The ACCC recommended promotion of the following principles:

- competition on the merits
- informed and effective consumer choice
- fair trading and transparency for users of digital platforms.[100]

3.106 Epic Games supported the principles proposed by the ACCC, adding:

> … it is important to recognise that the term "user of digital platforms" encompasses developers, as well as consumers … Developers must program and support an app both on iOS and Android OS to successfully commercialise an app, and must adhere to Apple's and Google's unilateral, arbitrary and often opaque app store terms, just as consumers must. Consequently, to ensure the effectiveness of any codes of conduct, "fair trading and transparency" principles should apply to users on both sides of the mobile app marketplace.[101]

3.107 The inclusion of principles in legislation would be consistent with the proposed UK Digital Markets regime. The UK Government has proposed to set out three high-level objectives to establish the types of behaviour it will regulate. While

---

95 Tech Council of Australia, *Submission 63*, p. 5.

96 See Boxes 3.2—3.5 for further detail about the EU Digital Markets Act.

97 Mr Luc Delany, Chief Executive Officer, International Social Games Association, *Proof Committee Hansard*, 3 October 2023, p. 35.

98 See, for example, ACCC, *Submission 8*, p. 9; Consumer Policy Research Centre, *Submission 60*, [p. 7].

99 See, for example, Consumer Policy Research Centre, *Submission 60*, [p. 6]; LIV, *Submission 12*, [p. 6]; Office of the Australian Information Commissioner, *Submission 61*, p. 10.

100 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 12.

101 Epic Games, *Submission 77*, Appendix A, [p. 7].

wording is yet to be finalised, the objectives will relate to 'fair trading', 'open choices' and 'trust and transparency'.[102]

Industry codes

3.108 In the context of industry codes, the Communications Alliance recommended self or co-regulatory approaches be considered:

> Industry codes and consultation process have provided practical and flexible frameworks for addressing issues that often appear intractable. By providing a channel for industry knowledge and commitment, solutions can be developed that promote compliance without restricting growth or innovation in very dynamic environments. This is particularly important to ensure digital innovation and investment, employment and skills development continue to benefit the Australian economy.[103]

3.109 The ACCC recommended it be given powers to introduce sector-specific mandatory codes to address competition issues such as anti-competitive self-preferencing, denying interoperability, anti-competitive tying, and unfair dealings with businesses. These powers would come from implementing legislation that included guiding principles.[104]

3.110 The ACCC stated '[e]ach code would be for a single type of digital platform service (i.e. service-specific codes) and contain targeted obligations based on the legislated principles. This would allow flexibility to tailor the obligations to the specific competition issues relevant to that service as these change over time'.[105]

3.111 Multiple submissions supported the ACCC's proposal as it would provide regulatory certainty while also remaining flexible.[106]

Solutions for vertical integration

3.112 Evidence to the committee suggested Australia's current merger and acquisition regime may be ineffective in digital platform markets. Submitters suggested

---

[102] UK Government, *A new pro-competition regime for digital markets - government response to consultation*, 6 May 2022, www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/outcome/a-new-pro-competition-regime-for-digital-markets-government-response-to-consultation (accessed 6 November 2023).

[103] Communications Alliance, *Submission 58*, p. 8.

[104] ACCC, *Submission 8*, p. 8.

[105] ACCC, *Submission 8*, p. 8.

[106] See, for example, Match Group, *Submission 73*, p. 2; Free TV Australia, *Submission 17*, p. 3; CBA, *Submission 71*, p 1; Centre for AI and Digital Ethics, *Submission 23*, [p. 11]; Commercial Radio & Audio, *Submission 43*, p. 2.

merger reform to address market power arising from vertically integrated companies.[107]

3.113 The Consumer Policy Research Centre recommended the merger and acquisition framework should be reviewed to consider 'the acquisition of existing or potential competitors, the economies of scope gained from additional data sets and growing network effects'.[108]

3.114 The ACCC recommended an economy wide merger review that considers acquisitions of digital platforms:

> Although such challenges are not unique to acquisitions by digital platforms, they are particularly acute in markets for digital platform services due to their fast-paced and dynamic nature, significant market concentration, high barriers to entry and expanding ecosystems. Network effects also mean that the gains from achieving market power are substantial, as such market power is more likely to be enduring.[109]

3.115 Free TV also suggested legislating requirements that assist in addressing the conflict of interest caused by vertical integration in an advertisement technology code:

> To address conflicts of interest, the Code should include ad exchange provisions that govern how auction processes, and any other ad tech services trading processes, are to be conducted by designated entities. This will ensure that exchange processes are both transparent and that conflicts of interest are adequately addressed.[110]

---

107 See, for example, ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 60; Consumer Policy Research Centre, *Submission 60*, [p. 3]; Centre for AI and Digital Ethics, *Submission 23*, [p. 13]; Epic Games, *Submission 77*, [p. 2].

108 Consumer Policy Research Centre, *Submission 60*, [p. 3].

109 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 59.

110 Free TV Australia, *Submission 17*, p. 21-22. Free TV Australia suggested '[w]hen operating exchange services, designated entities should be obliged to clearly disclose how and when buy and sell orders will be matched (including mechanics of the sales process and other aspects). Further, designated entities that provide both DSP [Display Side Platform] and SSP [Supply Side Platform] services must ensure that the auction, DSP bidding and SSP selection decisions for any transaction must be determined by an independent third party. In relation to pricing, different models could be adopted in the Code to achieve transparency for discrete services. For example, in relation to ad tech services, a real time dashboard of ad tech service provider costs for a campaign could be prescribed which would allow advertisers to consider the costs versus the potential benefits of going directly to publishers to engage in a direct deal.'

Solutions for self-preferencing

3.116 Multiple submissions called for regulation that prevents gatekeeper companies from self-preferencing and referenced international approaches that could guide Australia (see Box 3.2).[111]

3.117 Submitters recommended the introduction of a prohibition which would restrict a platform with dominant market power self-preferencing its services and products over those of third parties.[112]

3.118 The ACCC noted there may be 'legitimate justifications for some types of self-preferencing conduct, such as promoting efficiency, or addressing security or privacy concerns, which would need to be carefully considered in developing new obligations.'[113]

Box 3.2 International approaches to addressing self-preferencing

EU: The Digital Markets Act:

- prohibits gatekeepers from providing favourable treatment in ranking, indexing and crawling of their own products and services compared to similar services or products of a third party.
- requires gatekeeper platforms to apply transparent, fair and non-discriminatory conditions to such ranking.
- prohibits gatekeepers from using, in competition with business users, data that is not publicly available and generated by their business users.

UK: The UK Government's proposed pro-competition regime for digital markets addresses anti-competitive self-preferencing. It requires digital platforms to not influence competitive processes or outcomes in a way that unduly self-preferences a platform's own services over those of rivals and limits the ability of firms to use data collected from customers and business users for reasons other than the app review process.

Germany: Under the 10th Amendment to the German Competition Act, Germany's competition agency has the ability to prohibit companies from treating the offers of competitors differently from its own services.

111 See, for example, ACCC, *Submission 8*, p. 9; Free TV Australia, *Submission 17*, p. 18; Match Group, *Submission 73*, p. 25; Centre for AI and Digital Ethics, *Submission 23*, [p. 13]; Commercial Radio & Audio, *Submission 43*, pp. 6–7; Consumer Policy Research Centre, *Submission 60*, p. 3.

112 See, for example, ACCC, *Submission 8*, p. 9; Commercial Radio & Audio, *Submission 43*, pp. 6-7; Consumer Policy Research Centre, *Submission 60*, p. 3.

113 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 131.

US: The proposed American Innovation and Choice Online Act prohibits covered platforms from preferencing their own products, services or lines of business over those of another business user in a manner that would materially harm competition.

Source: Digital Markets Act 2022 (EU); UK Government, A new pro-competition regime for digital markets, July 2021; German Competition Act (DE); American Innovation and Choice Online Act 2021 (US).

Solutions for tying

3.119 Submitters supported regulation that prohibits digital platforms with dominant market power from tying services, in particular the tying of IAPs.[114]

3.120 Mr Delany recommended Australia adopt regulations:

> … allowing for competing app stores. The other, linked to that, is competing payments, even if through the Apple app store or through the Google Play store, so that the consumer can choose whether to use Apple Pay or Google payments. Or they could use PayPal or they could pay directly to the games company.[115]

3.121 Epic Games urged for 'implementation of provisions that would open mobile devices to alternative app distribution, including competing app stores and sideloading' to address tying concerns. It suggested to:

> … open-up existing mobile app distribution ecosystems, unlocking competition and innovation benefits. Any new regulation will also need robust anti-circumvention provisions to ensure Apple and Google comply with the terms and purpose of the law and do not shift their anticompetitive behavior [sic] into an adjacent portion of the mobile app ecosystem.[116]

3.122 Match requested prioritisation of legislation that bans forced IAPs 'because it can be solved much more simply than some of these other issues'.[117]

3.123 Submissions also highlighted international approaches that could be used to guide Australia (see Box 3.3).

Box 3.3 International approaches to address tying

EU: The Digital Markets Act:

- prohibits gatekeepers from requiring users to use certain services to use a core platform service.

[114] See, for example, ACCC, *Submission 8*, p. 9; Free TV Australia, *Submission 17*, p. 18; CBA, *Submission 71*, p. 3; Match Group, *Submission 73*, p. 2; Mr Luc Delany, Chief Executive Officer, International Social Games Association, *Proof Committee Hansard*, 3 October 2023, p. 36.

[115] Mr Luc Delany, Chief Executive Officer, International Social Games Association, *Proof Committee Hansard*, 3 October 2023, p. 36.

[116] Epic Games, *Submission 77*, [p. 2].

[117] Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy, Match Group, *Proof Committee Hansard*, 26 July 2023, p. 3.

- prohibits gatekeepers from requiring users to subscribe to, or register with, any other core platform services as a condition for using the gatekeeper's core platform services.
- prohibits gatekeepers from requiring users to use payment systems for in-app purchases of that gatekeeper.

UK: The proposed pro-competition regime recommended requirements that require firms with strategic market status to not bundle or tie its services in a way which have an adverse effect on users. It also recommended that the Digital Markets Unit be able to oblige certain firms to provide access to inventory on reasonable terms.

Germany: The 10th Amendment to the German Competition Act can require firms of paramount significance to not make the use of a service conditional on the use of another service.

US: The proposed American Innovation and Choice Online Act contain prohibitions on tying conduct. For example, it prohibits covered app stores from requiring developers to use an in-app payment system owned or controlled by the company.

South Korea: Amendments to the Telecommunications Business Act require major app store operators such as Apple and Google to unbundle the use of their proprietary in-app payment systems from the use of app distribution services.

The Netherlands: To comply with competition orders in the Netherlands, Apple now allows developers distributing dating apps on the App Store in the Netherlands to use a third-party payment system within the app.

Source: Digital Markets Act 2022 (EU); UK Government, A new pro-competition regime for digital markets, July 2021; German Competition Act (DE); American Innovation and Choice Online Act 2021 (US); Telecommunications Business Act (S.KOR); Match, Submission 73, p. 17.

3.124 In response to South Korean amendments to its Telecommunications Business Act that required app store operators to unbundle in-app payments from the use of apps, Google and Apple announced they will allow developers to add their own billing system. However, Google will still charge a commission, but deduct four per cent, and Apple will charge 26 per cent.[118] The South Korean

[118] Kotaro Hosokawa, *Apple accepts 3rd-party app payments in South Korea -- for a 26% fee*, 2 July 2022, https://asia.nikkei.com/Business/Technology/Apple-accepts-3rd-party-app-payments-in-South-Korea-for-a-26-fee (accessed 24 November 2023); James Vincent, *Google outlines plans for first alternative in-app payments in South Korea*, 4 November 2021, www.theverge.com/2021/11/4/22763040/google-in-app-purchases-alternative-south-korea-payments (accessed 24 November 2023).

Communications Commission is investigating Apple and Google over potential violations of the new legislation.[119]

3.125 Mr Delany argued the reductions are not meaningful as '[i]t's not worth the aggravation of setting up your entire own payment mechanism for a 3 per cent reduction in fee.'[120]

3.126 Epic Games cautioned:

> … in-app payment reform alone may be insufficient to discipline Apple's and Google's control over the mobile economy. While it is important to establish clear rules that make Apple and Google offer third party payment services, payments are just one part of a broader pattern of Apple's and Google's monopolist behaviour. Their ability to levy supracompetitive 'rents', whether levied through app store dominance or payment rules, are an indication of their respective monopolies, and require comprehensive action to prevent them from simply finding new ways to charge or allocate commissions in response to enforcement measures. Without the creation of an independent market for mobile app distribution, Apple and Google can continue to play an app store fee "shell game" with developers and consumers. That is why, as a baseline, the codes must provide for alternative app distribution means outside the proprietary app stores, including sideloading and competing app stores.[121]

Solutions for interoperability

3.127 Submissions called for regulation that promotes interoperability and cited international approaches that could guide Australia (see Box 3.4).[122]

3.128 For example, Free TV argued that regulations that ensure interoperability of designated entities with third-party vendors should be implemented:

> … to ensure that designated entities cannot use claimed technical limitations to entrench and extend their market power to unduly incentivise or lock other participants into using the designated entity's products or services. Interoperability measures would in part be addressed by including in the Code requirements for designated entities to apply the same rules, provide access to key inputs on fair and non-discriminatory grounds and give the same information to all other digital advertising services providers.[123]

---

119 Joyce Lee, *South Korea warns Google, Apple of possible fines over apps marketing*, 7 October 2023, https://www.reuters.com/technology/skorea-considers-505-mln-fine-against-google-apple-over-app-market-practices-2023-10-06/ (accessed 24 November 2023).

120 Mr Luc Delany, Chief Executive Officer, International Social Games Association, *Proof Committee Hansard*, 3 October 2023, p. 36.

121 Epic Games, *Submission 77*, Appendix A, [p. 8].

122 See, for example, Mr Mark Nottingham, *Submission 37*, p. 2; Free TV Australia, *Submission 17*, p. 3; ACCC, *Submission 8*, p. 9; Centre for AI and Digital Ethics, *Submission 23*, [p. 13].

123 Free TV Australia, *Submission 17*, p. 20.

3.129 Mr Nottingham suggested that regulation is needed, as specifications written by companies cater to their own needs, not those of competitors or society. He recommended using international standards as a guide:

> … existing international and open Standards Development Organisations (SDOs) like the IETF and W3C are the most suitable venues for creating interoperability specifications. They have the necessary expertise, a proven track record, are transparent, and have reasonable processes for avoiding domination by any one concern. Importantly, civil society organisations, academics and governments are already represented in their work. For example, the IETF MIMI Working Group has just been created. If it successfully delivers an appropriate specification, this should address the interoperability requirements for messaging created by the European Digital Markets Act.[124]

Box 3.4 International approaches to promoting interoperability

EU: The Digital Markets Act:

- includes measures to allow competing service and hardware providers to have effective interoperability for free.
- prohibits gatekeepers from mandating the use of a particular browser engine.
- requires gatekeepers to enable the installation and effective use of third-party apps and app stores.

The proposed Data Act sets out obligations on interoperability and measures to prevent anti-competitive practices within the cloud market (e.g. charging disproportionate switching fees).

UK: The UK Competition and Markets Authority has proposed potential interventions for mobile ecosystems to allow access for third-party app stores, browser engines and apps, subject to appropriate safeguards.

US: The Open Markets Act requires covered companies to allow and provide readily accessible means for consumers to install third-party app stores on the operating system, as well as the ability to hide or delete preinstalled app stores on the operating system.

Source: Digital Markets Act 2022 (EU); UK Government, Competition and Markets Authority, Mobile ecosystems: Market study final report, June 2022; American Innovation and Choice Online Act 2021 (US).

Regulatory designation

3.130 Some submissions cautioned the committee on a 'one-size-fits-all' approach to regulation that could affect smaller businesses.[125]

---

[124] Mr Mark Nottingham, *Submission 37*, p. 2.

[125] LIV, *Submission 12*, [p. 3]; Tech Council of Australia, *Submission 63*, p. 2; Blockchain & Digital Assets Pty Ltd, *Submission 18*, pp. 1–2.

3.131 The Law Institute of Victoria (LIV) explained:

> … the LIV cautions against reform which has the effect of limiting entrepreneurship or technological and small business innovation within Australia. The LIV supports reform which has the effect of creating opportunities for new market entrants to succeed or existing smaller technology organisations to grow. The LIV recommends that any regulatory framework distinguish between Big Tech companies with significant market power and smaller tech companies by determining a threshold based on net profit or the number of users.[126]

3.132 Some submissions recommended that competition legislation, and any codes, should apply only to designated entities.[127]

3.133 These submissions recommended a designation approach similar to approaches implemented overseas (see Box 3.5). Criteria for designation could include:

- designation if an entity reaches a certain number of users.
- designation if a certain revenue threshold is met.
- consideration of whether the platform holds an important intermediary position or if it has substantial market power.[128]

3.134 Free TV recommended Google, Meta and Apple and related bodies corporate be designated as they are dominant in each of the markets they operate.[129] It supported the first two criteria listed above:

> These criteria are objective and the thresholds would be able to be set at appropriate levels to capture only platforms that hold market power, without adding the uncertainty of introducing an additional threshold test, such as whether the platform is considered to be a critical trading partner, as suggested in the US antitrust bills. For transparency purposes, it is recommended that the new Part of the CCA provides that the ACCC should undertake a short consultation with all stakeholders, not simply the impacted entity, prior to a designation being made. If an entity is designated, that entity should be subject to each code that applies to any digital platforms services provided by that designated entity.[130]

Box 3.5 International approaches to designation criteria

EU: The Digital Markets Act designates a digital platform as a 'gatekeeper' if it achieved an annual turnover equal to or above €7.5 billion in each of the last three financial years.

---

126 LIV, *Submission 12*, [p. 3].

127 See, for example, Free TV Australia, *Submission 17*, p. 17; ACCC, *Submission 8*, pp. 8–9; Epic Games, *Submission 77*, Appendix A, [p. 6].

128 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 12; Free TV Australia, *Submission 17*, p. 18.

129 Free TV Australia, *Submission 17*, p. 17.

130 Free TV Australia, *Submission 17*, p. 18.

US: The proposed American Innovation and Choice Online Act covers platforms owned or controlled by a person with net annual sales of greater than US$550 billion.

Japan: The Act on Improving Transparency and Fairness of Digital Platforms designates businesses based on yearly sales income.

Source: Digital Markets Act 2022 (EU); American Innovation and Choice Online Act 2021 (US); Improving Transparency and Fairness of Digital Platforms Act (JPN).

Chapter 4
Bargaining imbalances

4.1 International digital platforms hold a significant level of power over individuals and Australian businesses, ranging from small enterprises operating via online marketplaces, news media selling content and buying advertising services, to the Australian Government's use of cloud infrastructure and services.

4.2 This chapter discusses issues relating to this bargaining imbalance, including:

- how unfair contract terms can be implemented by BigTech.
- unfair trading practices used by Big Tech.
- inadequacy of dispute resolution processes and options for reform.

Unfair bargaining power and contract terms

4.3 Businesses' reliance on Big Tech leaves them vulnerable to exploitative or unfair contract arrangements.

4.4 Submitters argued the significant market power of digital platforms means consumers have no or limited bargaining power to negotiate terms, conditions and prices.[1] This power imbalance means platforms can impose exploitative agreements where terms are offered on a 'take it or leave it' basis.[2] This imbalance is explored below across a range of markets and service types.

4.5 The NSW Small Business Commissioner 2022 Small Business Survey found:

> … one in four [small businesses] encountered difficulties with the digital platform or online marketplace. Qualitative survey responses suggest small businesses experience challenges leveraging the benefits of online marketplaces or digital platforms and accessing customer service and support … Reported challenges includes pricing structures that do not align with small business profit margins, high service charges without performance accountability and payment delays which make it difficult for small businesses to manage their cashflow.[3]

Data terms

4.6 A significant number of businesses are reliant on Big Tech for advertising on social media services and search engines. This reliance enables Big Tech to impose unfair conditions on business transactions, forcing businesses to grant

---

1 See, for example, Australian Institute of Company Directors, *Submission 28*, [p. 6]; Mr Cian Byrne, *Submission 75*, [p. 2]; NSW Small Business Commissioner, *Submission 6*, [p. 2].

2 See, for example, Centre for AI and Digital Ethics, *Submission 23*, [p. 12]; Free TV Australia, *Submission 17*, p. 10; Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy, Match Group, *Proof Committee Hansard*, 26 July 2023, p. 1.

3 NSW Small Business Commissioner, *Submission 6*, [p. 2].

access to user generated data and facilitating Big Tech gains in advertising revenue, against the threat of losing access to the platform service altogether.[4]

4.7 Free TV Australia (Free TV) advised the committee of multiple instances where Big Tech companies used their dominant market power to enforce non–negotiable contract terms. It submitted these terms are unfair and anticompetitive:

> … because there is no reason to link data collection with services offered in other markets, other than to provide such a financial disincentive for the publisher to opt out, that they continue to share the data with Google or Meta, as applicable, so as to not suffer revenue loss.[5]

4.8 It provided the following examples:

- Google requires publishers to give Google ownership of all data collected as part of providing ad server services. If an ad publisher opts out of this requirement, Google automatically disables eligibility of that publisher's inventory from accepting any Google data targeted campaigns.
- Meta forces publishers to share user data with Meta when implementing sharing tools to allow users to share articles on Meta's social media platforms.
- The Google Ad Manager product for connected televisions collects user data and passes it through the ad tech stack for use in other market segments. When requests have been made by app developers to stop this data collection practice, Google stated that this feature is 'part of their roadmap and is not able to be switched off locally.[6]

Books

4.9 Submissions commented on how the market power of large eBook sellers, particularly Amazon, creates negotiating imbalances and disadvantages physical and smaller businesses.

4.10 The Australian Publisher's Association observed:

> International online retailers like Amazon have significantly impacted physical bookstores, making it difficult for them to compete with their convenience, extensive selection, and discounted prices. This has led to a decrease in foot traffic to physical bookstores, negatively impacting small businesses that rely on in-store sales. Amazon's dominance has also made it harder for smaller publishers and independent authors to get their works noticed.[7]

---

4 See, for example, Centre for AI and Digital Ethics, *Submission 23*, [p. 12]; Free TV Australia, *Submission 17*, p. 10.

5 Free TV Australia, *Submission 17*, p. 10.

6 Free TV Australia, *Submission 17*, p. 10.

7 Australian Publisher's Association, *Submission 56*, p. 5.

4.11 The Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA) commented on issues caused by monopoly suppliers being able to unilaterally change terms without notice and control supply of digital resources. It provided an example of Amazon refusing to allow libraries to purchase certain eBooks:

> As authors are bound to exclusive publishing deals, when a platform such as Amazon refuses to license to libraries those books are not available to the wider public through the library service, cutting off equitable access to these resources. Unlike physical books, there are no alternative sellers for libraries if a monopolistic platform will not negotiate. The library cannot buy from another supplier, or purchase second hand materials. The community simply has no access.[8]

4.12 The ALIA and NSLA further stated that Amazon's practices affect the incomes of authors, for example by encouraging consumers to return audiobooks for full refunds:

> When an audiobook was "returned" the author had to pay back the money from the original sale. In essence Amazon was giving customers a library-like experience, however unlike a library which pays for content, this model was being financed from authors' meagre incomes.[9]

App stores

4.13 The Apple and Google app stores are nearly the only options for creators of mobile apps to provide their product to consumers. Therefore, developers must accept their terms and conditions of usage in order to sell their product.

4.14 Submitters argued this level of market control enables Apple and Google to impose prescriptive and even harmful conditions on app developers' access to each app store that may limit, eliminate, or otherwise interfere with app developers' ability to distribute their applications.[10]

4.15 Mr Luc Delany, Chief Executive Officer, International Social Games Association, stated:

> We are highly regulated by the app stores, which set up their own sets of policies, and they have a high degree of control over how our services are operated and how a consumer can use and purchase from us or, through the platform, through the app stores. The app stores dictate the terms of service. They are take it or leave it. They dictate if your service even gets in front of a customer and if it is discovered, how it's discovered.[11]

---

8 Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA), *Submission 57*, p. 2.

9 ALIA and NSLA, *Submission 57*, p. 3.

10 See, for example, Match Group, *Submission 73*, pp. 3–4; Mr Luc Delany, Chief Executive Officer, International Social Games Association, *Proof Committee Hansard*, 3 October 2023, p. 35.

11 *Proof Committee Hansard*, 3 October 2023, p. 35.

4.16 Similarly, Free TV gave an example of Apple changing terms without notice:

> … for apps that required a sign-on, those apps must now offer "Sign in with Apple" as an option. This change was made with no ability to negotiate with Apple for alternative arrangements. The announcement was made on 12 September 2019. Any apps that were in development at that time had to immediately comply with the new terms and conditions. Existing apps had until April 2020 to comply. While the development costs associated with this change were significant, more fundamentally, this changed the nature of the relationship between the consumer and the app developer/provider. Rather than a more direct communication between local content providers and their users, Apple now controls that interaction through a hashed e-mail address that routes all communication via their servers. There is no transparency as to how Apple itself uses the information that it is able to be obtained by performing this intermediation role.[12]

Cloud

4.17 In relation to cloud markets, some submissions argued that the dominant market power of Amazon Web Services makes it difficult for smaller businesses to negotiate contract terms and get fair prices.[13]

4.18 Mr Rob James, Principal Consultant and Chief Executive Officer, Rob James Consulting Pty Ltd, described the market as a 'pseudo-duopoly between Microsoft and Amazon' which affects the ability of small businesses to compete.[14] He stated smaller cloud businesses:

> … don't have the resources or the capabilities to be able to manage or negotiate a structure that is going to be suitable for them when dealing with large organisations that are very inept to be able to negotiate anything specific for them … you're limited to dealing with a handful of players that are based predominantly in the United States … Again, for larger public sector organisations that do have some buying power, that's less of an issue, but, for the small to medium sector, that does become a challenge ...[15]

4.19 This view was contested by Amazon Web Services, which argued that the cloud sector is highly competitive as it is 'a small fraction of the global IT services market' and faces numerous competitors.[16]

4.20 Submissions argued the dominance of some Big Tech providers in the cloud sector means they can impose non-transparent agreements, making it difficult for business consumers to understand conditions of signing up to a particular

---

12 Free TV Australia, *Submission 17*, p. 13.

13 See, for example, Mr Cian Byrne, *Submission 75*, [p. 2]; Australian Institute of Company Directors, *Submission 28*, [p. 6].

14 *Proof Committee Hansard*, 26 July 2023, p. 34.

15 *Proof Committee Hansard*, 26 July 2023, pp. 32–33.

16 Amazon Web Services, *Submission 46*, p. 5.

service, such as disadvantageous terms or switching costs.[17] Google summarised:

> Importantly, restrictive contracting and tendering practices are often not transparent to industry participants in confidential tender processes, and cloud customers may not appreciate the disadvantages of restrictive terms until they later seek to add new cloud functionality or switch some services (or consider upfront price too attractive to refuse in any event). With overly complex agreements that lock in clients for years to come, some legacy software vendors may be forcing customers toward a monolithic cloud model, but also creating downstream effects that would limit choice and potentially disrupt growing and thriving digital ecosystems around the world.[18]

4.21 The committee was advised that customer billing information is provided in an opaque fashion, making it difficult to switch between services because customers cannot understand their current consumption costs. One submission provided an example of the confusing billing system:

> Amazon Web Services [AWS] has multiple websites to determine your final bill or invoice. The information is spread across these multiple sites, making it very difficult (some would say impossible) to determine what cloud services have really been purchased. One of the billing websites ('AWS Cost Explorer API') requires users to pay to access the information about what the user has spent money on. Amazon Web Services has another billing related website that summarises the final costs as 'zero dollars' unless you expand each of the individual services that have been consumed. The immediate impression a user gets when visiting the billing summary is that they have not spent any money, which is very incorrect and, in my opinion, deceptive. Microsoft Azure and Google Cloud Platform both experience similar issues (not as poor in my view). An example that is common across each cloud provider is that users cannot map individual service usage to the amount it cost… The end result is that users of these cloud providers end up paying for services that they do not even know they have switched on or have enabled.[19]

Telecommunications

4.22 Optus highlighted the 'significant imbalance in power' between telecommunications companies and large 'streamers', such as Netflix, YouTube, Disney, Amazon Prime, Facebook, Instagram and TikTok.[20]

4.23 Optus raised issue with the fact that streamers do not pay for traffic over the telecommunications infrastructure. The rapid growth of telecommunications traffic has placed strain on communications infrastructure and forced

---

17 See, for example, Google, *Submission 49*, p. 20; Mr Cian Byrne, *Submission 75*, [p. 2].

18 Google, *Submission 49*, p. 20.

19 Mr Cian Byrne, *Submission 75*, [p. 2].

20 Optus, *Submission 76*, p. 5.

telecommunications providers to make large capital investment to keep up with demand. It is a growing concern for telecommunications providers to sustain the required growth.[21]

4.24 Streamers obtain additional revenue from high bandwidth services, without incurring additional costs. Optus summarised:

> Essentially, streamers benefit significantly from a substantial cross-subsidy provided by the Australian communications sector and internet users, leading to an unsustainable imbalance that permeates the entire telecommunication ecosystem.[22]

4.25 Optus recommended implementation of a policy that requires large streamers to contribute to investment costs. This could be through the establishment of regulated commercial agreements or a digital levy. The United Kingdom (UK), Spain, France and Switzerland have all implemented digital services taxes or levies of this kind.[23]

4.26 Relatedly, the Australian Small Business and Family Enterprise Ombudsman (ASBFEO) suggested the government continue to invest in regional broadband to support small businesses. Access to reliable internet supports competition as it allows businesses to innovate, reach new customers and grow online.[24]

Financial technology (fintech)

4.27 The committee was advised that there are a limited number of payment platforms used in Australia, creating an uncompetitive environment for payment technology pricing.[25]

4.28 AirWallex stated the current Australian payment laws and regulations exacerbate the market concentration of payment platforms such as Apple Pay and Google Pay.[26]

4.29 This market dominance makes it difficult for innovative fintech companies and payment providers to succeed, in turn limiting competition for bigger companies such as banks 'and ultimately leading to less choices and higher prices for Australian families and businesses'.[27] The small number of accessible

---

21 Optus, *Submission 76*, p. 5.

22 Optus, *Submission 76*, p. 5.

23 Optus, *Submission 76*, p. 3.

24 Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *Submission 39*, [p. 3].

25 Airwallex, *Submission 67*, [p. 2].

26 Airwallex, *Submission 67*, [p. 1].

27 Airwallex, *Submission 67*, [p. 2].

payment networks and technology platform providers means payment providers have limited ability to 'shop around' for better deals.[28]

4.30 AirWallex advised that to match consumer expectations, payment providers such as AirWallex must use popular online payment platforms. The Reserve Bank of Australia (RBA) mandates pricing restrictions on the fees paid by merchants for the use of card-based transactions (interchange fees). However, the RBA 'does not regulate the costs those payment platforms charge payment providers, and the interchange fee restrictions are less than it costs to use a payment platform'.[29]

4.31 Payment providers must therefore process transactions for consumers at a financial loss. When combined with RBA-enforced restrictions on what payment providers can charge for interchange fees, small fintech companies face a significant cost barrier to increased investment in Australia and delivering technological advances.[30]

4.32 AirWallex recommended reconsideration of the interchange fee ceiling to balance against the limited number of suppliers. For example, in Singapore and Hong Kong, interchange fees have a tiered system.[31]

Streaming video on demand

4.33 Screen Producers Australia (SPA) identified detrimental business practices applied in commercial commissioning contracts by global streaming video on demand (SVOD) platforms such as Netflix, Amazon Prime, Disney+ and Paramount+. SVODs are highly successful global technology businesses with rapidly increasing revenues and audiences, and which are increasingly replacing more traditional platforms of free to air TV, cinema and DVD as the predominant way Australians seek screen entertainment.[32]

4.34 SPA stated the rise in streamers has changed the bargaining dynamics between Australian content producers and streaming businesses, allowing them to impose unfair terms:

> With negotiating power largely in the hands of streaming services, Australian producers and creative contributors are increasingly expected to sign away a full suite of proprietary rights over a longer – sometimes indefinite time period. The result of this is the accelerating loss of Australian

28 Airwallex, *Submission 67*, [p. 4].

29 Airwallex, *Submission 67*, [pp. 1–2].

30 Airwallex, *Submission 67*, [p. 2].

31 Airwallex, *Submission 67*, [p. 5].

32 Screen Producers Australia (SPA), *Submission 15*, p. 2.

intellectual property and business autonomy for Australian screen producers.[33]

4.35 SPA considered the circumstances that led to the development of the News Media and Digital Platforms Mandatory Bargaining Code (NMBC) are nearly identical to the bargaining imbalances for Australian screen producers and called for enhanced contract protections in the screen industry.[34]

4.36 Internationally, France, the UK and Canada have implemented regulatory interventions to address the market imbalance faced by independent screen producers.[35] Their approaches range from a focus on collective bargaining rights for independent producers, investment requirements in cultural and linguistic content, and intellectual property rights arrangements.[36]

News Media

4.37 The NMBC came into effect on 3 March 2021.[37] The NMBC was conceived to address the bargaining imbalance between local news organisations and digital platforms using local news content on their services.[38] The mandatory code incentivised digital platforms to reach commercial deals with Australian news organisations for the inclusion of news media on platforms.

4.38 The Minister may designate a platform under the NMBC, initiating a mandatory process for negotiation and arbitration. When making a designation, the Minister must consider whether a platform's agreements have made a 'significant contribution to the sustainability of the Australian news industry'.[39] To date, no digital platform has been designated under the NMBC.[40]

4.39 However, Google and Meta have struck over 30 commercial agreements with Australian news businesses. Treasury considered these unlikely to have been made without the incentive of the NMBC.[41]

---

33 SPA, *Submission 15*, p. 2.

34 SPA, *Submission 15*, p. 5.

35 SPA, *Submission 15*, p. 7.

36 SPA, *Submission 15*, p. 7.

37 *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021*.

38 Special Broadcasting Service (SBS), *Submission 3*, p. 1.

39 *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021*, s. 52E.

40 Australian Communications and Media Authority, *News media bargaining code*, 18 May 2022, www.acma.gov.au/news-media-bargaining-code (accessed 23 June 2023).

41 The Treasury, *News Media and Digital Platforms Mandatory Bargaining Code: The Code's first year of operation*, November 2022, p. 1.

4.40 Although the NMBC has been positively received overall, some submitters suggested there is a need for reform.[42] The Special Broadcasting Service Corporation (SBS) stated the NMBC is a 'key support to public interest journalism, [but] it has not fully achieved its intended outcomes and there remains opacity about its effectiveness.'[43]

4.41 Submitters argued the failure to designate any platforms to date weakened the NMBC as there is not sufficient incentive for large platforms to negotiate.[44] SBS suggested Meta has not entered meaningful negotiations with SBS.[45] Commercial Radio & Audio (CRA) commented:

> 90% of commercial radio networks have been unable to strike a deal with Google.
>
> 95% of commercial radio networks have been unable to strike a deal with Meta.[46]

4.42 Despite the frustrations of some media organisations, Treasury argued the NMBC is fulfilling its purpose:

> … the objective of the [NMBC] is to address bargaining power imbalances so as to ensure news businesses receive fair remuneration from digital platforms for the value their content generates. It is not designed to redistribute resources across the news sector or to guarantee that all news businesses receive funding. Other policy and funding tools are available to achieve these objectives.[47]

4.43 CRA recommended a prominence regime to ensure Australian radio can compete with Big Tech:

> The prominence regime applicable to commercial radio must ensure free, easy and universal access to Australian free to air commercial radio stations on car entertainment systems, as well as through smart speakers and other connected devices that are capable of delivering radio. To maintain the current diversity and accessibility of radio content it is vital that any prominence regime applies equally to AM, FM and DAB radio.[48]

Reform to unfair contract terms

4.44 The Australian Competition and Consumer Commission (ACCC) proposed strengthening of contract terms to create a more even bargaining relationship

---

42 See, for example, SBS, *Submission 3,* p. 4; Commercial Radio & Audio (CRA), *Submission 43,* p. 3.

43 SBS, *Submission 3*, p. 2.

44 See, for example, SBS, *Submission 3,* p. 6; CRA, *Submission 43,* p. 5.

45 SBS, *Submission 3,* p. 6.

46 CRA, *Submission 43,* p. 3.

47 The Treasury, *News Media and Digital Platforms Mandatory Bargaining Code: The Code's first year of operation*, November 2022, p. 27.

48 CRA, *Submission 43,* p. 7.

between Big Tech and consumers.[49] This was supported by the Centre for AI and Digital Ethics.[50]

4.45 Free TV recommended a code which requires designated entities to offer fair terms and conditions of service that:

- restrict the ability of designated entities to charge inflated prices;
- impose positive obligations to provide fair and non-discriminatory terms of access to key services and platforms, supported by an audit obligation;
- prohibit terms of service that require acceptance of data collection by the platforms in the provision of services (such as Google's ad serving, or Meta's social sharing tools);
- address the restrictions on how publishers can seek to monetise their content, including by prohibiting restrictive terms relating to the placement and pricing of advertising and the sharing of their data with the digital platform …[51]

Unfair trading practices

4.46 Many submitters advised the committee that the current regulatory framework lacks adequate legal protections from unfair trading practices.[52] Unfair trading practices may create consumer harms and an unfair playing field for small businesses and can discourage small businesses from competing in markets.

4.47 In relation to potential consumer harms, the Consumer Policy Research Centre (CPRC) commented:

> Unlike other countries that have prohibitions on unfair practices, several business practices that lead to unfair consumer outcomes are currently not illegal in Australia. Examples include business models that thrive on high-pressure sales of low value products, that fail to provide accessible and meaningful support to their customers and are predicated on opaque business processes that undermine consumer autonomy. Often these unfair business practices target those consumers specifically experiencing vulnerability or disadvantage.[53]

4.48 The ACCC identified several harms that could be considered unfair trading practices but are unlikely to be covered by the Australian Consumer Law. These included:

---

49 Australian Competition and Consumer Commission (ACCC), *Submission 8*, p. 5.

50 Centre for AI and Digital Ethics, *Submission 23*, p. 13.

51 Free TV Australia, *Submission 17*, p. 21.

52 See, for example, Consumer Policy Research Centre (CPRC), *Submission 60*, pp. 6–7; Australian Competition and Consumer Commission (ACCC), *Submission 8*, p; Reset Australia, *Submission 74*, p. 14.

53 Consumer Policy Research Centre (CPRC), *Submission 60*, pp. 6–7.

- adopting business practices to dissuade a consumer from exercising their contractual or other legal rights;
- inducing consent or agreement by very long contracts, providing insufficient time to consider contracts or all-or-nothing 'clickwrap' consents;
- engaging in harmful and excessive tracking, collection and use of data; and
- using dark patterns and other interface design strategies (such as prominence and framing) which impede choice and harm consumers.[54]

Dark patterns

4.49 Submissions raised concerns about 'dark pattern' use, a practice which refers to a user interface which has been designed to take advantage of how users habitually use platforms thereby tricking them into doing things they didn't intend to. Dark patterns may confuse users into buying or signing up to something by accident, spending more money, or sharing more information than intended.

4.50 The CPRC stated 83 per cent of Australians have experienced negative consequences because of dark patterns. Manipulative online designs cost Australians money, lead to a loss of control over their personal information and impact their wellbeing.[55]

4.51 Australian research found that young people are especially vulnerable to dark patterns.[56] Reset Australia explained the prevalence of dark patterns employed in apps popular with young people to confuse users and obtain data:

> An analysis of the privacy policies and practices of 10 apps popular with Australian young people noted that eight of them deployed dark patterns, which actively attempted to "trick" young people into agreeing to sharing more personal data than is necessary. Dark patterns are frequently deployed in children's apps too. For example, kids games often ask children to share their location or phone books, or encourage them to "share their top score," which requires linking the app to other accounts or sharing it with contacts. It is not always explicitly clear that this will allow additional data collection and transfer. This active obfuscation is often exacerbated by potentially misleading statements by digital platforms … when questioned about behavioural advertising and children across 2021 and 2022, Meta issued a range of opaque potentially misleading replies.[57]

4.52 The ACCC raised issue with online service providers making it difficult for consumers to cancel subscriptions after free trials, with the consequence that

---

54 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, pp. 64–65.

55 CPRC, *Submission 60*, p. 2.

56 Alannah & Madeline Foundation, *Submission 41*, p. 6.

57 Reset Australia, *Submission 74*, p. 14.

many subscriptions roll-over to paid subscriptions despite consumers no longer using or wanting them.[58]

4.53 For example, Amazon is currently facing court action against the United States of America (US) Federal Trade Commission (FTC) for enrolling consumers into its paid Amazon Prime subscription without consent and then making it difficult to cancel. The FTC maintains this behaviour is manipulative, coercive or deceptive.[59]

4.54 In response to these concerns, Mr Michael Cooley, Director, Public Policy Australia, Amazon Australia, said the cancellation process had since been updated and is 'two clicks … simple, transparent and clear'.[60]

Unfair trading practices prohibition

4.55 The ACCC recommended an economy-wide unfair trading practices prohibition be implemented to protect consumers and small businesses.[61] This recommendation was supported by multiple submissions.[62]

4.56 The CPRC outlined potential harms and argued:

> Failure to protect consumers will mean that Australians will continue to be exposed to business models that manipulate consumer consent, use opaque business processes that undermine consumer autonomy or exploit consumer vulnerabilities. Australian consumers deserve better.[63]

4.57 The Centre for AI and Digital Ethics supported the introduction of a prohibition on unfair trading to better address 'systematic undesirable business practices' than currently covered by the *Competition and Consumer Act 2010* (CCA):[64]

> … we support substantive measures to require platforms to take responsibility for their dealings with consumers, and promote fair and honest practices. These include robust enforcement of the unfair contract terms provisions in the ACL [Australian Consumer Law] as applied to the

---

58 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 64.

59 ABC, *Amazon accused of duping millions of customers over Prime sign-ups by Federal Trade Commission*, 22 June 2023, www.abc.net.au/news/2023-06-22/amazon-sued-for-tricking-prime-customers/102508902 (accessed October 18 2023).

60 *Proof Committee Hansard*, 22 August 2023, p. 3.

61 ACCC, *Submission 8*, p. 5.

62 See, for example, CHOICE, *Submission 54*, p. 5; CPRC, *Submission 60*, p. 1; Centre for AI and Digital Ethics, *Submission 23*, [p. 3].

63 CPRC, *Submission 60*, p. 9.

64 Centre for AI and Digital Ethics, *Submission 23*, [p. 13].

> context of platform services. In particular, we support a prohibition on unfair trading to act as a 'safety net' catching other forms of unfair conduct.[65]

4.58 CHOICE also voiced its support for unfair trading laws and noted they work effectively in other jurisdictions including the United States, European Union (EU), UK and Singapore:

> Consumers still lack legal protections from unfair trade practices… This gap allows businesses to operate unfair business models with limited legal consequences. The ACCC's Digital Platforms Inquiry identified this as an important policy solution which will address consumer harm on digital platforms.[66]

4.59 The CPRC outlined several factors to consider when drafting an unfair trading prohibition, based on its analysis of international practices. It should:

- be drafted as a principles-based law but with specific guidance or an evolving a blacklist of unfair practices to give clarity to both regulators and businesses
- allow regulators to investigate and proactively enforce the law before widespread harm takes place
- have provisions in place for the law to evolve over time to address new and emerging unfair practices
- hold businesses accountable through penalties and enforcement action that effectively deter unfair business practices
- offer meaningful redress to consumers impacted by unfair practices
- quickly stop practices found to be unfair overseas from making their way to Australia
- expand the scope of consumer harm to include the impact on mental health in addition to financial and reputational loss.[67]

4.60 The government has acknowledged that unfair trading practices are not covered in existing provisions of Australia's consumer laws. Federal, state and territory consumer ministers agreed the matter warranted further investigation, so the Department of Treasury released a Regulation Impact Statement for public consultation, concluding in November 2023. Responses to that consultation are currently being considered and a Decision Regulatory Impact Statement will be produced during 2024 to discuss the results of the consultation process and identify a preferred regulatory response.[68]

---

65 Centre for AI and Digital Ethics and Melbourne Law School, *Submission to ACCC September 2022 interim report*, pp. 3–4.

66 CHOICE, *Submission 54*, p. 5.

67 CPRC, *Submission 60*, p. 7.

68 Treasury, *Unfair trading practices - Consultation Regulation Impact Statement*, https://treasury.gov.au/consultation/c2023-430458 (accessed 8 November 2023).

Dispute resolution processes and escalation

4.61 With the accelerated digitisation of services, particularly during the COVID-19 pandemic, individuals and businesses are increasingly reliant on digital platforms.

4.62 The ACCC noted:

> Digital platforms have fundamentally changed the way in which Australian small businesses connect and sell to their customers, and for many they are their only channel to their marketplace.[69]

4.63 As in any business relationship, problems and complaints can arise. Digital platforms most commonly receive complaints regarding decisions to block or terminate user accounts, changes to platform services as well as fake reviews, scams and harmful apps.[70]

4.64 While small businesses and consumers are protected under the Australian Consumer Law (ACL) including consumer redress options, enforcing these rights is challenging in the digital economy.

4.65 Dispute resolution can advance through four stages:

(1) internal resolution with the user utilising self-help material, FAQs or community forums;
(2) internal resolution using platform-led processes through webforms or in-situ reporting;
(3) external dispute resolution; and
(4) judicial resolution.[71]

Inadequate internal dispute resolution processes

4.66 Several submissions suggested the internal complaints handling mechanisms of many international digital platforms are difficult to access and are, in many cases, inadequate for small businesses and individuals to reach a satisfactory outcome when issues such as access difficulties or security breaches occur.[72]

4.67 A 2022 report commissioned by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) as part of an External Dispute Resolution Scheme Feasibility Study noted:

---

69 The Hon Bruce Billson, Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *Proof Committee Hansard*, 26 July 2023, p. 27.

70 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 88.

71 Accenture, 'Mapping dispute resolution on digital platforms', p. 21 in *EDR Feasibility Study Final Report*, Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), FOI 23-037, 14 November 2022.

72 See, for example, Australian Communications Consumer Action Network (ACCAN), *Submission 20*, p. 1; ASBFEO, *Submission 39*; ACCC, *Submission 8*, p. 4; NSW Small Business Commissioner, *Submission 6*, [p. 1]; CPRC, *Submission 60*, p. 5.

> Platforms have put in place a range of sophisticated capabilities to prevent and minimise approximately 75 million potential problems each year in Australia before they escalate. Machine learning, AI and specialist review teams work proactively to block harmful content, eliminate bad actors and scams, demote or remove fake reviews and enforce guidelines.
>
> These capabilities enable platforms to prevent 95% of potential problems before they were experienced by the user, or result in a complaint or dispute.[73]

4.68 Despite these capabilities, around 880 000 disputes arise each year that cannot be resolved within existing systems. Misdirection and lack of transparency around why content has been blocked or accounts suspended were key challenges for businesses and users. Additionally, 16 per cent of issues on digital platforms remain unresolved.[74]

4.69 The ACCC succinctly outlined the problem:

> Consumers and small businesses seeking to enforce their existing rights against digital platforms under the ACL face obstacles such as unclear and costly dispute resolution processes, as well as informational and power disadvantages.[75]

4.70 For many small and family businesses operating primarily on social media and digital platforms, restoring accounts that have been shut down after being hacked is particularly problematic as businesses are excluded from accessing the platform's internal complaints mechanisms without an active account.[76]

4.71 Small businesses and individuals also wear much of the costs of the resolution process.[77] DITRDCA's study stated:

> Given the scale and scope of interactions online, the economic cost of issues, complaints and disputes in Australia each year is $4.2 billion. Of which the majority ($3.7 billion) is the cost to users and businesses. A significant driver of this cost is the time and effort associated with misdirection and difficulties in resolution when an issue or complaint escalates to a dispute.[78]

4.72 The ASBFEO emphasised the need for improved processes:

---

73 Accenture, 'Mapping dispute resolution on digital platforms', p. 2 in *EDR Feasibility Study Final Report*, FOI 23-037, 14 November 2022.

74 Accenture, 'Mapping dispute resolution on digital platforms', p. 2 in *EDR Feasibility Study Final Report*, FOI 23-037, 14 November 2022.

75 ACCC, *Submission 8*, p. 4.

76 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 27.

77 Accenture, 'Mapping dispute resolution on digital platforms', p. 3 in *EDR Feasibility Study Final Report*, FOI 23-037, 14 November 2022.

78 Accenture, 'Mapping dispute resolution on digital platforms', p. 3 in *EDR Feasibility Study Final Report*, FOI 23-037, 14 November 2022.

> Implementing adequate internal dispute resolution processes and dedicated contacts would enable small businesses to have their dispute handled efficiently and resume operating their businesses sooner.[79]

4.73 The Australian Communications Consumer Action Network (ACCAN) found that almost three in four Australians agree that it needs to be easier to make a complaint and to get complaints resolved when interacting with digital platforms.[80]

Improving internal processes

4.74 The ACCC's 2019 *Digital Platforms Inquiry Final Report* recommended the Australian Communications Media Authority develop minimum internal dispute resolution standards to apply to digital platforms.[81]

4.75 The ACCC's 2022 *Digital Platform Services Inquiry interim report No. 5 – Regulatory reform* (ACCC Regulatory Reform Report) also outlined the need for:

> Mandatory internal dispute resolution standards that ensure accessibility, timeliness, accountability, the ability to escalate to a human representative and transparency.[82]

4.76 The ASBFEO advocated for a collaborative model with the ASBFEO working alongside digital platforms to improve their internal processes with a focus on preventative measures and information tools.[83] In particular, the ASBFEO noted digital platforms require functional support tools, internal escalation steps and real person contact points.[84]

International examples

4.77 Internationally, the EU's Digital Services Act (DSA) enables users to defend themselves against 'unjust restrictions' by setting out rules for internal complaints handling systems and out of court dispute mechanisms.[85]

4.78 Japan has placed co-regulatory obligations on specified digital platforms to create systems and procedures for complaints and dispute handling.[86]

---

79 ASBFEO, *Submission 39*, [p. 2].

80 ACCAN, *Submission 20*, p. 1.

81 ACCC, *Digital Platforms Inquiry Final Report*, June 2019, p. 37.

82 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 88.

83 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 28.

84 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, pp. 27–29.

85 Gesellschaft Für Freiheitsrechte e.V, *Submission 25*, [p. 3].

86 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 91.

External escalation

4.79 Where internal dispute resolution processes fail to reach a satisfactory outcome for users or businesses, disputes with digital platforms are often escalated to independent third parties, such as the ASBFEO, for assistance.

Current external resolution options

4.80 The ASBFEO currently assists with business-to-business dispute resolution, establishing connections with digital platforms, encouraging engagement, helping the parties to find a way forward and consider the type of resolution that may suit the parties. However, the committee heard that it is not appropriate for a government body to resolve every individual or small business dispute.[87]

4.81 The ASBFEO advised it has generally experienced constructive engagement with digital platforms when initiating contact on behalf of small and family businesses, including obtaining contact points within platforms to escalate disputes. However, the committee was advised that ASBFEO's experience is not always consistent or successful.[88]

4.82 While the ASBFEO plays a role currently providing some dispute resolution for small businesses it cannot make binding decision or order compensation. The committee was advised:

> … our legislation enables us to encourage their engagement and to suggest to them what a path forward to resolution might look like. In the absence of that, the only punitive action we can take is to perhaps provide a notification to other businesses that, in our dealings with this business, we haven't had satisfactory interactions, and people might want to think twice about doing so.[89]

4.83 The ASBFEO can also refer individual case matters to other agencies on critical matters (system wide or strategic matters) for their consideration.[90]

4.84 The ACCC also noted the limited powers of existing dispute resolution:

> In the ACCC's view, existing bodies lack the resources to deal with the range, volume and complexity of disputes occurring on digital platforms, and may not be capable of delivering sufficient remedies.[91]

---

87 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, pp. 27–28.

88 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 27.

89 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 29.

90 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 28.

91 ACCC, *Submission 8*, p. 7.

Reform to dispute resolution

4.85 Evidence to the committee supported the need for clearer complaints handing processes and proposed a range of dispute resolution and escalation options for improving consumer and competition outcomes.[92]

4.86 The ASBFEO proposed it could hold an expanded role as an external dispute resolution service, providing a formalised external escalation option for small business where internal resolution with platforms have been exhausted. However, the ASBFEO suggested a further escalation point to a regulator that is less 'light handed' than the ASBFEO and which holds determinative powers could also be considered.[93]

Consumer Voice

4.87 The ACCAN proposed a consumer voice be funded 'to advocate for consumers on digital platforms policy matters.' The consumer voice would engage with future policy and regulatory consultation processes around increasing digital platform issues facing consumers.[94]

Super complaints mechanism

4.88 One option the committee received support for was a 'super complaint' mechanism. Such a mechanism was seen by the ASBFEO as a way for credible dispute resolution agencies (such as the ASBFEO) to escalate and refer disputes between small business and digital platforms direct to the ACCC for guaranteed investigation.[95]

4.89 The proposed super complaints mechanism is similar to provisions for trusted flaggers in the EU's DSA[96] or provisions in the UK's Online Safety Act 2023 (see Box 4.1 for details).

4.90 The 2023-24 Budget included establishing the first phase of a 'super complaints' mechanism within the ACCC that 'will enable consumer and small business advocacy groups to submit a complaint to the ACCC where they have strong evidence of systemic market issues under the consumer law'.[97] The new

---

92 See, for example, CPRC, *Submission 60*, p. 1; The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 28.

93 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 28.

94 ACCAN, *Submission 20*, p. 2.

95 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 28.

96 DITRDCA, 'International Approaches to Regulating Dispute Resolution Processes for Digital Platforms – External dispute resolution pilot scheme feasibility study: report 1', July 2021, p. 27 in *EDR Feasibility Study Final Report*, FOI 23-037, 14 November 2022.

97 The Hon Andrew Leigh MP, Assistant Minister for Competition, Charities and Treasury, '*Empowering consumers and small businesses through a designated complaints function*,' *Media release*, 12 May 2023; Commonwealth of Australia, *Budget Measures: Budget Paper No. 2 2023-24*, p. 214.

designated complaint function will commence in July 2024.[98] It is unclear whether the new function will encompass digital platform related complaints made by the ASBFEO or similar bodies.

Box 4.1 UK Super Complaints Mechanism

The UK's Online Safety Act 2023 also includes provisions for 'super-complaints' for eligible entities to alert the regulator to their concerns about systemic issues. The UK government noted:

> Super-complaints will need to focus on the systems and processes that companies have in place, rather than any specific content issues. They will also need to focus on issues occurring across multiple in-scope services, as organisations can raise concerns about a single company's conduct through Ofcom's [Office of Communications] enforcement complaints processes.[99]

The UK regulator will accept super-complaints where provider services or conduct appears to or presents a material risk of:

- causing significant harm to users or members of the public;
- significantly adversely affecting the rights to freedom of expression within the law of users or members of the public;
- causing significant unwarranted infringements of privacy; or
- otherwise having a significant adverse impact on users or members of the public.[100]

Ombudsman scheme

4.91 Another dispute resolution option proposed was the establishment of a digital platforms ombudsman to provide an independent complaints escalation mechanism for consumers and small businesses.[101]

4.92 The ACCAN noted discussions have been ongoing for some time about the appropriate institutional arrangements, and urged the Government to make an in-principle decision by the end of 2023 on whether an ombudsman scheme will be established and which entity should provide the function. It advised:

> Consumers face significant harms on digital platforms in the form of social networking scams, mobile app scams and a lack of redress. It is essential that

98 Commonwealth of Australia, *Budget Measures: Budget Paper No. 2 2023-24*, p. 214.

99 UK Government, *Online Harms White Paper Government Response*, December 2020.

100 DITRDCA, 'International Approaches to Regulating Dispute Resolution Processes for Digital Platforms – External dispute resolution pilot scheme feasibility study: report 1', July 2021, p. 27, in *EDR Feasibility Study Final Report*, FOI 23-037, 14 November 2022.

101 See, for example, ACCAN, *Submission 20*, p. 2; CPRC, *Submission 60*, p. 5; Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, pp. 18–19.

> the consumer voice is strengthened through access to external dispute resolution and funded representation.[102]

4.93 The CPRC also supported the establishment of a digital platforms ombudsman, stating:

> There must be effective dispute resolution pathways to enable consumers to seek redress for when things go wrong in the online space. As consumers increase their engagement online, a Digital Ombudsman needs to be adequately resourced to meet benchmarks for industry-based customer dispute resolution to ensure consumers can effectively resolve any disagreements that will arise.[103]

4.94 In addition to being a central point for independent dispute resolution, an ombudsman could be well placed to identify systemic consumer harms on digital platforms.[104]

4.95 A digital platforms ombudsman was recommended by the ACCC in its 2019 Digital Platforms Inquiry final report. The ACCC noted an ombudsman would require powers to compel information, make binding decisions, order compensation as appropriate, and order the take down of scam content.[105]

4.96 In 2019, the government of the day committed to developing a pilot scheme to be assessed throughout 2020.[106] It is unclear how far this proposal progressed.

4.97 The ACCC reiterated its recommendation for an ombudsman scheme in its 2022 Regulatory Reform Report, detailing the benefits, scope and design considerations of such a scheme.[107] It noted an independent ombudsman scheme was:

> … important for ensuring the effectiveness of internal dispute resolution measures. In the ACCC's view, existing bodies lack the resources to deal with the range, volume and complexity of disputes occurring on digital platforms, and may not be capable of delivering sufficient remedies.[108]

---

102 ACCAN, *Submission 20*, p. 1.

103 CPRC, *Submission 60*, p. 5.

104 ACCAN, *Submission 20*, p. 2.

105 ACCC, *Digital Platforms Inquiry Final Report*, June 2019, p. 37.

106 Australian Government, *Regulating in the digital age, Government Response and Implementation roadmap for the Digital Platforms Inquiry*, 2019, p. 7.

107 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, pp. 98–104.

108 ACCC, *Submission 8*, p. 7.

4.98 While supportive of the notion of a digital platforms ombudsman, Meta advised the role and powers of any new agency or body needed to be 'flesh[ed] out'.[109] Meta highlighted that it is currently referred complaints from a range of government bodies including Scamwatch, the eSafety Commissioner, Human Rights Commission, Privacy Commissioner and the ASBFEO. While a single point of contact may be more streamlined, Meta highlighted the complaint issues being handled are very diverse.[110]

Judicial resolution

4.99 Once other channels for resolution are exhausted, judicial resolution can be the final escalation point for business disputes, including those involving digital platforms.

4.100 Where the regulator is unlikely to prosecute a case, there is a need for small business access to justice that is right-sized, affordable and timely.[111]

4.101 The ASBFEO has previously highlighted the ACCC's priority to pursue cases where broader systemic issues are apparent. Due to limited capacity, the ACCC rarely engages in individual small business disputes:

> … many small businesses facing anti-competitive conduct are left to either accept this conduct or defend their own economic interests.
>
> Further, the ACCC's focus on systemic issues results in any resolution and applied penalty occurring significantly after the anti-competitive conduct is experienced by the individual small business. This delayed action and any resulting penalties applied does little to rectify the relevant damage experienced by the small business.[112]

4.102 The ACCC noted in its Regulatory Reform Report the limitation of judicial remedies in certain cases:

> … where disputes are largely low in individual value but high in volume, and involve multiple jurisdictions, use of the State and Courts as an enforcement mechanism is not practicable or cost effective.[113]

4.103 The ASBFEO advised that a judicial approach operating similarly to state level small claims tribunals would assist small businesses to escalate more serious matters which may not be picked up by a regulator. However, it noted the constraints of chapter III of the Constitution require a federal determinative forum to be a court. In light of this, the ASBFEO proposed a Federal Small

---

109 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansar*d, 22 August 2023, pp. 19–20.

110 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 20.

111 The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 31.

112 ASBFEO, Submission to Treasury's consultation on the *Treasury Laws Amendment (Competition and Consumer Reforms No.1) Bill 2022*, [p. 1].

113 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 88.

Business and Codes List be established in the Federal Circuit Court of Australia.[114] It noted such an arrangement 'would empower small businesses to defend their own economic interests, reducing the need for government intervention.' The ASBFEO stated:

> … the introduction of the list would provide a low-cost alternative for small businesses to utilise should they seek a timely, cost-effective judgement, or where other dispute resolution options have failed.[115]

[114] The Hon Bruce Billson, ASBFEO, *Proof Committee Hansard*, 26 July 2023, p. 30.

[115] ASBFEO, *Submission 39*, [p. 2].

Chapter 5
Data

Overview

5.1 This chapter examines privacy and competition concerns in relation to data collection practices of Big Tech and proposed solutions to address these concerns.

Data collection and collation

5.2 Data in this context refers to information about consumers. Data can include sensitive information such as a consumer's full name, address, phone numbers, driver's license details, income, occupation and educational background. It may be collected many ways including online through use of websites or in-person by using store loyalty cards.

5.3 Data collation, aggregation or linking refers to how data is sorted within a database. Data collected from multiple sources, such as browsing activity, signing up for a service, public records and financial records, may be collated to build detailed profiles of users.

5.4 The Human Rights Law Centre (HRLC) explained profiling:

> Profiling refers to the platforms' practice of building a 'profile' of a person's personal attributes and interests through tracking their behaviour over time, which can then be used for targeted advertising and personalised recommender systems.[1]

5.5 These profiles are extremely valuable to companies, who use them to target ads, sell products and influence user behaviour.[2] The potential harms to consumers from data collection and collation are discussed below. The particular harms and safety concerns arising from the collection and collation of children's data are considered in Chapter 8: Online safety.

Concerns with data collection

5.6 Submissions raised concerns that consumer data may be used to manipulate user behaviour and/or put consumers at risk of price discrimination.[3]

---

1 Human Rights Law Centre (HRLC), *Submission 50*, p. 12.

2 See, for example, Australian Competition and Consumer Commission (ACCC), *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 31; Free TV Australia, *Submission 17*, p. 9; Commonwealth Bank of Australia, *Submission 71*, p. 4; Mr Joshua Zubak, *Submission 27*, p. 1.

3 See, for example, CHOICE, *Submission 54*, p. 4; Consumer Policy Research Centre, *Submission 60*, p. 1; Mr Joshua Zubak, *Submission 27*, p. 1.

5.7 The Foundation for Alcohol Research and Education explained how profiles made through data collection are used to tailor marketing to influence consumer purchases:

> By design, people who purchase harmful and addictive products the most are also targeted by digital marketing models the most. Extensive data collection allows digital platforms to develop detailed psychometric profiles that are combined with detailed accounts of people's browsing behaviour. These insights are used to tailor marketing activities, including content and messaging, towards an individual's specific susceptibilities. In the case of alcohol marketing, this ability to prey on people's susceptibilities is particularly harmful because it can disproportionately target people experiencing alcohol dependence.[4]

5.8 The Consumer Policy Research Centre (CPRC) identified that digital platforms may use and link data to unfairly exclude consumers from accessing certain products and services or target consumers to expose their vulnerabilities for commercially beneficial outcomes.[5] Profiles made through data aggregation:

> … effectively "score" their value – with a view to identifying and retaining profitable customers through advertisements (and avoiding those who are not profitable). A lack of transparency and accountability within such processes means it is difficult for consumers to see how their profile is produced; understand the impact it will have on them; or influence, appeal or correct assumptions based on wrong information. Profiles can also be used to set prices, leading to some groups of consumers paying more for the same service.[6]

5.9 CHOICE detailed its finding on the use of facial recognition technology by major Australian businesses, employed without informed consumer consent or with only inconspicuous disclosure. CHOICE noted the risks of this practice included data breaches involving biometric data, inaccurate assessments and potentially hardcoding biases and discrimination.[7]

Data brokers

5.10 Data collected by businesses is also used to create revenue by selling this data on to data brokers. Data brokers are organisations that collect and buy vast amounts of data to aggregate and on-sell to other companies. Aggregated data is bought and used for commercial purposes, such as creating targeted advertising.

---

4 Foundation for Alcohol Research and Education, *Submission 33*, p. 4.

5 Consumer Policy Research Centre, *Submission 60*, p. 2.

6 Consumer Policy Research Centre, *Submission 60*, p. 2.

7 CHOICE, *Submission 54*, p. 4.

5.11 Mr Rob James, Principal Consultant and Chief Executive Officer, Rob James Consulting Pty Ltd, explained that data brokerage is a $200 billion industry with significant power:

> … that industry has spent over $56 million lobbying the US government for regulation in its own favour. That's more than Facebook, Apple, Microsoft and Google combined have spent lobbying the US government. So it's a huge market sector, extremely valuable, and it does impact Australian citizens' data and the privacy of their information. The depth of the data that is held by these brokers is quite broad, and, if that data were to be breached, the malicious activity—what we've seen historically from hacks—could be quite significant to us.[8]

5.12 Digital Rights Watch described how digital platforms have changed from focusing on providing services to collecting data, creating privacy risks:

> This shift of focus away from the service or product itself and towards the commodification of data enables and encourages a data-gluttonous logic in which data is collected for the sake of it, rather than to meet a specific functional or practical necessity. In turn, this amplifies invasion of privacy, broadens the risks associated with compromised digital security, and, critically, creates a dynamic in which people are data subjects but never data agents. By and large, people generate an immense amount of data to the benefit of a handful of corporations, which is in turn used to fuel further profits by way of targeted advertising and the manipulation of attention, as something to be bought and sold in the data broker industry, or used to build more products divorced from the underlying wants and needs of the people from whom the data was extracted.[9]

5.13 The committee notes the next report in the Australian Competition and Consumer Commission's (ACCC) ongoing *Digital Platforms Services Inquiry* is considering the supply of data broker services in Australia.

Lack of user control

5.14 Many submissions were concerned that companies obtain data without active participation or even awareness of the people from whom data is being extracted.[10]

5.15 The Attorney-General's Department stated:

> Submitters [to the Privacy Act Review] noted that targeting has the potential to cause significant harm when individuals have limited awareness of why and how they are being targeted and no control over it, and where targeted content and advertising may be used to manipulate, discriminate, exclude and exploit individuals based on their vulnerabilities.[11]

---

8 *Proof Committee Hansard*, 26 July 2023, p. 34.

9 Digital Rights Watch, *Submission 68*, p. 11.

10 Mr Joshua Zubak, *Submission 27*, p. 1.

11 Attorney General's Department, *Submission 51*, p. 16.

5.16 The CPRC's research indicated:

> … consumers are uncomfortable with the amount of information collected about them and would prefer to have greater control over that data collection. Control is particularly lacking given that personal data can often be traded between firms deeply embedded in supply chains without a direct link to consumers or even the basic service they'd signed up for. In addition, it can be difficult for consumers to know where and how to remove their associated data from brokers' holdings.[12]

5.17 Professor Toby Walsh, Chief Scientist, AI Institute, University New South Wales, explained how data is collected even when consumers are offline:

> We need stronger privacy laws to protect what might be called our "analog privacy". Increasingly, our digital devices are collecting information about our non-digital selves. I can give many examples. Fitbit monitors your heart-beat. Your Android smart-watch tracks your every movement in the real world. AndMe collects information about your genotype. All of this is information about our "offline" analog selves rather than our online digital selves. With digital information, we can refuse cookies, connect with a VPN, or find other ways to hide our digital footprint. But analog information is much harder to hide. FitBit's term of service mean that FitBit own your heart-beat. AndMe claim a non-exclusive license to your genes. As most of these devices collecting analog information about us are not considered to be medical, such analog information is currently not treated with the care and sensitivity it deserves.[13]

5.18 The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression outlined that:

> The systematic collection of behavioural data and targeted advertising can violate the right to freedom of opinion; and the lack of transparency around platforms amplification of content online 'points towards an unacceptable level of intrusion into individuals' right to form their ideas free from manipulation and right to privacy'.[14]

Ineffective consent procedures

5.19 Submissions suggested that processes for user consent to collection of data are inadequate. Consent is typically bundled with the decision to use a particular product and may not be considered free and informed because users tend to not understand the quantity of their data that will be obtained or how it will be used.[15]

---

12 Consumer Policy Research Centre, *Submission 60*, pp. 2–3.

13 Professor Toby Walsh, *Submission 42*, [p. 3].

14 Human Rights Law Centre, *Submission 50*, p. 12. See also United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Disinformation and freedom of opinion and expression*, 13 April 2021, UN Doc A/HRC/47/25, pp. 14–15.

15 See, for example, Professor Jeannie Marie Paterson, Professor of Consumer Law, Director, Centre for AI and Digital Ethics, *Proof Committee Hansard*, 26 July 2023, p. 46; Mr Joshua Zubak,

5.20 The CPRC argued that consent processes need reform:

> Australia's privacy law still relies on notification and consent as the primary means of protecting consumers. By forcing consumers into a situation where they "decide once" about whether to share their data but bear the consequences potentially for the remainder of their life is not a fair trade. This starkly contrasts with the knowledge and capability of firms to understand the value and potential use of data.[16]

5.21 Submissions highlighted terms and conditions as being ineffective at helping consumers understand what data is being collected.[17]

5.22 The Office of the Australian Information Commissioner's (OAIC) *Australian Community Attitudes to Privacy Survey 2020* found that 69 per cent of individuals do not read privacy policies attached to any internet site, largely due to their length and complexity. The OAIC commented:

> Even where individuals do read privacy policies and APP 5 notices, they may feel resigned to consent to the use of their information to access online services because they do not feel there is an alternative. As digital products and services become more entrenched in individuals' lives as the way in which we work, study and engage socially it is increasingly difficult to avoid pervasive tracking and data handling practices that do not align with their preferences.[18]

5.23 The Australian Media Literacy Alliance (AMLA) stated:

> Currently only a quarter (26%) of adults are confident they understand the terms and conditions of social media platforms, including what data is being collected, and by implication how that is being used. The increased proliferation of AI generated content, where it is unclear what underlying data is being drawn upon and how answers are being created, only increases these challenges.[19]

5.24 The committee noted that under the Australian Privacy Principles (APPs), APP entities[20] are only to collect personal information about an individual directly from that individual. Data collation or profiling using information beyond that

---

Submission 27, p. 3; Mr Tom Leuner, Executive General Manager, Mergers, Exemptions and Digital, ACCC, *Proof Committee Hansard*, 22 August 2023, p. 34.

16 Consumer Policy Research Centre, *Submission 60*, p. 6.

17 See, for example, Consumer Policy Research Centre, *Submission 60*, pp. 2–3; Australian Media Literacy Alliance (AMLA), *Submission 55*, [p. 3].

18 Office of the Information Commissioner (OAIC), *Submission 61*, p. 3.

19 AMLA, *Submission 55*, [p. 3].

20 The OAIC states APP entities are 'Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million have responsibilities under the Privacy Act, subject to some exceptions'. See OAIC, *Rights and responsibilities*, www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities (accessed 15 November 2023).

provided directly from a user is illegal if a company can 'reasonably and practicably' request it from the user themselves.[21]

5.25 Examples of times it may be unreasonable or impractical include 'collection by a law enforcement agency of personal information about an individual who is under investigation', where direct collection may jeopardise an investigation; or to obtain updated address details for an individual where delivery of legal or other official documents is necessary.[22] Organisational privacy policy terms discussing collection from third parties or disclosure of data to 'trusted partners' do not create an exception to the direct collection rule. However, the provision is rarely enforced.[23]

Privacy and security concerns

5.26 Submissions asserted that privacy is a human right which needs to be protected.[24]

5.27 With the widespread collection and processing of personal data by digital platforms, individual privacy concerns are growing.[25] Submitters were concerned about the use of their data for profiling and manipulation, as well as risks from potential data breaches, such as identity theft or online harassment.[26]

The Privacy Act

5.28 The *Privacy Act 1988* (Privacy Act) contains a set of principles that outline how organisations are permitted to handle personal information. This includes obligations in relation to the collection, use and disclosure of personal information, adequately protecting personal information and providing transparency in relation to this information handling.

---

21 Katharine Kemp, 'This law makes it illegal for companies to collect third-party data to profile you', *The Conversation*, 21 September 2022.

22 OAIC, *Chapter 3: APP 3 Collection of solicited personal information*, 22 July 2019, www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information (accessed 15 November 2023).

23 Katharine Kemp, 'This law makes it illegal for companies to collect third-party data to profile you', *The Conversation*, 21 September 2022.

24 See, for example, Digital Rights Watch, *Submission 68*, p. 4; Apple, *Submission 70*, p. 1.

25 Vault Cloud, *Submission 38*, [p. 3].

26 See, for example, CHOICE, *Submission 54*, p. 4; Consumer Policy Research Centre, *Submission 60*, p. 1; Mr Joshua Zubak, *Submission 27*, p 1.

5.29 The OAIC highlighted '[t]he flexible principles-based nature of the Privacy Act also means it is adaptable to changing technology, and able to complement other legislation or regulatory frameworks that deal with related issues'.[27]

The Privacy Act Review

5.30 The Privacy Act Review commenced in October 2020, following the ACCC *2019 Digital Platforms Final Report* that recommended broad reform of Australia's privacy framework. The review aimed to modernise the Privacy Act to keep up with the increased volume and granularity of personal data being collected by companies including digital platforms.

5.31 The *Privacy Act Review Report 2022* makes 116 proposals for reform, which are designed to better align Australia's laws with global standards and improve protection of Australians' privacy. The proposals focus on three categories:

- Information protections: these proposals include recognising the public interest to society of protecting individuals' privacy, regulating 'targeting' of individuals based on information which relates to them but that may not uniquely identify them and enabling privacy codes to be made by the Information Commissioner in certain circumstances.
- Privacy protections: these proposals include strengthening privacy protections for children, improving individuals' control over their personal information, including through a right to seek erasure of personal information, and giving individuals more transparency and control over direct marketing.
- Enforcement: these proposals include equipping the OAIC with more options to enforce privacy breaches, enhancing the OAIC's ability to proactively identify and address privacy breaches, and providing new pathways for individuals to seek redress in the courts for privacy breaches, including through a new tort for serious invasions of privacy.[28]

Security concerns

5.32 As companies increase the amount of data they hold, consumer concerns about privacy and cyber security are growing.

5.33 Vault Cloud commented on cyber security as an increasing concern:

> The lack of transparency and control over how personal data is being used is a critical concern that needs to be addressed … The increasing reliance on IT has created new security challenges, such as cyberattacks and data breaches. These threats can cause significant damage to individuals, businesses, and even entire countries. There is a need for stronger

---

[27] OAIC, *Submission 61*, p. 2.

[28] Attorney General's Department, *Privacy Act Review Report*, 16 February 2023, www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report (accessed 6 November 2023).

> regulations that can protect against these threats and ensure that appropriate cybersecurity measures are in place.[29]

5.34 CHOICE discussed how the increased collection of data has led to privacy breaches:

> Data breaches can have devastating impacts on Australian consumers, exposing people to financial loss, emotional distress and loss of trust in private markets. In light of recent major data breaches affecting millions of people, the case for strengthening Australia's privacy laws and regulatory enforcement powers has never been clearer. Businesses profit from monetising consumer data – and not just technology businesses. They often collect unnecessary amounts of data to exploit and on-sell to data brokers. Recent data breaches in Australia were a result of the vast amount of data collected by big and small businesses in recent years, as well as outdated regulations governing data collection.[30]

Australian government data and use of cloud services

5.35 The Department of Home Affairs noted '[t]he rising use of online and digital services by Australians requires increased efforts to manage government systems and data holdings, effectively and securely'. The Hosting Certification Framework (HCF) is one policy designed to ensure data is 'hosted with the appropriate level of privacy, sovereignty, and security controls'.[31]

5.36 Submitters commented on current controls in place to safeguard Australian Government data, including the HCF, in addition to concerns around data sovereignty and localisation.

Hosting Certification Framework

5.37 Certification under HCF is required for businesses wanting to enter cloud contracts with government. Under the HCF, hosting providers must demonstrate that data will only move between customers and geo-locked strategic certified data centre facilities and will not leave Australia at any point.[32]

5.38 The Digital Transformation Agency (DTA) stated:

> The DTA has found that global service providers, with workforces and facilities located outside of Australia, have had challenges in complying with some of the control objectives under the HCF … An issue is ensuring personnel that would have unescorted physical or logical access to sensitive or classified government data, obtain Australian Government Security Vetting Agency (AGSVA) security clearances. There are also requirements around executive control and influence of strategic decisions that have been

---

29 Vault Cloud, *Submission 38*, [p. 3].

30 CHOICE, *Submission 54*, p. 3.

31 Department of Home Affairs, *Safeguarding Australian Government data*, www.hostingcertification.gov.au (accessed 7 November 2023).

32 Digital Transformation Agency, *Submission 7*, p. 3.

> challenging for global providers. The DTA is addressing these challenges in partnership with the relevant industry and government parties by applying interim controls to address the associated risks until the HCF requirements can be met.[33]

5.39 The Tech Council of Australia (TCA) recommended examining the impact of the HCF. It argued the framework may duplicate existing requirements, which may be covered by other standards, such as the International Financial Reporting Standards or the European Union (EU) General Data Protection Directive (GDPR). This disproportionately disadvantages small businesses when competing with larger companies that may be better placed to respond to regulatory uncertainty and absorb costs.[34]

5.40 The TCA stated there are high barriers to entry for tech businesses wanting to enter into government contracts generally and there is a need to make procurement systems more open and transparent.[35]

Data sovereignty and localisation concerns

5.41 Data sovereignty is a growing concern for Australians, with the OAIC's *Australian Community Attitudes to Privacy Survey 2020* stating that 74 per cent of Australians consider it to be 'a misuse of personal information' if their data has foreign processing access, an increase from 68 per cent in 2013.[36]

5.42 Vault Cloud provided a helpful definition:

> Data sovereignty refers to the right of a nation to control and manage its own data, regardless of where that data originated and [is] stored. This means that a country has the authority to determine how its data is collected, processed, and shared, as well as enforce its own laws and regulations related to data protection and privacy. Data sovereignty is often linked to national security, as countries may be concerned about foreign access to sensitive data.
>
> Data localisation, on the other hand, refers to the requirement that data be stored within a particular country's borders. This does not mean that a country has full control of the data as the laws of other counties may also apply.[37]

5.43 Many currently available cloud services are hosted overseas, with one submitter suggesting '[n]o cloud provider has any interest in expanding certain types of cloud services into Australia'.[38]

---

33 Digital Transformation Agency, *Submission 7*, p. 3.

34 Tech Council of Australia, *Submission 63*, p. 9.

35 Tech Council of Australia, *Submission 63*, p. 9.

36 Vault Cloud, *Submission 38*, [p. 5].

37 Vault Cloud, *Submission 38*, [p. 7].

38 Mr Cian Byrne, *Submission 75*, [p. 3].

5.44 Multiple submissions raised privacy concerns about Australian data being stored overseas, especially sensitive government data.[39] For example, Digital Rights Watch (DRW) raised concerns with the public sector storing data in private cloud services:

> … particularly if there is a risk that those companies might exit the Australian market, if those services are hosted overseas and subject to different regulatory environments, or if those companies display poor workplace behaviours or corporate citizenship.[40]

5.45 Vault Cloud argued both data sovereignty and data localisation are important to protect citizen data collected by government:

> Often, there is little to no choice in what personal information is stored by the Government. The public, therefore, has a higher standard for Government when it comes to the management of personal data. When people provide personal data to the Government, there is an expectation that this data will be stored and managed within Australia …
>
> Data sovereignty is important for protecting the privacy of individuals and safeguarding against the misuse of personal data. It is essential to ensure that the data of Australian citizens is safeguarded, and that the data is not used for purposes that are detrimental to the public interest.[41]

5.46 Submitters raised concerns that data stored overseas may be subject to foreign regulations and authorities and any governments those authorities have agreements with.[42]

5.47 Vault Cloud argued:

> When in country data is stored on services, which are subject to foreign laws, an organisation retains substantial legal obligations concerning that data's protection. However, the information may no longer be under their control and could be impacted by the laws and actions of a foreign country. This includes the future (as yet unwritten) laws of a foreign country. While the privacy laws of foreign countries may align to Australia's today, there is no certainty that they will do so in the future … It is essential to ensure that the data of Australian citizens is safeguarded, and that the data is not used for purposes that are detrimental to the public interest.[43]

---

39 See, for example, Digital Rights Watch, *Submission 68*, p. 19; OVHcloud, *Submission 72*, p. 7; Vault Cloud, *Submission 38*, [p. 7].

40 Digital Rights Watch, *Submission 68*, p. 19.

41 Vault Cloud, *Submission 38*, [p. 7].

42 See, for example, Vault Cloud, *Submission 38*, [p. 7]; OVHcloud, *Submission 72*, p. 7; Digital Rights Watch, *Submission 68*, p. 19.

43 Vault Cloud, *Submission 38*, [p. 6].

5.48 Vault Cloud highlighted that the US does not use public clouds for sensitive data and instead uses special sovereign variants known as 'Government Cloud', 'Community Cloud', 'Sovereign Cloud' or 'Secure Cloud'.[44]

5.49 On the other hand, some submitters argued against data sovereignty and localisation, framing it as being unnecessary and hindering business innovation.[45] For example, Meta stated:

> Data localisation policies in particular, not only impact the foundations o[f] the open internet, but also impose unnecessary costs and technical challenges on what should be efficiency-based decision-making processes, making them market blockers rather than the drivers of economic growth some imagine them to be.[46]

5.50 Microsoft outlined the importance of non-localised cloud infrastructure to protect information during the Ukraine war:

> … defence against a military invasion now requires for most countries the ability to disburse and distribute digital operations and data assets across borders and into other countries.[47]

5.51 The Australian Institute of Company Directors (AICD) 'caution[ed] around any further recommendations on data localisation'.[48] Mr Simon Mitchell, Senior Policy Adviser, the AICD, stated:

> … we have seen insufficient evidence that new comprehensive data localisation obligations are necessary or will improve the overall cyber-resilience and data management practices of Australian companies. It may be the case that requiring Australian companies to find domestic alternatives to a big tech cloud provider, by way of example, could deny businesses cost-effective, secure and innovative data protection solutions. The unintended consequence of such a policy could be to make individual Australians' data less secure.[49]

5.52 The Developers Alliance argued:

> Regulating data management on a globally dispersed platform presents multiple challenges. Firstly, cloud providers seldom have rights to access the data and processes they host for their customers. Secondly, what data they can access is often encrypted. Thirdly, the idea of where data is "located" is often a complex question. Fourthly, cloud providers can find themselves bound by conflicting laws where international authorities seek

---

44 Vault Cloud, *Submission 38*, [p. 6].

45 See, for example, Microsoft, *Submission 47*, p. 8; Mr Simon Mitchell, Senior Policy Adviser, Australian Institute of Company Directors, *Proof Committee Hansard*, 26 July 2023, p. 5.

46 Meta, *Submission 69*, p. 73.

47 Microsoft, *Submission 47*, p. 8.

48 *Proof Committee Hansard*, 26 July 2023, p. 8.

49 *Proof Committee Hansard*, 26 July 2023, p. 5.

> access to data from third jurisdictions or by acting extraterritorially. Mandating the localization of data for regulatory reasons is often used as a pretext for digital trade barriers, inviting reciprocity.[50]

Competition concerns

5.53 Big Tech use their dominant market position to collect vast quantities of user data and make these datasets exclusively available through the platform's own products and services.[51] For instance, Google bundles use of the data it collects within its own products in related markets across the digital advertising supply chain.[52]

5.54 Submissions indicated that lack of access to relevant data held by Big Tech creates a substantial barrier to entry and growth for competing businesses because Big Tech's wealth of data enables them target ads to specific consumers.[53] For example, Free TV Australia (Free TV) advised that data creates:

> … an insurmountable barrier to entry (and expansion) in the market for the provision of ad tech services. It is not practically feasible, in the short to medium term, for any other ad tech services providers to collect such broad ranging and unique data sets in relation to users to compete effectively with Google. Given this, a stark choice exists, either regulatory intervention occurs or Google will continue to dominate the ad tech services market in Australia.[54]

5.55 Submitters suggested Big Tech may also use third party generated data for anti-competitive purposes such as purchasing competitor products or creating similar products or features.[55] For instance, the Centre for AI and Digital Ethics stated Amazon is known to use seller data to create their own cheaper Amazon alternatives.[56]

5.56 The Commonwealth Bank of Australia stated this data advantage is exemplified by the Consumer Data Right (CDR), as most companies covered are Australian businesses:

> In the context of digital platforms, the unintended consequences of this is that domestic companies would be required to share their data with many

---

50 Developers Alliance, *Submission 35*, [p. 3].

51 Free TV Australia, *Submission 17*, p. 9.

52 Free TV Australia, *Submission 17*, p. 9.

53 See, for example, Commonwealth Bank of Australia, *Submission 71*, p. 4; Free TV Australia, *Submission 17;* Law Institute of Victoria, *Submission 12*, [p. 3]; ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 166.

54 Free TV Australia, *Submission 17*, p. 9.

55 See, for example, Law Institute of Victoria, *Submission 12*, [p. 3]; Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

56 Centre for AI and Digital Ethics, *Submission 23*, [p. 12].

> platforms today even though they are competing directly with them. This is further compounded by the lack of a broad definition of reciprocity. That is, under a broad definition, a party that becomes accredited to receive CDR data would also have an obligation share their data. The lack of a broad definition only adds to the competitive advantage that platforms have when it comes to Australians' data.[57]

Proposed solutions

5.57 This section explores a range of proposed solutions to the data issues raised throughout this chapter. Options raised by submitters include implementing the proposed Privacy Act reforms, a right to delete data, a statutory tort, obligations for companies to handle data fairly, prohibitions on targeted advertising, limits on data use and aggregation, and engaging with businesses.

5.58 Submitters also raised the importance of effective enforcement and international alignment.

The Privacy Act Review

5.59 Multiple submissions supported proposed reforms to the Privacy Act.[58] For example, the Australian Communications Consumer Action Network stated:

> We consider that it's appropriate that consumers have greater rights to not have their data collected, have greater rights to expressed consent to control how their data is collected and used by businesses. We're supportive of consumers having broader rights with respect to seeking redress where there have been breaches of their privacy. But, broadly speaking, we're quite supportive of the general thrust of the overall reforms.[59]

5.60 The AICD stated it supported modernising the Privacy Act, but raised concerns about some proposed reforms:

> … we are concerned that many of the proposed reforms are being advanced by a perception that Australia's privacy laws are weak and poorly performing, therefore warranting existing elements to be strengthened and made more prescriptive. Such a significant policy case needs to be comprehensively tested from a cost benefit perspective to ensure that the likely benefits will outweigh costs, for instance to innovation and business competitiveness with global counterparts.[60]

5.61 As one example, the AICD called for greater analysis of proposed removal of the existing small business exemption under the Privacy Act. It advised:

---

[57] Commonwealth Bank of Australia, *Submission 71*, p. 4.

[58] See, for example, Australian Communications Consumer Action Network, *Submission 20*, p. 37; Digital Industry Group Inc., *Submission 65*, p. 1; Mr Roger Somerville, Head, Australia and New Zealand Public Policy, Amazon Web Services, *Proof Committee Hansard*, 3 October 2023, p. 4.

[59] Australian Communications Consumer Action Network, *Submission 20*, p. 37.

[60] Australian Institute of Company Directors (AICD), *Submission 28*, [p. 4].

> This would be a significant change that would impose sweeping obligations on millions of small businesses and would come with material compliance costs at both an individual and aggregate business level. Our understanding is that under the proposed reforms the full suite of Privacy Act obligations will be imposed on small businesses, including for example the requirement to have a nominated senior manager be accountable for privacy. This approach, on first reading, appears disproportionate to the risk posed by many small businesses in mishandling personal information and will involve extensive compliance costs for potentially limited public benefit. Rather we would recommend that the Government focus on how such small businesses can be best supported, including in terms of building their cyber resilience and data management practices.[61]

Right to delete data

5.62 Under the Privacy Act Review, a right of erasure has been proposed. A right of erasure was supported by the Association of Heads of Independent Schools of Australia:

> Young people should not be burdened throughout their lifetime by a public profile generated by the malice of others or their own immaturity.[62]

5.63 Similarly, Mr James stated:

> … if we as Australians want to enforce our own privacy rights to have that data deleted, it's close to impossible or extremely expensive to do. If we had some mechanisms to enable consumers to go through a process to work with those data brokers and have their data removed, that's something that I think would go a long way towards protecting citizens' information.[63]

Statutory tort

5.64 Several submissions expressed support for the introduction of a statutory tort as proposed in the Privacy Act Review.[64] Mr Mark Nottingham, expert advisor to the UK Competition and Markets Authority's Digital Markets Unit, stated this 'would help to give the Privacy Act the teeth that it is so often missing.'[65]

5.65 Children and Media Australia (CMA) commented in support:

> CMA can see the advantage of a statutory tort in that companies would be forced to take the risk of litigation into account when determining their practices, which means a significant chance of potential accountability shaping those choices. This means of deterring undesirable behaviour

---

61 AICD, *Submission 28*, [p. 4].

62 Association of Heads of Independent Schools of Australia, *Submission 13*, p. 3.

63 Mr Rob James, Principal Consultant and Chief Executive Officer, Rob James Consulting Pty Ltd, *Proof Committee Hansard*, 26 July 2023, p. 34.

64 See, for example, Mr Mark Nottingham, *Submission 37*, p. 4; Children and Media Australia, *Submission 53*, p. 2; Ms Elizabeth Hampton, Deputy Commissioner, OAIC, *Proof Committee Hansard*, 22 August 2023, p. 29.

65 Mr Mark Nottingham, *Submission 37*, p. 4.

> would be a useful addition to mechanisms such as market forces and negative publicity; and may be all the more helpful considering that under the digital platform business model there is no particular need to please the user/consumer.[66]

5.66 Submissions suggested there should be adequate options for consumers if they identify misuse of their data, without having to go through courts, which involves access to justice issues.[67] For example, CMA suggested:

> … there are risks associated with relying entirely on aggrieved consumers to undertake litigation: it can lead to significant burdens on individuals to prosecute the common good, and windfall gains at the other end. Therefore CMA submits that the ACCC should be empowered and resourced to bring representative actions under any statutory tort.[68]

Obligations to handle data fairly

5.67 Evidence to the committee supported implementation of a positive obligation for digital platforms to handle data fairly or in the best interests of users.[69]

5.68 The OAIC supported the proposed reform in the Privacy Act Review, establishing a positive obligation on organisations to handle personal information fairly and reasonably. It suggested:

> … a positive obligation for organisations to handle data fairly and reasonably would give individuals greater confidence that they will be treated fairly when they choose to engage with a service. This would prevent consent being used to legitimise handling of personal information in a manner that, objectively, is unfair or unreasonable.[70]

5.69 CHOICE stated a duty of care requirement should be implemented and 'require entities to take reasonable care not to cause foreseeable harm to consumers through collection, handling and use of their data'.[71]

5.70 The CPRC argued in favour of a provision to make companies responsible for delivering safe, secure data-driven products and services:

> Incorporating a duty of care or best-interests duty (similar to a fiduciary duty), especially for how consumer data is treated and how choice architecture is presented and implemented on digital platforms, can help add a level of accountability on digital platforms that could significantly reduce the likelihood of consumer harm. It could also lead to pro-business

---

66 Children and Media Australia, *Submission 53*, p. 2

67 See, for example, Dr Shaanan Cohney, Senior Lecturer, School of Computing Information Systems, private capacity and Researcher, Centre for AI and Digital Ethics, *Proof Committee Hansard*, 26 July 2023, p. 49; Children and Media Australia, *Submission 53*, p. 3.

68 Children and Media Australia, *Submission 53*, p. 2.

69 See, for example, CHOICE, *Submission 54*, p. 5; OAIC, *Submission 61*, p. 3.

70 OAIC, *Submission 61*, p. 3.

71 CHOICE, *Submission 54*, p. 5.

> benefits by increasing consumer trust in those platforms that actively build this into their business model. The idea of a best interests duty for consumer data is relatively new and unexplored in the Australian context. As a next step, CPRC recommends an inquiry to explore how to construct and implement positive obligations on businesses to use data in consumers' interests.[72]

5.71 The Centre for AI and Digital Ethics stated it is insufficient to rely on notice and consent regimes to address privacy harms. It noted that individuals 'cannot be meaningfully expected to spend the large amount of time necessary to analyse and ruminate over consent for each service for which they engage'.[73] It supported:

> … a regime that requires platforms to adhere to pro-privacy. We support regimes to allow individuals to correct errors in their collected information, withdraw consent for process, and to mandate subsequent erasure. There are additional safeguards that protect consumers despite the illusory nature of online consent. We support standardised and simple consent on-boarding, with standard iconographs and layouts, to help minimise consumer consent fatigue.[74]

Prohibitions on targeted advertising

5.72 Submissions supported the introduction of a prohibition on targeted advertising without free and informed consent from users.[75]

5.73 The Obesity Policy Coalition stated this is particularly important for the marketing of harmful products, such as unhealthy food and alcohol. It recommended:

> … that express consent be required for digital platforms, including social media services, to collect, use or disclose an individual's personal information or data for commercial marketing purposes, particularly in terms of marketing for unhealthy food and drinks. These protections should enable individuals to effectively opt-out of commercial marketing, and in particular harmful industry marketing.[76]

5.74 The HRLC expanded:

> Instead of permitting profiling by default and allowing users to opt out, regulation in Australia should go further by requiring default settings to not be based on profiling. This would ensure that users who are less aware of the operation of recommender systems will not be treated less favourably

---

72 Consumer Policy Research Centre, *Submission 60*, p. 7.

73 Centre for AI and Digital Ethics, *Submission 23*, [p. 5].

74 Centre for AI and Digital Ethics, *Submission 23*, [p. 5].

75 See, for example, HRLC, *Submission 50*, p. 12; Foundation for Alcohol Research and Education, *Submission 33*, p. 5; Obesity Policy Coalition, *Submission 19*, p. 5.

76 Obesity Policy Coalition, *Submission 19*, p. 5.

> and would limit the role of personalised content recommendation systems in amplifying disinformation and hate speech.[77]

Limits on data use and aggregation

5.75 Multiple submissions suggested limiting data use and aggregation by digital platforms.[78]

5.76 The ACCC recommended obligations to address barriers to entry and expansion caused by the market power of big tech. Subject to privacy considerations, it suggested:

- data access requirements which require designated platforms to provide access to specific data sources on an agreed basis to rivals;
- data portability requirements which would allow a consumer to request designated platforms transfer their data to them or a third party; and
- data use limitations which would place restrictions on how a designated platform collects, stores, or uses certain data.[79]

5.77 Free TV suggested regulation to limit data use, to strike a balance between privacy harm minimisation and promoting competition:

> … Free TV submits that given the legitimate privacy concerns raised by these [ACCC] approaches, the only effective way to remedy the identified competition harms at the current time would be to limit data use by designated entities. This would be privacy enhancing, in that it would limit the use of data about individuals as compared to data portability or interoperability arrangements, which would increase the use of such data. The pro-competitive effects of limiting the ability of designated entities to leverage their data advantages would far outweigh the decreases in efficiency for designated entities caused by the implementation of these measures.[80]

Business engagement

5.78 Several submissions suggested the government partner with industry to ensure that companies have the knowledge and expertise to combat cyber security threats.

5.79 The AICD suggested the government partner with industry to ensure greater coordination across relevant agencies, clarity on regulator responsibilities and proactive threat and intelligence sharing. Additionally, it recommended:

---

77 HRLC, *Submission 50*, p. 12.

78 See, for example, Free TV Australia, *Submission 17*, p. 20; ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 168; Mr Joshua Zubak, *Submission 27*, p. 5.

79 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 168.

80 Free TV Australia, *Submission 17*, p. 20.

- a safe harbour or protected information mechanism where an organisation can share information of a significant cyber incident with a regulator(s) to assist in response and recovery without concern that the information will subsequently be used in enforcement action;
- consideration of how existing reporting and notification obligations (e.g. SOCI [Security of Critical Infrastructure] Act obligations, Notifiable Data Breaches Scheme) can be harmonised or streamlined with the goal that an organisation only needs to report or notify to the Government once;
- targeted support for SME [small to medium enterprises] and NFPs [not for profits] to build cyber security resilience and improve data management practices, education, information sharing and guidance in the event of experiencing and recovering from a cyber security incident ...[81]

5.80 The Council of Small Business Organisations Australia (COSBOA) also recommended the government focus on educating and upskilling small businesses so that they feel empowered to take ownership to mitigate risk, voluntarily upskill their staff, and ensure safe data collection:

> The introduction of a Small Business Privacy Code, including a best practice guide and checklist for compliance, would be a helpful solution. Ideally, small businesses would be supported through a program such as COSBOA's Cyber Wardens pilot program which aims to become Australia's first cyber safety workplace certification or micro-credential for the small business sector. The program is designed by small business for small business, and aims to upskill the nation's small business workforce to give owners and employees the knowledge and tools they need to safely engage in the digital economy. This program would complement the Small Business Privacy Code, helping small businesses understand and mitigate risk when engaging with big technology companies, achieve best practice and ensure compliance with regulatory requirements.[82]

5.81 BSA – The Software Alliance noted the Department of Home Affairs Trusted Information Sharing Network (TISN) is a positive example of an effective and innovative public-private partnership mechanism:

> The TISN is comprised of representatives from different critical infrastructure sectors, and each sector is supported by an Australian Government agency — usually the agency that has regulatory responsibility for that sector. Under the TISN Data Sector Group, data storage and processing service providers, which include cloud service providers, work together with government agencies to: a) identify and manage risks to critical infrastructure; b) address security gaps within sectors and implement mitigation strategies; c) inform future policy and programs to

---

81 AICD, *Submission 28*, p. 3.

82 Council of Small Business Organisations Australia, *Submission 59*, p. 2.

> further support critical infrastructure resilience; and d) achieve the objectives of the Critical Infrastructure Resilience Strategy.[83]

Enforcement

5.82 Multiple submissions argued that the existing provisions of the Privacy Act need to be better enforced.[84] For example, the CPRC commented:

> For legislation and its respective penalties to be effective, they need to be supported by regular surveillance and enforcement by the regulator to educate and shift the market towards a more consumer-centric approach to the digital economy.[85]

5.83 CHOICE argued the OAIC should be strengthened:

> OAIC is under-resourced and lacks many of the regulatory powers of its consumer protection counterparts, including the ACCC and the Australian Securities and Investment Commission (ASIC). A permanent increase in funding will provide OAIC the resources needed to investigate other breaches. It will also allow OAIC to take preventative measures to mitigate the risk of future data breaches.[86]

5.84 The OAIC agreed, stating it is looking for expanded powers including:

> … a new mid-tier civil penalty provision for interference with privacy that doesn't meet the threshold of 'serious and repeated' and a low-level tier of civil penalty provisions for administrative breaches of the act, with some infringement notice powers.[87]

5.85 Several submissions supported increasing penalties to incentivise digital platforms to address privacy risks.[88]

5.86 The Centre for AI and Digital Ethics stated:

> Stronger penalties increase the likelihood that a CISO [Chief Information Security Officer] can get access to decision-makers with budget assigning powers (particularly the Board) and helps a CISO to make the for diverting funds to improving cyber security. This is justifiable as organisational failures in cybersecurity impose substantial financial and non-financial

---

83 BSA – The Software Alliance, *Submission 32*, pp. 6–7.

84 See, for example, Mr Mark Nottingham, *Submission 37*, p. 4; Consumer Policy Research Centre, *Submission 60*, [p. 6].

85 Consumer Policy Research Centre, *Submission 60*, [p. 5].

86 CHOICE, *Submission 54*, p. 5.

87 Ms Elizabeth Hampton, Deputy Commissioner, OAIC, *Proof Committee Hansard*, 22 August 2023, p. 29.

88 See, for example, Consumer Policy Research Centre, *Submission 60*, [p. 5]; Law Institute of Victoria, *Submission 12*, [p. 7]; Centre for AI and Digital Ethics, *Submission 23*, [p. 3].

> externalities on ordinary Australian who suffer privacy loss, identity theft, and financial fraud as the result of hacks.[89]

5.87 The Centre for AI and Digital Ethics recommended proportional penalties relative to the amount of sensitive information an organisation holds rather than the size of the organisation:

> Doing so could create a powerful incentive for smaller and medium sized organisations (who generally have fewer resources to devote to cyber security and data protection) to avoid collecting and storing too much sensitive information. However, there may be diminishing returns thus extreme penalties may be no additional help and may simply be viewed as unduly harsh. Further, such unreasonably harsh penalties may incentivise organisations or staff to hide problems rather than dealing with them openly, thus weakening the response capability.[90]

5.88 The Law Institute of Victoria suggested capping penalties at a percentage of revenue 'to incentivise regulatory compliance in industry, whilst ensuring that small and medium companies are not disproportionately affected by overwhelming penalties'.[91]

International alignment

5.89 Multiple submissions supported international alignment of data laws and supported implementing a similar approach to the EU GDPR (see Box 5.1).[92] For example, the Developers Alliance commented:

> On data privacy, the EU's GDPR provides a valuable test case. While most of the regulation has seen strong industry support, its data export provisions have proven unworkable in part because they create localized exceptions which are not extended internationally. This lack of international comity has resulted in rules which promote internet fragmentation, an outcome we fear is inevitable as extra-territorial regulations multiply around the world. We highlight internet fragmentation due to incompatible international regulations the single greatest threat to Australia's digital economy.[93]

5.90 The Irish Council for Civil Liberties supported implementation of the GDPR but highlighted the importance of enforcement as the GDPR has been frequently infringed upon without action by regulating authorities.[94]

---

89 Centre for AI and Digital Ethics, *Submission 23*, [pp. 3–4].

90 Centre for AI and Digital Ethics, *Submission 23*, [p. 4].

91 Law Institute of Victoria, *Submission 12*, [p. 7].

92 See, for example, Developers Alliance, *Submission 35*, [p. 4]; Irish Council for Civil Liberties, *Submission 36*, p. 3; Mr Roger Somerville, Head, Australia and New Zealand Public Policy, Amazon Web Services, *Proof Committee Hansard*, 3 October 2023, p. 4; Australian Medical Association, *Submission 66*, p. 3; Microsoft, *Submission 47*, p. 14.

93 Developers Alliance, *Submission 35*, [p. 4].

94 Irish Council for Civil Liberties, *Submission 36*, p. 3.

5.91 The AICD cautioned the committee on implementing the GDPR in Australia:

> More generally, we understand that research conducted into the GDPR in the EU has identified legitimate questions about its effectiveness in improving privacy and has had potential detrimental impacts on innovation. These studies point to the clear need for the Government to comprehensively consider the appropriateness of broadly adopting the GDPR model in Australia.[95]

Box 5.1 The EU General Data Protection Directive

The GDPR established additional obligations for businesses and rights for individuals. Examples of requirements include:

- Businesses must inform consumers about data collected.
- Consumers can request a record of data held by businesses and have options to have it deleted.
- Businesses cannot combine data collected from different parts of their business.

The GDPR also grants national authorities additional investigative and sanctioning powers, including the ability to raid organisations, compel information, impose significant fines, and 'block data use, which is the ultimate sanction for international digital platforms'.

Source: General Data Protection Regulation 2016 (EU); Irish Council for Civil Liberties, Submission 36, p. 1.

[95] AICD, *Submission 28*, [p. 5].

Chapter 6
Algorithmic transparency

Overview

6.1 Algorithms are essential in the digital environment. They facilitate a level of personalisation, helping users navigate the immense volume of online material to discover content of relevance and interest.[1]

6.2 The Office of the eSafety Commissioner (eSafety) provided the following overview of the role of algorithms in digital services:

> An algorithm is a coded sequence of instructions that is often used by online service providers to prioritise content a user will see.
>
> These instructions are determined by platforms based on many factors, such as user attributes and patterns, and can involve personalised suggestions to achieve a particular goal, such as discovering new artists, friends, products, activities, and ideas, as well as helping business and creators efficiently reach a target audience.
>
> For these reasons, algorithms are used by almost all digital platforms to amplify, prioritise and recommend content and accounts to their users. Their use and sophistication continues to grow, with multiple algorithms typically being active within a platform at any given time, all completing different tasks with different outcomes.[2]

6.3 Algorithms are also used by some digital platforms to assist with content moderation, identification of harmful material as well as for targeted advertising.

6.4 Automated decision making (ADM) may sometimes use artificial intelligence (AI) technologies but is often guided by rules-based formulas.

Risks from algorithm and ADM use by digital platforms

6.5 The committee received concerns that algorithms used by digital platforms do not operate in a way that adequately supports community values, such as fairness, accuracy, privacy and user safety.[3]

---

1 See, for example, Australian Broadcasting Corporation (ABC), *Submission 4*, p. 2; Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), *Submission 9*, p. 4; Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 17.

2 Office of the eSafety Commissioner (eSafety), *Submission 2*, pp. 2–3.

3 ABC, *Submission 4*, p. 2, DITRDCA, *Submission 9*, p. 4, CHOICE, *Submission 54*, p. 1.

6.6 At the heart of concerns around the emerging risks and harms is a lack of transparency around the information and user behaviour that influences the algorithmic operation and an algorithm's intended outcome.

6.7 The risks associated with some algorithms, particularly those used to curate social feeds and in search functions, are of growing concern.[4] The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) noted that the use of algorithms can lead to risks across a number of areas including:

- dis- and misinformation
- ranking and search algorithms relevant to how news is served to consumers
- digital and media literacy initiatives
- social harm issues – including echo chambers, online hate speech, and social media feed curation
- discoverability of Australian screen and music content on streaming services
- general consumer harms, including algorithmic biases or discrimination.[5]

6.8 Evidence suggested algorithms have the potential to amplify online harms including radicalisation, cause exposure to material a user would not have sought out, improperly elevate harmful messages or voices through filter bubbles in addition to ad targeting and erosion of privacy.[6]

6.9 This chapter explores some of these algorithmic related risks in more detail and considers the role of transparency in mitigating online algorithm harms.

Social harm concerns

Filter bubbles/echo chambers

6.10 A filter bubble is a term used to describe the effect of online algorithms and user behaviour resulting in users being presented with material reflecting limited perspectives.

6.11 eSafety provided the following definition of an echo chamber or filter bubble:

> An echo chamber, also known as a filter bubble, is an environment where a person mostly encounters information or opinions that reflect and reinforce their own. An online echo chamber can develop when a user only follows or interacts with like-minded people, or when recommender systems keep serving content that aligns with the user's search and engagement history.[7]

---

4 DITRDCA, *Submission 9*, p. 4.

5 DITRDCA, *Submission 9*, p. 4.

6 DITRDCA, *Submission 9*, p. 4.

7 eSafety, *Glossary*, www.esafety.gov.au/about-us/glossary (accessed 17 October 2023).

6.12 A range of submissions discussed the risks of algorithms operating in a way that creates filter bubbles or echo chambers.[8]

6.13 One of the risks of algorithms amplifying some content is it may deprioritise or exclude viewpoints or ideas contrary to the user's existing beliefs. The committee was advised that 'echo chambers can impact a person's freedom of thought, access to information and autonomy, and can contribute to polarisation'.[9]

6.14 Algorithm design elements can encourage, facilitate or intensify risks and harms including engagement in, or exposure to anti-social behaviour. The Alannah & Madeline Foundation advised:

> It is harder to attribute this problem directly to design issues, but it seems reasonable to assume the risk is enhanced by features like popularity metrics, which can serve to reward shocking or emotive content; manipulation of user emotions, for example through recommending of extreme material; and 'echo chambers' encouraged by algorithms which sometimes function to normalise anti-social conduct.[10]

6.15 eSafety also noted the potential for algorithms to amplify harmful and extreme content. Where platforms aim to optimise user engagement via content feeds, there is a risk that their algorithms will display increasingly shocking or extreme content to consumers. This content draws comments and is in turn considered 'engaging' by algorithms, so is thus amplified to an extensive number of users, 'increasing the content's reach and potential impact'.[11]

6.16 eSafety raised additional risks:

> Sometimes these algorithms operate in a way that results in the wide dissemination of content before human and editorial oversight is triggered. They can also artificially promote content that has been deemed 'engaging' without balancing other types of content and viewpoints.
>
> On an individual level, these processes can increase the impact experienced by those exposed to harmful material. On a broader societal level, the amplification of content that promotes discriminatory views, such as sexism, misogyny, homophobia, or racism, may have adverse effects, such as normalising prejudice or hate. This may also contribute to radicalisation towards terrorism, violent extremism, and provide users with avenues to find associated groups.[12]

---

8 See, for example, ABC, *Submission 4*, pp. 2–3; eSafety, *Submission 2;* Office of the Australian Information Commissioner (OAIC), *Submission 61;* Commercial Radio & Audio (CRA), *Submission 43*; DITRDCA, Submission 9, p. 4.

9 eSafety, *Submission 2*, pp. 3–4.

10 Alannah & Madeline Foundation, *Submission 41*, p. 6.

11 eSafety, *Submission 2*, p. 3.

12 eSafety, *Submission 2*, p. 3.

6.17 That said, eSafety also highlighted that these issues may be overstated despite some evidence linking algorithms to filter bubbles.[13]

6.18 The Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry Final Report considered evidence both suggesting and disputing the existence of filter bubbles and echo chambers. Focusing on the impacts on the consumption of journalism, it concluded:

> Algorithmic curation on digital platforms and user behaviour on social media have the potential to cause 'echo chamber' and 'filter bubble' effects, although the extent of any harm caused by these effects in Australia is not yet clear.[14]

6.19 The ACCC further commented:

> The specific effect is likely to depend on the algorithm in operation at the time, and the behaviours and cultures of platform users.[15]

Bias and discrimination (hate speech/online hate)

6.20 The committee heard that the use of certain algorithms and ADM also risks creating or exacerbating existing online discrimination, bias and market inequalities.[16]

6.21 ADM can make inaccurate and wrong decisions and create barriers for consumer redress.[17] Examples included Airbnb's social scoring algorithm which is based on personal data, including social media activities, and which can be used to determine a user's access to the service. Users have no oversight over how their score is created or decisions such as account suspension are made.[18] CHOICE also highlighted Tinder's use of algorithms to create different charge rates based on a user's age, geographical location and sexuality.[19]

6.22 ADM may also result in 'an intensification and amplification of pre-existing issues, problems and inequalities, rather than meaningfully changing them'.[20] For example, Digital Rights Watch noted:

> Automated decision making systems used in recruitment can exacerbate pre-existing biases, in turn hindering people's economic opportunities. For

---

13 eSafety, *Submission 2*, p. 4.

14 ACCC, *Digital Platforms Inquiry Final Report*, June 2019, p. 345.

15 ACCC, *Digital Platforms Inquiry Final Report*, June 2019, p. 349.

16 CHOICE, *Submission 54*, p. 1.

17 CHOICE, *Submission 54*, p. 1.

18 CHOICE, *Submission 54*, p. 2.

19 CHOICE, *Submission 54*, p. 2.

20 Digital Rights Watch, *Submission 68*, p. 31.

> example, research has shown that recruitment algorithms favour male applicants.[21]

6.23 The Human Rights Law Centre (HRLC) noted gaps in current regulations enable online hate speech to persist, with the burden of identifying, avoiding and responding to harm borne by the affected individuals and communities.[22] It stated:

> In Australia, victims of online hate speech have faced difficulty asserting their right to freedom from discrimination. For example, platforms have argued that they are beyond the reach of Australian privacy and anti-discrimination laws due to their corporate structure and incorporation in other countries.[23]

6.24 Reset Australia highlighted the limitations of current legislation, noting:

> Regulation focuses on individual pieces of content, and overlooks the role of platforms in promoting harmful content to children (via algorithms, for example). Hate speech, mis & disinformation are not adequately addressed in the current framework, but can be harmful.[24]

6.25 The Australian Muslim Advocacy Network (AMAN) proposed the introduction of a duty of care on digital platforms 'to uphold Australian hate speech standards, which may prompt platform investment in compliance units. Currently, they do not invest in this'.[25]

6.26 The committee notes algorithms and ADM are also used by platforms for content moderation and safety. Meta advised about its 'increased use of proactive detection technology to identify and proactively remove and action hate speech'.[26] Ms Mia Garlick, Regional Director of Policy, Meta, explained:

> I think this is an example of artificial intelligence and machine learning improving over time. When we first started disclosing our figures in relation to this, we were proactively identifying and removing around 13 per cent of all hate speech that we removed, and that's now well up over 80 per cent. We've certainly been working to make sure that we are able to be a lot more proactive in terms of removing harmful and hateful content on our services to make sure that people are coming to the platform and advertisers are advertising on the platform in connection to content that they find valuable and relevant.[27]

---

21 Digital Rights Watch, *Submission 68*, p. 31.

22 Human Rights Law Centre, *Submission 50*, p. 8.

23 Human Rights Law Centre, *Submission 50*, p. 8.

24 Reset Australia, *Submission 74*, p. 6.

25 Australian Muslim Advocacy Network (AMAN), *Submission 44*, p. 23.

26 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 23.

27 *Proof Committee Hansard*, 22 August 2023, p. 23.

International approaches

6.27 The Irish Council for Civil Liberties advised the new European Union (EU) Digital Services Act (DSA) contains relevant provisions important for reducing online hate and hysteria (see Box 6.1 for details of relevant Articles).

Box 6.1 EU Digital Services Act

The Irish Council for Civil Liberties explained:

> First, Article 38 compels digital platforms to give people the option to switch off the toxic algorithms that show them personalised material based on their political or philosophical views, or ethnicity or other intimate characteristics. These recommender systems cause hate and division, for the reasons set out at paragraph 7 (a), above [see submission]. The option to switch off a recommender system must be available whenever these algorithm[s] are active.
>
> Second, Article 34 and 35 of the DSA require large digital platforms to assess and mitigate the risks caused by their systems, including risks to civic discourse and public security. This may be effective if we can avoid the platforms turning it in to compliance theatre.

The DSA will be enforceable on large digital platforms from February 2024.

Irish Council for Civil Liberties, Submission 36, pp. 3–4.

6.28 AMAN advised the United Kingdom (UK) online safety legislation relies on a user empowerment focus to address online hate and misinformation, which comes with risks:

> We agree that user empowerment is important. However, we note the inherent limitations of user empowerment: Communities that are hyper-sceptical of hate speech controls and more likely to embrace absolutist free speech. They will not use options to remove hate speech and misinformation. This means that targeted 'outgroups' will continue to be endangered by dehumanising disinformation operations.[28]

Influence on public debate and democratic processes

6.29 Submissions noted the risks of algorithms and ADM to public debate and democratic processes. As discussed above, algorithms may filter out or favour particular information and viewpoints, intentionally or otherwise.

6.30 The Australian Broadcasting Corporation (ABC) raised concerns that 'algorithms applied by search engines and social media (for example Meta's Facebook and Google's YouTube) can influence the news and information that

[28] AMAN, *Submission 44*, p. 23.

people see, potentially leading to a concentration of power over public discourse and opinion formation'.[29] It further explained:

> … well-functioning democracy depends on the free flow of accurate information, objective analysis, and diverse opinions. When an algorithm suggests and automatically plays the next video or recommends social media pages to a user, it is filtering information based on what the user appears to be most interested in. This can push users into a feedback loop and an endless cycle of like-minded content, which can present a particular risk when the content is biased or misleading, or doesn't show information that presents a different point of view. [30]

6.31 Vault Cloud advised:

> … the flow of information and algorithmic bias creating "echo chambers" or polarisation could potentially shape or manipulate public opinion resulting in herd mentality, which could cause destabilisation.[31]

6.32 The committee was advised that aggregated data reflecting consumers' activities, interests, values, attitudes and needs is increasingly being leveraged by political parties to run campaigns. Further, targeted campaigns to influence user behaviour are permeating into the political sphere 'as exhibited by the 2016 Facebook-Cambridge Analytica matter' which:

> … raises the concern that attempts by political parties to influence individual behaviour threatens to undermine the integrity of the electoral process by interfering in the political and civic communication that is essential to representative democracy.[32]

Content moderation

6.33 In addition to content recommendations, algorithms are used by digital platforms for content moderation and safety processes. The committee received evidence in support of greater transparency around content moderation decisions.

6.34 The AMAN noted that 'platforms use algorithms to prevent and reduce harms by semi-automating the process of flagging, removing, and re-ranking third-party contents likely to violate platform policies or laws'.[33] However, it advised:

> When this process is performed at scale, the algorithms cannot perform perfectly and are continuously optimized to balance between precision and accuracy.

---

29 ABC, *Submission 4*, p. 2.

30 ABC, *Submission 4*, p. 2.

31 Vault Cloud, *Submission 38*, [p. 7].

32 Mr Joshua Zubak, *Submission 27*, p. 5.

33 AMAN, *Submission 44*, pp. 15–16.

> If a platform prioritizes accuracy over precision in using algorithms for content moderation, its process would have a high false positive rate. Most large platforms therefore choose to prioritize precision over accuracy, which allows most users to post contents but can sometimes lead to extensive harm when false negatives are shared widely.[34]

6.35 The AMAN further advised:

> … the ability to assess dehumanising information operations with accuracy and precision is more possible than identifying violations of hate speech policies at large, because there is a visible and distinct formula that such operations use in order to dehumanise an outgroup to an ingroup audience.[35]

6.36 Digital Rights Watch (DRW) highlighted risks with moderation algorithms and community guidelines used by some platforms. It advised that, while automated systems may be necessary, decisions need to be made about who defines and designs the systems that curate content, and for what purpose. Those decisions have been made by private companies making curation decisions driven exclusively by the desire for profit and growth.[36]

6.37 DRW explained the resulting risks included an exportation of United States (US) cultural values via 'community guidelines' onto a global scale as the majority of dominant digital platforms are based in the US. The design and implementation of 'a set of globally homogenous moral standards' by digital platforms impacts 'creative, cultural, and educational online expression in places whose norms may not align with those of the United States'.[37] DRW noted:

> … artistic expression that includes nudity, as well as sexual education and activism have all been caught up in strict conservative content moderation policies regarding nudity. In 2018, Zuckerberg said it's "easier to detect a nipple than hate speech with AI."[38]

6.38 Another risk DRW identified was the difficulty in accurately identifying and removing content en masse without a resulting over- or under- capture of particular forms of content:

> Automated content moderation on popular social media sites has caused harm to users by disproportionately removing some content over others, penalising Black, Indigenous, fat, and LGBTQ+ people.[39]

---

34 AMAN, *Submission 44*, pp. 15–16.

35 AMAN, *Submission 44*, p. 16.

36 Digital Rights Watch (DRW), *Submission 68*, p. 27.

37 DRW, *Submission 68*, p. 26.

38 DRW, *Submission 68*, p. 26.

39 DRW, *Submission 68*, p. 26.

6.39 Some platforms acknowledge the risks around content moderation. For example, Meta advised that it is a founding member of the Digital Trust and Safety Partnership (DTSP) 'which is developing approaches to evaluate digital platforms' content moderation practices and drive globally consistent trust and safety outcomes.[40]

Dis- and misinformation

6.40 Misinformation is false, misleading or deceptive information that can cause harm. The Australian Communications and Media Authority (ACMA) advises that misinformation can include:

- made-up news articles
- doctored images and videos
- false information shared on social media
- scam advertisements.[41]

6.41 The ACMA explains:

> Misinformation can pose a risk to the health and safety of individuals, as well as society more generally. We have seen this with misinformation about COVID-19 vaccines and 5G technology.
>
> Some misinformation is deliberately spread – this is called disinformation – to cause confusion and undermine trust in governments or institutions. It is also used to attract users to webpages for financial gain, where they may click on ads or be lured into financial scams.
>
> But not all misinformation is deliberately spread to cause harm. Sometimes users share misinformation without realising it.[42]

6.42 The rise of dis- and misinformation online, particularly on social media platforms, was noted in several submissions.[43]

6.43 A prime example of dis- and misinformation, was the threat it created to public health during the COVID-19 pandemic.[44] The HRLC explained:

> The COVID-19 pandemic highlighted both the rapidly evolving nature of online mis- and disinformation, as well as its potential to undermine public health and fuel discrimination. Misleading content about the origin and nature of the virus spread rapidly across digital platforms in Australia. This disinformation combined with hate speech online to fuel discrimination and stoke violence against Asian people in Australia, threatening their safety.

---

40 Meta, *Submission 69*, p. 70.

41 ACMA, *Online Misinformation*, www.acma.gov.au/online-misinformation (accessed 21 September 2023).

42 ACMA, *Online Misinformation*, (accessed 21 September 2023).

43 See, for example, Centre for AI and Digital Ethics, *Submission 23*, [p. 15]; Human Rights Law Centre (HRLC), *Submission 50*, p. 6; Australian Media Literacy Alliance, *Submission 55*, p. 2.

44 Centre for AI and Digital Ethics, *Submission 23*, [p. 15]; HRLC, *Submission 50*, p. 6.

> Australian health authorities pointed to the spread of online mis- and disinformation contributing to a spike in cases during a critical period in 2000.[45]

6.44 Similarly, the HRLC advised the risks of disinformation influencing or even undermining democratic election processes:

> Powerful false narratives can be quickly amplified to millions with the potential to confuse the public, distort outcomes and undermine public confidence in electoral processes and results.[46]

6.45 It further noted:

> Facebook identified 2.2 billion fake accounts as engaging in "coordinated inauthentic behaviour" in the lead-up to the 2019 election. Local disinformation campaigns, such as Mediscare in 2016 and Death Tax in 2019, are becoming a common feature of Australian elections as campaigns and news consumption move further online.[47]

Existing regulatory framework

6.46 In 2021 a voluntary Australian Code of Practice on Disinformation and Misinformation (ACPDM) was created with eight signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitter. The voluntary code is administered by Digital Industry Group Inc. (DIGI). Signatories release an annual transparency report on the measures they are taking to address dis- and misinformation.[48]

6.47 The DITRDCA advised:

> The ACMA's June 2021 Report on the adequacy of digital platforms' disinformation and news quality measures explored the question of whether the voluntary code meets community expectations. It made a number of findings and recommendations which have informed both DIGI's recently revised Code, released in December 2022, and the Government's decision to introduce new powers for the ACMA to combat dis- and misinformation on digital platforms.[49]

6.48 The ACMA report noted 'existing efforts by signatories to the voluntary industry code were a good first step in efforts to tackle misinformation and disinformation on digital platform services'.[50]

---

45 HRLC, *Submission 50*, p. 6.

46 HRLC, *Submission 50*, p. 6.

47 HRLC, *Submission 50*, pp. 6–7.

48 ACMA, *Online Misinformation*, (accessed 21 September 2023).

49 DITRDCA, *Submission 9*, p. 9.

50 DITRDCA, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet*, June 2023, p. 3.

6.49 Despite this, the government has proposed additional reserve powers for the ACMA to act, should industry efforts in regard to misinformation and disinformation be inadequate.[51]

6.50 It was not clear to the Communications Alliance what evidence prompted the Government to make moves towards implementing additional regulations or legislation in this area when the voluntary code has only been in operation for a limited time.[52]

6.51 Under the proposal, the new laws would provide the ACMA with additional powers to combat online dis- and misinformation. The new powers are designed to strengthen and support the existing voluntary code and will extend to non-signatories of the voluntary code.[53] DITRDCA noted:

> The new powers will enable the ACMA to monitor efforts and require digital platforms to do more, placing Australia at the forefront in tackling harmful online misinformation and disinformation, while balancing freedom of speech.
>
> The proposed powers would:
>
> - enable the ACMA to gather information from digital platform providers, or require them to keep certain records about matters regarding misinformation and disinformation
> - enable the ACMA to request industry develop a code of practice covering measures to combat misinformation and disinformation on digital platforms, which the ACMA could register and enforce
> - allow the ACMA to create and enforce an industry standard (a stronger form of regulation), should a code of practice be deemed ineffective in combatting misinformation and disinformation on digital platforms.
>
> The ACMA will not have the power to request specific content or posts be removed from digital platform services.[54]

6.52 DIGI indicated to the committee its support for the proposal that would see the ACMA granted an additional oversight role of the ACPDM and dis- and misinformation more broadly.[55]

---

51 DITRDCA, *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet*, June 2023, p. 1.

52 Communications Alliance, *Submission 58*, p. 6.

53 DITRDCA, *New ACMA powers to combat misinformation and disinformation*, www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation (accessed 20 October 2023).

54 DITRDCA, *New ACMA powers to combat misinformation and disinformation*, (accessed 20 October 2023).

55 DIGI, *Submission 65*, p. 1.

6.53 Public consultation on the exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 closed in August 2023. [56] The Bill has not yet been introduced into Parliament.

6.54 Agencies in the Communications portfolio, including the ACMA and eSafety, also use a range of less direct levers to counter the effects of dis- and misinformation such as:

- support for high quality public interest journalism, e.g. through funding of ABC and SBS
- education programs to improve media and digital literacy in the community
- provision of reliable information including in languages other than English, e.g. SBS provided critical COVID-19 health information in 63 languages
- the ACMA, under the *Broadcasting Services Act 1992*, regulating news and journalism content on traditional radio and television broadcasting services
- new powers currently under development that will allow the ACMA to combat online dis- and misinformation.[57]

Concerns Raised

Self-regulation and co-regulation

6.55 Submissions argued that self-regulation through the ACPDM is inappropriate for digital platforms where community needs and public interest are not at the forefront of business practices.[58] For example, the HRLC submitted:

> In the European Union, introduction of the Digital Services Act was driven by growing recognition that self- and co-regulatory models are inadequate and ineffective.[59]

6.56 See Box 6.2 below for details of the EU's approach to disinformation.

6.57 The AMAN noted the current Australian voluntary code has no effective enforcement mechanism when the existing measures are not achieving the desired outcome.[60]

---

[56] DITRDCA, *New ACMA powers to combat misinformation and disinformation*, (accessed 20 October 2023).

[57] DIGI, *Submission 65*, p. 9.

[58] HRLC, *Submission 50*, p. 9; CPRC, *Submission 60*, p, 9.

[59] HRLC, *Submission 50*, p. 9.

[60] AMAN, *Submission 44*, p. 7.

Box 6.2 International approaches

EUs Code of Practice on Disinformation

The EU 2022 Code of Practice on Disinformation is a key component of the EU's strategy to combat disinformation online. It is also a voluntary code. The DITRDCA advised:

> Under the updated Code, signatories commit to action in several domains, including; demonetising the dissemination of disinformation; ensuring the transparency of political advertising; empowering users; enhancing cooperation with fact-checkers; and providing researchers with better access to data.[61]

Additionally, the EU DSA establishes a co-regulatory approach to managing online dis- and misinformation, requiring designated online platforms to have measures in place to mitigate risks from the spread of illegal content.

The DSA is regulated by a new European Board of Digital Services and the European Commission, which will have 'direct enforcement powers and be able to impose fines of up to 6% of a service's global turnover for breaches.'[62]

Content moderation focus inappropriate

6.58 The HRLC also advised measures to address online harm must look beyond content moderation and beyond the current focus, as indicated in transparency reports under the voluntary code, on content takedown and flagging.[63] This approach experiences a lag following identification of material, with action often occurring well after damage is done.[64] The HRLC noted:

> … defining and identifying disinformation and harmful content is difficult, especially in real time and across hundreds of languages and countless societal contexts, and platforms are poorly placed to arbitrate the appropriateness of political content.[65]

6.59 The committee was advised that there are also censorship risks arising from content moderation approaches. The HRLC stated:

> Around the world, there is a growing body of evidence of excessively broad and vague laws becoming tools of governments to compel private companies to police communication in ways that unjustifiably limit public

61 DITRDCA, *Submission 9*, p. 10.

62 ACMA, *Submission 24*, p. 3.

63 HRLC, *Submission 50*, p. 8.

64 HRLC, *Submission 50*, p. 8.

65 HRLC, *Submission 50*, p. 8.

> debate and freedom of expression. Responses to the problem of disinformation, whether on the part of governments, regulatory bodies or platforms themselves, must not infringe upon the right to freedom of expression and the right to access information – two cornerstones of democratic discourse.
>
> Regulation that relies on content moderation can lead to limits on these rights in circumstances where it was never intended. This is because penalising platforms for content-moderation failures incentivises platforms to err on the side of caution, resulting in restrictions on freedom of expression and the right to access information in circumstances well beyond what was contemplated by the regulatory model.
>
> By focusing on content moderation alone, governments miss the opportunity to address the upstream drivers of disinformation and hate speech, which will be far more effective in the long term.
>
> For all these reasons, content moderation ought to be seen as only one part of any comprehensive and effective framework for digital regulation.[66]

6.60 Further, the Developers Alliance emphasised that remedies to misinformation should focus on the users creating the misleading content rather than the platform. It advised:

> We fundamentally believe that users should be accountable for what they post, not platforms. Platforms in turn should be obligated to publish and enforce policies for what is allowable on their service, and to enable their user community to participate in the content moderation process. Platforms should not be placed in the position of being punished for user behavior [sic] that violates their policies if it somehow evades reasonable moderation processes.[67]

6.61 Meta highlighted that it is always conscious of the fine balance between free speech and managing dis- and misinformation when setting its internal policies. Meta approaches misinformation in the following way:

> Our approach to misinformation falls under a three-part framework, and we have provided detail on each of these below:
>
> - **Remove** misinformation that is likely to directly contribute to imminent physical harm, interfere with the functioning of political processes (including voter and census interference), and certain highly deceptive manipulated media.
> - **Reduce** the spread of misinformation that is identified and verified as false by independent third party fact-checkers.
> - Promote authoritative information and develop tools to **inform** our users, so they can make their own decisions on what to read, trust and share.[68]

---

66 HRLC, *Submission 50*, pp. 8–9.

67 Developers Alliance, *Submission 35*, p. 6.

68 Meta, *Submission 69*, p. 12.

Proposed action to address dis- and misinformation

Regulatory intervention

6.62 Some submissions supported regulatory intervention. For example, the HRLC supported the notion that regulator-drafted industry standards should be the norm.[69]

6.63 The Consumer Policy Research Centre noted the voluntary ACPDM was inadequate, proposing that digital platforms be obliged to report their compliance with the code to an adequately resourced regulator that can assess and enforce the code. It stated '[c]ompliance reporting must be transparent so businesses can be publicly accountable for their performance against the obligations'.[70]

6.64 The Special Broadcasting Service Corporation (SBS) also supported regulatory interventions 'to protect the availability of reliable, trusted and impartial news and information'. It noted these features are particularly important in contexts in which distribution platforms (such as Meta) hold monopolistic, or near monopolistic, positions over markets and audiences.[71]

6.65 Google emphasised the need for flexibility in any regulatory response to accommodate changes in the fast-moving digital world and leave room for innovative, adaptable solutions. It noted 'the risk of enshrining into law responses or frameworks that might prove counterproductive or outdated in the months that follow'.[72] Further, Google stated:

> We note that the threat models continue to evolve as bad actors change their attack patterns and Internet uses change over time–remedies that were effective two years ago may not be best suited to the next wave of challenges.[73]

Increase digital media literacy

6.66 Some submissions called for increased digital and media literacy to assist identifying trustworthy online material.[74]

---

69 HRLC, *Submission 50*, p. 9.

70 Consumer Policy Research Centre (CPRC), *Submission 60*, p. 9.

71 Special Broadcasting Service Corporation (SBS), *Submission 3*, p. 6.

72 Google, *Submission 49*, p. 15.

73 Google, *Submission 49*, p. 16.

74 Australian Media Literacy Alliance (AMLA), *Submission 55*, [p. 1]; Australian Medical Association (AMA), *Submission 66*, pp. 5–6; Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA), *Submission 57*, pp. 1, 6; Google, *Submission 49*, p. 15.

6.67 The Australian Media Literacy Alliance (AMLA) defines media literacy as 'the ability to critically engage with media in all aspects of life. It is a form of lifelong literacy essential for full participation in society'.[75]

6.68 The committee was advised by the AMLA that Australia has low digital literacy confidence:

> Research by AMLA core members shows that many adults and children have a low level of confidence in their own media abilities and most say they are not getting support to help them. Just one third of young Australians think they can tell fake news from real news, and almost two thirds (64%) of adults are not confident that can tell if a website can be trusted. Media literacy competency is negatively correlated with being more than 55 years old, having low literacy, living with a disability, having a low income or living in regional Australia. [76]

6.69 The AMLA proposes working with the Australian Government to progress a national media literacy policy, strategy and framework for media literacy. The AMLA explained:

> National approaches support media literacy educators, including schools, libraries, national organisations and media organisations, to work together in a coherent way while allowing for benchmarking over time. The strategy should work across all ages, but include particular attention to adults who were not able to access curriculum resources through schools, and those with lower media literacy skills and include the development of resources, toolkits and networking opportunities.[77]

6.70 Similarly, the Australian Medical Association (AMA) advised digital literacy can enhance overall health literacy. This in turn can be bolstered by enhancing the prominence of reputable health sources such as Health Direct. The AMA noted sites like Health Direct 'need to be the first sites to show up on search browsers … to help counter access to misinformation'.[78]

6.71 The AMA also proposed further Australian Government investment in 'long-term, robust online advertising to counter health misinformation, including on social media channels'.[79] It stated:

> This should include promotion of vaccine safety, as well as campaigns on the health risks associated with alcohol, junk food, online gambling, tobacco and other drugs. We also implore international digital health platforms to

---

75 AMLA, *Submission 55*, [p. 1].

76 AMLA, *Submission 55*, [pp. 1–2].

77 AMLA, *Submission 55*, [pp. 1–2].

78 AMA, *Submission 66*, p. 5.

79 AMA, *Submission 66*, p. 6.

> acknowledge their public health responsibility and work actively to counter health misinformation on their platforms.[80]

6.72 More broadly, the committee was advised by the Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA) that the Australian government needs to work with these organisations 'to provide targeted support for library staff and educators dealing with the impact of new technologies on media and information literacy, alongside resources to support community media literacy'.[81]

Australian content discoverability

6.73 The committee heard that access to Australian content, including television, music, publishing, video games and radio is at risk from algorithmic prominence decisions set by platforms, such as on transactional video-on-demand and subscription services.[82]

6.74 The DITRDCA noted:

> … the ready availability of mass content produced in other countries on streaming services, particularly the United States, risks crowding out the voices of Australian storytellers. Australia's content and cultural sectors also face various issues in how cultural content is made accessible and visible on digital platforms' algorithmically-driven recommendation systems. In particular, the prominence of content on platforms and services can influence users' viewing choices, thereby impacting the success of Australian content.[83]

TV and news journalism

6.75 The ABC advised the committee that its ability to fulfill its role as a national broadcaster, such as its contribution to a range of social and cultural outcomes including trusted independent public interest journalism, is directly related to the ease with which its content and services can be found and accessed by Australians.[84]

6.76 Audience viewing behaviour has shifted to increased use of technology and platforms including the use of aggregated search applications (aggregator apps) such as Apple TV and Google TV. [85]

---

80 AMA, *Submission 66*, p. 6.

81 ALIA and NSLA, *Submission 57*, p. 8.

82 See, for example, ABC, *Submission 4*; DITRDCA, *Submission 9*, p. 12; Screen Producers Australia, *Submission 15*; CRA, *Submission 43*; Free TV Australia, *Submission 17*; Australian Publishers Association, *Submission 56*.

83 DITRDCA, *Submission 9*, p. 4.

84 ABC, *Submission 4*, p. 3.

85 ABC, *Submission 4*, pp. 3–4.

6.77 ABC highlighted that search and recommendation facilities on aggregator apps employ algorithms to determine the prominence of content presented to viewers.[86] Lack of algorithmic transparency means users and content providers alike are unaware of how programs are selected for prominence.[87] ABC commented:

> The ABC provides data about the programs on ABC iview to the aggregator platforms to aid discovery via their aggregated search facilities and expects that, if a search turns up content on ABC iview and the user selects it, the platform will launch the ABC iview app to play it. However, within their apps and devices, Apple and Google are also promoting purchase of their own content through subscriptions or transactional video-on-demand (TVOD) purchases. Search and discovery of free ABC content can be effectively used to promote paid versions of the same programs. Moreover, the Corporation has no way of ensuring that its versions of programs will be most prominently displayed in search results.[88]

Publishers and authors

6.78 ALIA and NSLA raised concerns about prominence decisions made by algorithms and the impacts on Australian creators and authors. They argued in favour of increased transparency:

> Algorithmic transparency may be particularly important when applied to vertically integrated platforms. Platforms that act as producer, seller and distributor have an inbuilt incentive to promote their own products. For libraries concerned with creation of accurate, quality and local content, this is concerning. A very simple example is the way that platforms may promote international bestsellers or "homebrand" author content which is either cheaper to produce or in which they get a larger profit margin, over Australian creators. Lack of algorithmic transparency means that it is not possible to see the extent to which Australian authors being disadvantaged, and consumers are often unaware that the results that they see are the result of priorities and decisions made to maximise profits.[89]

6.79 The Australian Publishers Association noted similar concerns:

> A continued concern is that algorithms of retailers do little to support or make visible Australian cultural content. Given the number of books that are released globally in any year and available at any one time, there is a clear national value in Australian content being foregrounded and visible.[90]

6.80 The committee was advised by DRW that platforms' algorithmic decisions:

---

86 ABC, *Submission 4*, p. 3.

87 ABC, *Submission 4*, p. 4.

88 ABC, *Submission 4*, p. 4.

89 ALIA and NSLA, *Submission 57*, p. 6.

90 Australian Publishers Association, *Submission 56*, p. 3.

> … can have the effect of flattening out the diversity of content, instead promoting and recommending the most popular, dominant content, often at the detriment of smaller, independent creatives and artists.[91]

6.81 This is visible on streaming services, such as Spotify and Netflix, and with books on Amazon or Audible.[92]

Music and radio

6.82 In the realm of music content streaming, the DITRDCA advised:

> There are crossover issues between algorithmic transparency, and discoverability and availability of Australian music on music streaming services.[93]

6.83 The DITRDCA is exploring 'how Australian content can be more easily and readily accessed on music streaming services'. This would include:

> … the role that streaming service algorithms play in accessibility and discoverability. Algorithmic transparency is also likely to be a priority for Australian music content creators as they aim to improve their revenue streams.[94]

6.84 Commercial radio has an important role in providing 'local content, news and emergency information to Australians who receive no other local free to air broadcast content.'[95] It also plays a socially inclusive role, engaging with local communities and supporting Australian stories and voices.[96]

6.85 Commercial radio has strict legislated Australian content requirements, including minimum hours of hyper-local content broadcasts by regional stations, and rules for local staffing, facilities and news content in the event of a change of control. Commercial radio stations are also required under their Code of Practice to play minimum amounts of Australian music, including a portion of work by new artists.[97]

6.86 Despite these important roles, Australian commercial radio is also affected by the prominence decisions of platforms. Commercial Radio & Audio advised that listening over connected devices represents an increasing portion of radio listenership. It stated:

> If radio is not afforded prominence on these devices, it may face significant challenges. Prompt action must be taken to protect Australian radio long

---

91 DRW, *Submission 68*, p. 27.

92 DRW, *Submission 68*, p. 27.

93 DITRDCA, *Submission 9*, p. 13.

94 DITRDCA, *Submission 9*, p. 13.

95 CRA, *Submission 43*, p. 10.

96 CRA, *Submission 43*, p. 13.

97 CRA, *Submission 43*, p. 11.

> term, given the rapid growth of connected devices, particularly in vehicles and smart speakers.[98]

National Cultural Policy

6.87 The DITRDCA has a policy and program development and delivery role under the National Cultural Policy.[99]

6.88 In January 2023 the Australian Government released *'Revive: a place for every story, a story for every place'* (Revive) – Australia's National Cultural Policy for the next five years.[100]

6.89 Among other requirements, Revive 'introduces requirements for streaming services to ensure continued access to Australian screen content' and 'commits to Government action to ensure Australian music is "visible, discoverable and easily accessible across platforms to all Australians"'.[101]

6.90 The DITRDCA's submission stated:

> Discoverability of Australian music content on streaming platforms and services is vital for Australian artists that distribute their music online, and compete with internationally recognised artists both abroad, and even in Australia.[102]

Prominence framework

6.91 The committee was advised that the government has committed to introducing a prominence framework for broadcaster video-on-demand 'to ensure local TV services are easy for Australian audiences to find on connected TV devices.'[103] However, this framework will not apply to the use of the algorithms on computing devices. [104]

6.92 ABC suggested an expansion of the prominence framework could be considered as part of the framework review following its first year of operation.[105]

---

98 CRA, *Submission 43*, p. 7.

99 DITRDCA, *Submission 9*, p. 5.

100 DITRDCA, *Submission 9*, p. 12

101 DITRDCA, *Submission 9*, p. 12

102 DITRDCA, *Submission 9*, p. 5.

103 See, for example, ABC, *Submission 4*, p. 3; CRA, *Submission 43*, p. 1; DITRDCA, *Prominence for connected TV devices*, www.infrastructure.gov.au/media-communications-arts/television/prominence-connected-tv-devices (accessed 5 October 2023).

104 ABC, *Submission 4*, p. 3.

105 ABC, *Submission 4*, p. 4.

Targeted advertising and harmful product marketing

6.93 Algorithms drive decisions around users' exposure to particular advertising and can therefore give rise to safety issues directly affecting children, young people and vulnerable users.[106]

6.94 eSafety noted it is difficult to measure the severity of harms caused by algorithmic decisions about online advertising as some types of content may be harmful only to a limited group of people and communities, such as dieting ads.[107]

6.95 These concerns are discussed further in Chapter 8: Online safety.

Lack of transparency

6.96 The overarching concern with algorithm use and ADM processes by digital platforms is a lack of transparency around the inputs, assumptions and intended purpose of particular algorithms or ADM.[108]

6.97 eSafety advised:

> While the use of algorithms offer social and economic benefits, their design and purpose can be opaque, and they can be also exploited by users (both businesses and individual end-users) as well as the digital platform, resulting in harm to some individuals.[109]

6.98 AMLA emphasised the importance of transparency for consumers, including the need for accessible information on if and how consumers can control or influence advertising and personalised content they are exposed to.[110] AMLA stated:

> Transparency plays an important role in enabling Australians to productively engage with digital media. Many Australians do not understand why they see what they see, as the algorithms that determine what content is served to whom, and based on what data, are invisible.[111]

6.99 The HRLC noted a lack of voluntary transparency from platforms around their algorithm use:

> The Australian public currently has few meaningful opportunities to ever understand how platforms and algorithms shape the information environment in which we form views and make decisions. It is largely thanks to industry whistleblowers that we have achieved any scrutiny and

---

106 eSafety, *Submission 2*, p. 4.

107 eSafety, *Submission 2*, p. 4.

108 See, for example, eSafety, *Submission 2*, p. 4; ABC, *Submission 4*, pp. 2–3; SBS, *Submission 3*, pp. 8–9; Mr Joshua Zubak, *Submission 27*, p. 5.

109 eSafety, *Submission 2*, p. 2.

110 AMLA, *Submission 55*, [p. 3].

111 AMLA, *Submission 55*, [p. 3].

> accountability for the big tech companies. Now and into the future, we should not need to rely on whistleblowers in order to understand the ways we are tracked and targeted, and the systems that determine the information that is delivered to us.[112]

6.100 Further, CHOICE highlighted that the existence and use of ADMs is often hidden from consumers. It noted that:

> This limits the ability of consumers to provide consent and restricts the ability of regulators and government to assess algorithms. The use of ADM by business should be clearly disclosed on consumer-facing platforms like websites or apps. ADM should also be disclosed in privacy policies in plain language, and should be available for regulators to audit.[113]

6.101 eSafety welcomed the initial efforts by industry to increase transparency but noted they are limited and do not offer substantive explanations of the ways in which algorithms may or may not contribute to online harms.[114]

Transparency risks

6.102 The committee also heard some concerns about the risks of sharing details about particular algorithm design, including potential manipulation or exploitation of the algorithms by users, businesses, or bad actors.[115]

6.103 eSafety noted:

> While eSafety appreciates the significance of minimising the opportunity for key algorithms to be 'gamed' by businesses or bad actors, it is important to ensure that digital platforms are accountable for the impact of their design choices and that users are empowered to make informed decisions.[116]

Current regulatory measures

6.104 Currently, there is no comprehensive mechanism to assess the measures implemented by digital platforms to address harms arising from algorithm and ADM use.

6.105 There is ongoing work across government and a number of mechanisms that target specific 'problem areas'. For example, the government is progressing work to better understand the operation of algorithms on digital platforms which 'will also consider findings from other work underway across Government throughout 2023'.[117] Work in progress includes:

---

112 HRLC, *Submission 50*, p. 10.

113 CHOICE, *Submission 54*, p. 3.

114 eSafety, *Submission 2*, p. 4.

115 See, for example, eSafety, *Submission 2*, p. 4; Developers Alliance, *Submission 35*, p. 3.

116 eSafety, *Submission 2*, p. 4.

117 Australian Government, *Response to the House of Representatives Select Committee on Social Media and Online Safety report*, March 2023, p. 16.

- the Attorney General's Department preparing a response to the *Privacy Act Review Report 2022*;
- the Digital Platforms Regulators Forum undertaking a literature review examining algorithms, including in recommender systems, content moderation and targeted advertising, 'to enhance members' understanding of associated regulatory risks';[118]
- the Department of Industry, Science and Resources conducting a review of AI regulation and ADM.[119]

6.106 This work will culminate in a joint report to government by the first quarter of 2024 including:

> … options to build capability around future algorithm research and expertise, and with advice on whether Government regulation of algorithms is required and, if so, what options for regulation are available.[120]

6.107 eSafety advised that it is undertaking a number of regulatory steps 'with the aim of increasing platforms' transparency and accountability in relation to how algorithms can impact user safety, including exercising new powers under the OSA [Online Safety Act]'.[121]

6.108 The DITRDCA also advised:

> Noting the need for a consideration of algorithms to be aligned across Government, the Department has commenced preliminary work with other agencies to consider the type and scale of harms as a result of algorithmic use, as well as the current transparency levels of various algorithms.[122]

The argument for change

6.109 eSafety explained:

> Given the complex, evolving, and dynamic nature of algorithms and their use in the online environment, there is no single, fixed regulatory approach to address their potential benefits and harms.[123]

6.110 The DITRDCA noted the concerns raised in the Final Report of the House of Representatives Select Committee's Inquiry into Social Media and Online Safety

---

118 Australian Government, *Response to the House of Representatives Select Committee on Social Media and Online Safety report,* March 2023, p. 16.

119 Australian Government, *Response to the House of Representatives Select Committee on Social Media and Online Safety report,* March 2023, p. 16.

120 Australian Government, *Response to the House of Representatives Select Committee on Social Media and Online Safety report,* March 2023, p. 16.

121 eSafety, *Submission 2*, p. 2.

122 DITRDCA, *Submission 9*, p. 5.

123 eSafety, *Submission 2*, p. 5.

about 'the opaqueness of algorithms, which has the potential to heighten harms associated with them'.[124] The DITRDCA noted:

> The Committee was of the view that a statutory requirement for platforms to provide the details of how they are working to minimise harms caused by algorithms would increase transparency without compromising commercially sensitive information. The Department is developing advice to the Government about the Committee's findings.[125]

6.111 The committee was advised that the *Privacy Act Review Report 2022* makes proposals relating to algorithmic transparency and DIGI indicated these proposals should be contemplated in the context of the ongoing Government work on AI and ADM.[126]

6.112 The Foundation for Alcohol Research and Education also raised the need to 'implement mandatory requirements for digital platforms to make advertising information accessible, including their data practices and automated decision systems'.[127]

Possible solutions

International approaches of interest

6.113 Internationally, policy makers and regulators are attempting to address the same concerns as Australia in relation to online safety and algorithmic transparency.

6.114 Common approaches include increasing transparency and accountability, risk-based regulatory regimes, and systematic reporting requirements.[128]

6.115 eSafety highlighted the following key international frameworks:

- The UK Algorithmic Transparency Standard for use of algorithmic tools in government decision making:

  > The UK Central Data and Digital Office (CCDO) has developed the Algorithmic Transparency Standard, a recording standard that helps public sector bodies provide clear information about the algorithmic tools they use and why they are using them. The Standard is one of the world's first policies for transparency on the use of algorithmic tools in government decision making and is internationally renowned as best practice.[129]

---

124 DITRDCA, *Submission 9*, p. 5.

125 DITRDCA, *Submission 9*, p. 5.

126 DIGI, *Submission 65*, p. 2.

127 Foundation for Alcohol Research and Education, *Submission 33*, p. 5.

128 eSafety, *Submission 2*, p. 9.

129 eSafety, *Submission 2*, p. 9.

- The EU DSA:

> The DSA includes data access obligation and transparency measures for major digital platforms, which extends to the algorithms used for recommending content or products to users.[130]

6.116 The European Centre for Algorithmic Transparency supports enforcement of the DSA:

> It contributes scientific and technical expertise to the Commission's exclusive supervisory and enforcement role of the systemic obligations on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) provided for under the DSA.[131]

Risk-based framework

6.117 Evidence to the committee emphasised the need for a risk-based regulatory model.

6.118 For example, DIGI advised it 'agrees with the need for risk-based frameworks to prevent and address issues related to the use of Artificial Intelligence (AI) and Automated Decision Making (ADM), such as preventing discrimination'.[132]

6.119 The HRLC argued for a comprehensive transparency framework:

> … regulation should be focused on increasing transparency and accountability. Transparency features of an appropriate regulatory model should place the onus on digital platforms to identify the risks posed by their platforms and the steps they will take in response, as well as providing information to users about their advertising and recommender systems. These obligations should be reinforced by a well resourced, independent regulator with the power to verify digital platforms' information, and hold them accountable for failures to report and act.[133]

6.120 CHOICE further highlighted that:

> Consumers do not have strong protections from business' use of harmful ADM practices. The Federal Government should legislate a risk-based ADM framework, with restrictions and prohibitions on harmful use. This can be achieved either by:
>
> (a) expanding Office of the Australian Information Commissioner's (OAIC) Privacy Impact Assessment compliance scheme to cover private businesses and to incorporate a risk-based framework on ADM; or

---

130 eSafety, *Submission 2*, p. 9.

131 European Commission, *European Centre for Algorithmic Transparency*, https://algorithmic-transparency.ec.europa.eu/about_en (accessed 1 November 2023).

132 DIGI, *Submission 65*, p. 2.

133 HRLC, *Submission 50*, p. 10

(b) establishing separate legislation which regulates the use of artificial intelligence including ADM.[134]

6.121 The HRLC supported regulator-drafted industry standards as the norm.[135]

Lead regulator

6.122 The OAIC advised the committee that consideration should be given to whether existing bodies could be resourced to take on any new regulatory activities in relation to algorithms. It noted:

> Given the work already taking place to regulate algorithms and the range of existing regulatory bodies operating in relation to digital platforms, careful consideration should be given to whether establishing an oversight body would be the most appropriate model.[136]

6.123 The Centre for AI and Digital Ethics supported enhancing the ACCC and the ACMA's investigative capacity by expanding in-house technical research and data science expertise, to facilitate independent investigations and better discharge their regulatory duties.[137] Noting the ACCC holds a similar role to the US Federal Trade Commission (FTC), the Centre for AI and Digital Ethics advised:

> We highlight the FTC's recent announcement of an Office of Technology which will hire individuals with backgrounds in technology to augment the FTC's consumer protection and antitrust missions. We advocate for a similar expansion of capabilities at the ACCC and support the parallel appointment of a Chief Technologist.[138]

6.124 CHOICE similarly advised that:

> The Federal Government should empower an existing regulator with the adequate resources and expertise to regulate ADM. The regulators most suitable for this role would be the ACCC or OAIC. Without strong regulators, consumers may be unfairly discriminated against, excluded, and profiled by ADM systems.[139]

Key features for regulatory intervention

6.125 eSafety noted some general principles for any regulation or oversight of algorithms:

> Any regulation or oversight of algorithms should safeguard the rights of users, preserve the benefits of these systems and foster healthy innovation.

---

134 CHOICE, *Submission 54*, p. 3.

135 HRLC, *Submission 50*, p. 9.

136 OAIC, *Submission 61*, p. 6.

137 Centre for AI and Digital Ethics, *Submission 23*, [p. 1].

138 Centre for AI and Digital Ethics, *Submission 23*, [p. 3].

139 CHOICE, *Submission 54*, p. 3.

Important considerations for regulatory efforts targeted at algorithms include:

- harmonising efforts across global government agencies to avoid a fragmented regulatory environment and unnecessary duplication
- understanding the underlying ad-based revenue models which many large digital platforms employ and aligning incentives so that safety considerations are considered in tandem with business incentives
- enhancing education and algorithmic literacy in recognition of the fast-paced nature of technology and that regulation alone is not able to remove all risks.[140]

6.126 The ABC drew attention to features of the EU's DSA, which call for greater algorithm transparency and intend to hold platforms to account for the societal harms stemming from the use of their services. The ABC noted that these provisions appear to 'provide some positive elements that could be reflected in any potential Australian regulatory model'.[141]

6.127 The Tech Council of Australia advised that the EU General Data Protection Regulation 'provides a right to meaningful information about the logic involved in automated decisions, such as those used in recommendations systems, credit and insurance risk systems, advertising programs and social networks'. It noted that the Attorney-General's Department has recommended a similar right in the Privacy Act Review, alongside other transparency requirements that would apply to ADM.[142]

Algorithm code reviews

6.128 The committee was advised by eSafety that code or pseudo-code reviews are not a practical solution given the expertise and time required and the ever-changing nature of the codes.[143] Clear legislative mandates would be required to support the associated access to potentially sensitive user data and the process employed to conduct the reviews.[144]

140 eSafety, *Submission 2*, p. 5.

141 ABC, *Submission 4*, p. 3.

142 Tech Council of Australia, *Submission 63*, p. 10.

143 eSafety, *Submission 2*, p. 6.

144 eSafety, *Submission 2*, p. 6.

Data access regime/public interest research

6.129 Evidence to the committee indicated a high level of support for transparency around advertising, recommender and content moderation systems for public interest research.[145]

6.130 This is a key feature of the EU's DSA and was noted by a range of submitters. For example, the HRLC advised:

> Under the DSA, on request from the relevant regulator, platforms are required to provide external researchers with access to data for the purposes of conducting research on detection, identification and understanding of the systemic risks to which risk assessments apply, and assessment of the adequacy, efficiency and impacts of platforms risk mitigation measures. This data access regime is another significant feature of the DSA, and reinforces commitments made by signatories to the EU's Strengthened Code of Practice on Disinformation.[146]

6.131 The HRLC further noted:

> Concerns raised by digital platforms about the implications of sharing their data with governments and researchers – such as privacy and exploitation concerns – are legitimate, but they are also surmountable. Rather than allowing these concerns to outweigh the critical value of transparency, they should be addressed through appropriate safeguards for protecting sensitive data.[147]

6.132 The Centre for AI and Digital Ethics also supported protections for public interest research and enhancements to the regulator's analytical and investigative capacities to combat the spread of dis- and misinformation. It noted that '[r]esearchers investigating harms of digital platforms have in the past been subject to reprisals and hindrances by the platforms themselves'.[148] It stated:

> We support the introduction of mandatory reporting and disclosure laws for Big Tech companies, protections for public interest research, and enhancements to regulator's [sic] analytical and investigative capacities, to combat the spread of mis- and dis-information on digital platforms.[149]

---

[145] See, for example, ALIA and NSLA, *Submission 57*, p. 8; HRLC, *Submission 50*, p. 11; Centre for AI and Digital Ethics, *Submission 23*, [p. 15]; AMAN, *Submission 44*, p. 18; Gesellschaft Für Freiheitsrechte, *Submission 25*, pp. 3–4.

[146] HRLC, *Submission 50*, p. 11.

[147] HRLC, *Submission 50*, p. 11.

[148] Centre for AI and Digital Ethics, *Submission 23*, [p. 15]

[149] Centre for AI and Digital Ethics, *Submission 23*, [p. 3]

Chapter 7
Consumer harms

Scams, harmful apps and fake reviews

Overview

7.1 Increasing use of online platforms has provided a low-cost avenue for scammers and harmful apps to reach substantial numbers of consumers and businesses.

7.2 Submissions raised significant concern about the growing proliferation of online scams and other harms.[1] The committee was advised that:

> Trust and confidence in the digital economy are essential. Consumers and businesses will only embrace digital opportunities if they are confident they can trust the technologies and the entities with which they interact online. Recent rapid growth in scams and fraud is undermining this confidence.[2]

7.3 This chapter considers the nature and scale of intentionally harmful activities taking place on digital platforms, current regulatory measures, the responsibilities and roles of digital platforms and adequacy of their current approaches, and potential mechanisms to address growing concerns.

7.4 Online safety risks beyond scams, harmful apps and fake reviews, particularly risks for children, are discussed in Chapter 8: Online safety.

7.5 The committee notes the considerable body of investigative work undertaken by the Australian Competition and Consumer Commission (ACCC) in this field and draws on its research.

Scams

7.6 The committee was advised that the impact on Australians of scams originating from digital platforms is 'disproportionately higher than other channels'.[3] The Commonwealth Bank of Australia highlighted:

> Recent analysis from the Australian Financial Crimes Exchange shows that digital platforms, whether they be web or app based, account for close to

---

1 See, for example, Free TV Australia, *Submission 17*, p. 13; Match Group, *Submission 73*, p. 6; Commonwealth Bank of Australia (CBA), *Submission 71*, p. 4; Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *Submission 39*; Meta, *Submission 69*, p. 40.

2 CBA, *Submission, 71*, p. 4.

3 CBA, *Submission, 71*, p. 4.

> half of scams exposures yet only approximately 20% of all scams origination.[4]

7.7 Given the broad range of online scams utilising a variety of approaches, anyone can be a victim of scams. Approaches may include:

> … dating and romance scams, identity theft, unexpected money or winnings, threats and extortion, job recruitment, investments, charities, phishing, hacking, remote access scams and attempts to gain personal information, e-commerce scams, and telephone and messaging scams.[5]

7.8 The ACCC highlighted how scams often utilise multiple services to defraud victims, with digital platforms, like telecommunications services, situated at the start of the 'scam chain of events'. It found:

> The ACCC has received increasing numbers of reports to Scamwatch where victims were targeted via a digital platform service, then drawn to an encrypted messaging app, before being induced to make payments through a bank or cryptocurrency service.[6]

Scale of the problem

7.9 Financial losses from online scams, such as those conducted via social media platforms and mobile apps, are currently responsible for a small proportion of the total losses from scams but continue to grow.[7]

7.10 The ACCC outlined that financial losses reported to Scamwatch significantly increased between 2020 ($49 million) and 2021 ($92 million). Similarly, the ACCC's review of Scamwatch data 'shows that reported losses to scams in 2022 on social networks increased by approximately 42% and on mobile apps by approximately 98%'.[8] Actual losses are likely much higher, given only 13 per cent of victims are estimated to report their losses to Scamwatch.[9] Box 7.1 elaborates on cryptocurrency scams.

---

4 CBA, *Submission 71*, p. 4.

5 Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), *Submission 9*, p. 10.

6 Australian Competition and Consumer Commission (ACCC), *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 74.

7 DITRDCA, *Submission 9*, p. 10.

8 Australian Communications Media Authority (ACMA), *Submission 24*, p. 4.

9 ACCC, *Submission 8*, p. 6; Australian Communications Consumer Action Network (ACCAN), *Submission 20*, p. 1.

Box 7.1 Case study: cryptocurrency scams

Cryptocurrency scams are particularly on the rise, with consumer reports to the ACCC and Scamwatch data suggesting many investment scams use digital platform services to target victims.[10]

The Centre for AI and Digital Ethics highlighted:

> … cryptocurrency investment scams were the "main driver" of the sharp 35% increase in investment scam losses in 2021 from the previous year, with Australians reporting $99 million lost to these scams.[11]

The ACCC noted 'cryptocurrency was also the most common payment method for investment scams'.[12]

Fake advertising is also a feature of cryptocurrency scams. Free TV Australia advised that images of well know TV presenters such as Karl Stefanovic and David Koch have been used in fake endorsements to lure social media users into scam cryptocurrency investments.[13]

The Centre for AI and Digital Ethics proposed cryptocurrency investments and investments in blockchain products be restricted to 'sophisticated investors':

> … where such investments have not met a bar similar to those faced by ordinary issuers of securities, to avoid the proliferation of scams and fraudulent activity that current characterises the market for these digital assets.[14]

The Developers Alliance noted:

> Cryptocurrency regulation is rapidly evolving as fraud and speculation emerge as fundamental drivers of adoption. We would simply highlight that virtual transactions and payments are here to stay, and that confidence in these processes and systems is fundamental to economic stability and growth.[15]

---

10 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 75.

11 Centre for AI and Digital Ethics, *Submission 23*, [p. 7].

12 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 75.

13 Free TV Australia, *Submission 17*, pp. 13–14. Also see Casey Briggs, 'Inside the world of fake ad scams stealing the identities of Kochie and celebrities like him around the world', *ABC News*, 6 November 2023.

14 Centre for AI and Digital Ethics, *Submission 23*, [p. 2].

15 Developers Alliance, *Submission 35*, [p. 5].

Fake reviews

7.11 Fake or manipulated reviews are also a cause of significant harm to consumers and small businesses. The ACCC noted in its Regulatory Reform Report:

> … as Australians spend more time and money online, consumers and small businesses are more reliant on online reviews and more vulnerable to harms from fake or manipulated reviews.[16]

7.12 Fake reviews are instigated by a range of actors, from malicious actions by past employees or competitors[17] through to commercial service providers generating hostile fake reviews for existing providers to support consumer traction for new entrants.[18]

7.13 Fake reviews have significant impacts on the businesses, products and markets they target, such as:

- undermining consumer choice;[19]
- distorting competition;[20]
- causing financial losses for small business owners if they are targeted;[21]
- causing reputational damage and impacting future customers;[22]
- undermining credibility of legitimate small businesses;[23] and
- small business being held to ransom by scammers seeking payment for review removal.[24]

Current regulation

Limitation of current regulations

7.14 The committee was advised that current regulations do not adequately capture digital platforms' role with respect to scams, fake reviews and harmful apps. The regulations have not kept pace as scammers pivot from phone call and text message scams to social media and other applications.[25]

---

16 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 73.

17 NSW Small Business Commissioner, *Submission 6*, p. 2.

18 ASBFEO, *Submission 39*, [p. 2].

19 ACCC, *Submission 8*, p. 6.

20 ACCC, *Submission 8*, p. 6.

21 ACCC, *Submission 8*, p. 6.

22 NSW Small Business Commissioner, *Submission 6*, p. 2.

23 NSW Small Business Commissioner, *Submission 6*, p. 2.

24 ASBFEO, *Submission 39*, [p. 2].

25 ACMA, *Submission 24*, p. 4.

7.15 The ACCC noted that additional measures are required to supplement the essential role of Australian Consumer Law (ACL) in a manner more targeted to digital platforms, in light of the scale of harm from online scams, harmful apps and fake reviews.[26]

7.16 The ACCC further highlighted that the *Competition and Consumer Act 2010* and the ACL 'are not well-suited' to digital platform services given '[e]nforcement of these laws is also necessarily retrospective, addressing particular instances of conduct on a case-by-case basis after harms have already occurred'.[27]

7.17 Lengthy redress processes cause further damage to small businesses where fake reviews or fraudulent misrepresentation of a business remain visible on a platform during investigation processes.[28] ASBFEO noted:

> This can impact not only business viability but the mental health of the small business operator and their employees.[29]

7.18 New protections which came into effect in 2022 'requiring telecommunications providers to identify, trace and block SMS scams' saw around 90 million scams SMS blocked in the first six months of operation.[30] However, these new protections do not apply to digital platforms and cannot be extended under current laws.[31] The ACMA advised:

> Digital platforms and messaging applications that are not required to prevent scams on their service will become an increasingly attractive target for scammers.[32]

7.19 Small businesses are particularly vulnerable to intentional online harms as they lack resources to identify and counter scams[33] and encounter difficulties accessing processes to verify and remove fake reviews.[34]

National anti-scams centre

7.20 The Australian Government has committed to introducing strengthened measures to combat scams.[35]

---

26 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 74.

27 ACCC, *Submission 8*, p. 4.

28 ASBFEO, *Submission 39*, [p. 3].

29 ASBFEO, *Submission 39*, [p. 3].

30 ACMA, *Submission 24*, p. 4.

31 ACMA, *Submission 24*, p. 4.

32 ACMA, *Submission 24*, p. 4.

33 ASBFEO, *Submission 39*, [pp. 1–2].

34 NSW Small Business Commissioner, *Submission 6*, p. 2.

35 DITRDCA, *Submission 9*, p. 11.

7.21 Establishment of the National Anti-Scams Centre (NASC) as part of the ACCC in July 2023 is one such initiative, helping to coordinate efforts across those government agencies with a role in preventing scams. The NASC noted that it works 'together with government, industry, other regulators, law enforcement bodies and community organisations to make it more difficult to scam Australians'.[36]

7.22 Noting the significant losses from investment scams, the first NASC 'fusion cell' (time-limited taskforce) intends to focus on these and aims to identify methods for disrupting investment scams to minimise scam losses. Future fusion cells will target other particular scam types.[37]

Scamwatch

7.23 Scamwatch is a program run by the NASC to collect reports about scams from businesses and consumers. Scamwatch uses this information to help issue warnings and to take action to stop scams.

7.24 Scamwatch also provides guidance and up-to-date information to help the community identify and avoid scams[38] such as advice for dealing with impersonation of a business online.[39]

Platform responsibilities and practices

7.25 The committee heard from some digital platforms about the systems they have in place to combat scams and harmful apps.

7.26 Ms Mia Garlick, Regional Director of Policy, Meta, advised that Meta works hard to combat scams at all levels, working with regulators in different countries to share information and seek redress for customers.[40] Meta stated:

> In October 2022, we reported that we had identified more than 400 malicious android and iOS apps that were designed to steal Facebook login information and compromise people's accounts. These apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors,

---

36 Australian Government, National Anti-Scam Centre, *Scamwatch*, 'About us', www.scamwatch.gov.au/about-us (accessed 2 November 2023).

37 ACCC, *National Anti-Scam Centre's first fusion cell to disrupt investment scams*, www.accc.gov.au/media-release/national-anti-scam-centres-first-fusion-cell-to-disrupt-investment-scams (accessed 2 November 2023).

38 Australian Government, National Anti-Scam Centre, *Scamwatch*, 'About us', www.scamwatch.gov.au/about-us (accessed 2 November 2023).

39 Australian Government, National Anti-Scam Centre, *Scamwatch*, 'Advice for dealing with impersonation of your business online', www.scamwatch.gov.au/research-and-resources/resources/advice-for-dealing-with-impersonation-of-your-business-online (accessed 2 November 2023).

40 *Proof Committee Hansard*, 22 August 2023, p. 18.

> games, VPN services, business apps and other utilities to trick people into downloading them.
>
> We've reported these malicious apps to our peers at Apple and Google and they have been taken down from both app stores. We also alerted people who may have unknowingly self-compromised their accounts by downloading these apps and sharing their credentials, and are helping them to secure their accounts.[41]

7.27 Meta outlined how its Community Standards 'prohibit inauthentic accounts or behaviour that intends to mislead users',[42] stating:

> … we use a combination of system and human review to detect and enforce against those who perpetrate cyber security risks.
>
> As bad actors have become more sophisticated, so too have our efforts to detect and enforce against them. In recent years, we have invested significantly in artificial intelligence to detect harmful content and accounts, before a user needs to see it.[43]

7.28 Meta believes it has greater than 99 per cent efficacy removing fake accounts before they are publicly identified.[44]

7.29 Apple highlighted the safeguards provided by its developer verification process:

> To develop and install apps on iOS or iPadOS, developers must register with Apple giving their real-world identity. This ensures that apps on the App Stores are submitted by identifiable persons or organisations and deters the creation of malicious apps.[45]

Inadequacy of current approaches

7.30 The ACCC's Regulatory Reform Report noted current action by digital platforms against scams, harmful apps and fake reviews is not adequate. It stated:

> Digital platforms that host or otherwise act as intermediaries between scammers and their victims are in a unique position to identify and stop scams and harmful apps, and are well placed to remove harmful apps. However, platforms are relatively free to choose how they deal with these issues, and the ACCC considers that platforms could do more to protect consumers. This includes providers of search, social media, online private

41 Meta, *Submission 69*, p. 41.

42 Meta, *Submission 69*, p. 40.

43 Meta, *Submission 69*, p. 40.

44 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 18.

45 Apple, *Submission 70*, p. 9.

messaging, app store, online retail marketplace and digital advertising services.[46]

7.31 The ACCC highlighted it was particularly concerned about the following failings in current digital platform processes:

- **Failure to act on user reports:** platforms have at times failed to remove scams, harmful apps and fake reviews when notified by consumers, businesses, media, and other concerned parties (for example, public figures whose identities have been misused).
- **Inadequate business user verification systems:** scammers continue to proliferate fraudulent pages on digital platforms, including pages impersonating public figures and legitimate businesses. Not only does this harm consumers, but it also harms those public figures and businesses that have been impersonated.
- **Platforms hosting ads for investment scams:** digital platforms continue to host insufficiently vetted ads that direct consumers to investment scams.
- **Platforms providing insufficient detail about what verification steps they use for reviews, if any:** many platforms do not inform consumers about whether they have measures to check or verify the legitimacy of reviews and if so, what those measures are. This prevents consumers from making informed choices based on the most reliable sources.
- **Inconsistent and vague transparency reporting by digital platforms:** digital platforms' voluntary transparency reports do not allow consumer advocacy groups or regulators to effectively evaluate their consumer protection strategies or provide sufficient accountability to users.[47]

7.32 Many of these concerns were echoed in submissions to the committee.

7.33 Free TV Australia (Free TV) emphasised the need for digital platforms, particularly social media platforms, to take more responsibility to ensure 'material which they have the ability to control (and accordingly which they have the ability to remove from their sites) is not fake, damaging, misleading or defamatory'.[48]

7.34 Digital platforms have drawn criticism and been subject to legal proceedings in relation to inadequate takedown processes for fake and misleading advertising.[49] For example, the ACCC commenced proceedings against Meta in 2022 in relation to the publication of scam ads featuring prominent Australians

---

46 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, pp. 45–46.

47 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 82.

48 Free TV Australia, *Submission 17*, p. 23.

49 Free TV Australia, *Submission 17*, p. 13.

without their consent. Free TV highlighted that digital platform takedown processes remain inadequate despite this action.[50]

7.35 Further, Free TV advised that platforms are persistently slow to respond to takedown requests.[51] It submitted:

> Fake ads continue to quickly reappear after they are taken down. These inadequate takedown processes damage the business reputations of broadcasters and also the personal reputations of the celebrities and media personalities that are misrepresented.[52]

7.36 The NSW Small Business Commissioner similarly noted:

> Requiring digital platforms to prevent and remove fake reviews, scams and harmful apps in a timely fashion would be an important step in ensuring digital platforms provide a credible space for small businesses to sell goods and services. Stronger protections requiring platforms to do so is justified given they hold a gatekeeper role and are the only party that is able remediate a fake, misleading or deceptive review. The Commission has heard from many small businesses who have faced long delays in their attempts to have fake removed and difficulty in locating who to speak to within a platform to make such requests.[53]

7.37 Match Group (Match) asserted that the dominant positions of Apple and Google in the provision of in-app payment processing services created 'little incentive to develop new features to combat scams or otherwise protect consumers'.[54]

7.38 Match further advised that mandatory in-app payment system tying by Apple and Google restricts the user data available to app developers, therefore hindering the ability of app developers to detect and respond to scams and keep bad actors off their services.[55]

7.39 DITRDCA also raised concerns that platforms and digital services can 'inadvertently profit from scams occurring across their services, either directly through the sale of ad space for fraudulent products or services, or indirectly through commissions on apps and sales'.[56]

---

50 Free TV Australia, *Submission 17*, p. 23; Casey Briggs, 'Inside the world of fake ad scams stealing the identities of Kochie and celebrities like him around the world', *ABC News*, 6 November 2023.

51 Free TV Australia, *Submission 17*, pp. 13–14.

52 Free TV Australia, *Submission 17*, p. 13.

53 NSW Small Business Commissioner, *Submission 6*, pp. 2–3.

54 Match Group, *Submission 73*, p. 13.

55 Match Group, *Submission 73*, Appendix 2 (Match Group, 'Response to the Government consultation on the ACCC's regulatory reform recommendations for digital platforms', *Submission by Match Group Inc. to Treasury*), p. 3.

56 DITRDCA, *Submission 9*, p. 10.

Possible solutions

7.40 Some submissions provided overarching commentary and highlighted additional considerations when reflecting on how best to tackle intentional online harms.

7.41 Meta called for action by the government and regulators against scammers on online platforms and other communications services, particularly in pursuing legal action against scammers.[57] It noted that 'creating real world consequences for scam advertisers and other bad actors … is important to maintain the integrity of our services'.[58]

7.42 The CBA noted the need for shared responsibility by all industry players to prevent and mitigate harms from scams.[59]

7.43 Finally, Match emphasised the need for consultation with the eSafety Commissioner on any measures to address scams, harmful apps and fake reviews.[60]

7.44 In addition to measures to protect digital platform users where a power imbalance exists, such as adequate internal dispute resolution processes and escalation options[61] (discussed in Chapter 4: Bargaining imbalances), the ACCC emphasised in its Regulatory Reform Report that mandatory processes should apply to all relevant digital platforms 'to prevent and remove scams, harmful apps, and fake reviews on the platforms' services'.[62]

7.45 The ACCC outlined that mandatory processes should include:

- a notice-and-action mechanism
- verification of certain business users
- additional verification of advertisers of financial services and products
- improved review verification disclosures
- public reporting on mitigation efforts.[63]

7.46 It further outlines that these measures should apply, at a minimum, to:

- search, social media, online private messaging, app store, online retail marketplace, and digital advertising services, in respect of scams
- app stores in respect of harmful apps

---

57 Meta, *Submission 69*, p. 42.

58 Meta, *Submission 69*, p. 42.

59 CBA, *Submission, 71*, p. 4.

60 Match Group, *Submission 73*, p. 6.

61 ACCC, *Submission 8*, pp. 6–7; Dr Gareth Downing, Deputy CEO, ACCAN, *Proof Committee Hansard*, 26 July 2023, p. 36.

62 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 73.

63 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 73.

- search, social media, app stores, online retail marketplace, and digital advertising services, in respect of fake reviews.[64]

7.47 The ACMA and the Australian Communications Consumer Action Network expressed support for the introduction of new legislation[65] requiring 'digital platforms and messaging applications to identify and block scam activities, as is required for telecommunications providers'.[66]

Notice-and-action mechanism

7.48 Submissions supported the implementation of the ACCC's recommendation[67] for a mandatory 'notice-and-action' mechanism enabling any individual or entity to report a scam, illegal content or harmful app and obliging the digital platforms receiving the report to take appropriate action in response.[68]

7.49 The ACCC advised:

> Verification of advertisers, app developers and merchants would reduce the prevalence of scams and harmful apps, better protecting would-be victims from monetary losses and psychological impacts, and additional verification of advertisers of financial services and products would better protect consumers from predatory parties.[69]

7.50 Notice-and-action mechanisms will soon be required in Europe under the Digital Services Act and are being considered for digital platforms operating in the United Kingdom.[70]

Codes

7.51 Some submissions suggested the ACCC's proposal for additional measures to promote consumer safety could be achieved with sector specific codes such as for marketplace services and social media services.[71]

7.52 DITRDCA highlighted that the Treasury is consulting on a possible Government response to the ACCC report and advised DITRDCA 'is actively working with

---

64 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 73.

65 Dr Gareth Downing, Deputy CEO, ACCAN, *Proof Committee Hansard*, 26 July 2023, pp. 35-36.

66 ACMA, *Submission 24*, p. 4

67 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 72.

68 See, for example, ASBFEO, *Submission 39*, [p. 2]; CBA, *Submission 71*, p. 4; Match Group, *Submission 73*, p. 13; DITRDCA, *Submission 9*, p. 11.

69 ACCC, *Submission 8*, p. 7.

70 ACCC, *Digital platform services inquiry, Interim report No. 5 – Regulatory reform*, September 2022, p. 83.

71 See, for example, Match Group, *Submission 73*, p. 13; Free TV Australia, *Submission 17*, p. 23; Dr Gareth Downing, Deputy CEO, ACCAN, *Proof Committee Hansard*, 26 July 2023, pp. 36–37.

the Treasury and the ACMA to shape advice to the Government in relation to measures to address online scams'.[72]

[72] DITRDCA, *Submission 9*, p. 11.

Chapter 8
Online safety

Overview

8.1 Many submissions raised concerns about online children's safety and the role of digital platforms.

8.2 This chapter considers the potential risks from the collection of children's data by digital platforms. It then examines evidence received by the committee, with a focus on the two main themes: unethical behaviours and criminal behaviour online.

8.3 The chapter will then examine the current digital platform regulatory framework supporting online safety for children, and potential ways to strengthen protections for children online, including international approaches.

Digital platforms, data, and children

8.4 Digital platforms harness high volumes of data from consumers, as well as connecting consumers to unprecedented levels of information. Among consumers are children, young adults, and vulnerable people, who unknowingly generate data that is captured, processed, and used for undisclosed purposes. As UNICEF highlighted, the 'digital ecosystem is so complex and seamless that neither children or their adult guardians are fully aware of how their data is being captured and used, nor what the potential benefits and risks are'. [1]

8.5 The committee considered evidence on the risks to consumers more broadly from digital platforms' data collection practices in Chapter 5: Data.

8.6 There is a strong connection between interaction with digital platforms and risks to vulnerable groups of people, in particular, children. The Office of the eSafety Commissioner (eSafety) and UNICEF's submissions both highlighted that children increasingly rely on digital platforms to learn, develop cognitive skills, socialise, and build their identity.[2] Research indicates that 94 per cent of children in Australia are already online by the age of 4 years.[3]

8.7 Ms Sarah Davies, Chief Executive Officer of the Alannah & Madeline Foundation, detailed the potential risks arising from children engaging with digital platforms:

---

1 UNICEF, *Submission 14*, p. 11.

2 Office of the eSafety Commissioner (eSafety), *Submission 1*, p. 11; UNICEF, *Submission 14*, p. 8.

3 eSafety, *Submission 1*, p. 11.

> Many digital platforms are designed to be highly engrossing and difficult to put down. They handle vast amounts of personal information about their users, and the users do not understand and certainly don't have any say over what happens to their personal information. Now, there may be no intention to cause harm to children, but many of these platforms have turned out to be risky by design. Those risks include loss of control over personal information, contact with undesirable individuals, financial loss, exposure to age-inappropriate advertising and other content, and dysregulated tech use that then has flow-on effects for children's mood, health, and overall well-being.[4]

8.8 Child safety risks associated with data collection and algorithms include:

- friend/follower suggestions that can pressure children to interact with strangers and recommend dangerous accounts;
- encouraging 'doomscrolling'[5], which can limit exposure to diverse content, and deliver increasingly problematic content;
- encouraging dangerous viral challenges;[6]
- promoting beauty stereotypes which may be unrealistic or harmful;
- normalising the sexualisation of young people; and
- recommending content that may be appropriate for adults but harmful to children who are not developmentally ready for it (i.e. violent or sexually explicit material).[7]

8.9 Many submitters raised concerns about the quantity of children's data being collected by digital platforms.[8] Ms Alice Dawkins, Executive Director at Reset.Tech Australia (Reset.Tech), emphasised the volume of data collection for the intention of marketing to children:

> The best available estimate of the amount of data collected by advertisers about children and young people is that, by the time a child has turned 13,

---

4 *Proof Committee Hansard*, 26 July 2023, p. 12.

5 Doomscrolling refers to excessively scrolling through bad news on social media and is considered problematic news consumption. See Ms Freya Thomson, *What is doomscrolling and why is it bad for us?*, 9 September 2022, www.openaccessgovernment.org/what-is-doomscrolling-and-why-is-it-bad-for-us/143139/ (accessed 22 August 2023).

6 Viral challenges are online or social media driven trends encouraging users to upload videos of themselves copying a dare or stunt. For example, the 'ice bucket challenge' saw users pouring a bucket of ice water over their own or another person's head. Challenges are usually started by social media users, and some can be significantly dangerous.

7 eSafety, *Submission 2*, p. 4; Association of Heads of Independent Schools of Australia (AHISA), *Submission 13*, p. 8.

8 See, for example, eSafety, *Submission 2*; Cancer Council Australia, *Submission 5*; Alcohol and Drug Foundation, *Submission 10*; Alcohol Change Australia, *Submission 11*; Association of the Heads of Independent Schools of Australia, *Submission 13*; UNICEF, *Submission 14*; Obesity Policy Coalition, *Submission 19*; Reset.Tech Australia, *Submission 31*; Alannah & Madeline Foundation, *Submission 41*; Office of the Australian Information Commissioner, *Submission 61*.

> there are about 72 million data points on them … within that 72 million, that's hundreds or, perhaps, thousands of companies who know things such as the precise geolocation of a child for the purpose of selling them products.[9]

8.10 Ms Dawkins added that children's data is collected from multiple sources of interaction with digital platforms. This not only includes social interaction, but also education interaction, emphasising that regulation of digital platform data collection practices is not currently effective (for an example, see Box 8.1).[10] Ms Davies echoed these sentiments during the public hearing, agreeing that there is no day-to-day regulation of children's data protection, 'and there needs to be.'[11]

Box 8.1 Case study: Children's data collection

A prominent videoconferencing provider in Victoria was found to be collecting data from students, presumably during their school day, including their unique identifier, such as their phone handset serial codes.

Crucially, the provider was engaging in something called 'ID bridging', which means it was identifying individual students and linking their data to enhance the data profile on them.

The provider collected precise location data of children, the time at their current location and their last known location. The provider collected contact information, including saved profile photos of contacts on children's phones. The provider embedded three programs known as Software Development Kits (SDKs) that allowed third-party advertising technology (adtech) companies to access the students' data.

The privacy policy was found to be deceptive and failed to declare the collection of these persistent identifiers, the practice of ID bridging, the call logs, the contact information, the use of embedded SDKs and the identity of third parties receiving user data.

There was a lack of ramifications for the deceptive practices.

Source: Ms Alice Dawkins, Executive Director, Reset.Tech Australia, Proof Committee Hansard, 26 July 2023, pp. 16–17.

8.11 In its submission, UNICEF highlighted the primary concern around children's data collection:

---

9 *Proof Committee Hansard*, 26 July 2023, p. 16.

10 Ms Alice Dawkins, Executive Director, Reset.Tech Australia, *Proof Committee Hansard*, 26 July 2023, p. 16.

11 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 14.

> Children are more vulnerable than adults and less able to understand the long-term implications of consenting to their data collection. Given children's greater cognitive, emotional, and physical vulnerabilities, privacy concerns that exist for adults are amplified for children.[12]

8.12 The Australian Medical Association echoed this concern and added that:

> Children's location data in particular is extremely sensitive, presenting significant risk if this data is inappropriately disclosed.[13]

Unethical and criminal online behaviours

8.13 Child safety in the digital age was a high priority for a number of submitters to the inquiry. Concerns ranged from harmful product marketing to children and youth using targeted advertising through to online child sexual exploitation and abuse.

8.14 Further, the Attorney-General's Department emphasised that 'while these digital platforms provide critical educational and social connections for young people, they have also enabled existing and new forms of online harms, the most serious being child sexual exploitation and abuse'.[14]

Harmful product marketing

8.15 As discussed in Chapter 5: Data, profiling refers to the platforms' practice of building a 'profile' of a person's personal attributes and interests through tracking their behaviour over time, which can then be used for targeted advertising or to manipulate or discriminate against individuals.[15]

8.16 The Attorney-General's Department highlighted that that risks of targeting are especially 'acute for children due to their particular susceptibility and developing cognitive abilities'.[16]

8.17 Harmful product marketing was highlighted by submitters as an online safety concern for children. Evidence suggested that harmful product marketing is targeting children on digital platforms, undermining children's health, and wellbeing. Submitters raised specific concerns around aggressive alcohol advertising, gambling, promotion of unhealthy food choices, and targeting children with dieting products, potentially increasing the risk of developing body image issues.[17]

---

12 UNICEF, *Submission 14*, p. 11.

13 Australian Medical Association, *Submission 66*, p. 3.

14 Attorney-General's Department, *Submission 51*, p. 4.

15 Human Rights Law Centre, *Submission 50*, p. 12.

16 Attorney-General's Department, *Submission 51*, p. 16.

17 See, for example, Cancer Council Australia, *Submission 5*; Alcohol and Drug Foundation, *Submission 10*; Alcohol Change Australia, *Submission 11*; Association of the Heads of Independent Schools of

8.18 Alcohol Change Australia's submission identified concerning behaviour by large social media digital platforms:

> Meta has been found to have flagged children as being 'interested' in harmful products, including alcohol. It has also been found to use personal data collected to create profiles of young people with harmful or risky interests, including 13–17-year-olds interested in alcohol, smoking, and gambling. Even worse, Meta allowed advertisers to buy access to the young people profiled as having harmful interests.[18]

8.19 The Alcohol and Drug Foundation echoed these concerns, highlighting the unethical behaviours of online tracking, profiling, and data collection enabled by digital platforms have facilitated harmful marketing of alcohol. For example:

> During the COVID-19 pandemic, the alcohol industry used digital platforms to aggressively promote rapid delivery services and drinking at home, exacerbating vulnerabilities already caused by the pandemic.[19]

8.20 The committee was warned that alcohol and unhealthy diets are a risk factor for cancer and increased exposure to harmful marketing is contributing to alcohol use among young people.[20]

8.21 Submitters also highlighted concern for marketing of dieting products and the potential affects this can have on some people and communities, particularly young people and those who have experienced or are at risk of eating disorders.[21]

Child sexual exploitation

8.22 The committee also heard concerns around the use of platforms to further illegal activities. The proliferation of online child sexual exploitation and abuse occurring on digital platforms has continued to escalate year on year in volume of reports and severity of crime type.[22] The Attorney-General's Department emphasised the increasing volume of online child sexual abuse material (CSAM), noting:

> The United States based National Centre for Missing and Exploited Children (NCMEC) reported 29.3 million reports of apparent child sexual abuse material made to their CyberTipline in 2021, up from 21.7 million in 2020 …

Australia, *Submission 13*; Obesity Policy Foundation, *Submission 19*; Australian Medical Association, *Submission 66*, pp. 3–5.

18 Alcohol Change Australia, *Submission 11*, [p. 2].

19 Alcohol and Drug Foundation, *Submission 10*, pp. 1–2.

20 See, for example, Cancer Council Australia, *Submission 5*, [p. 1]; Obesity Policy Coalition (OPC), *Submission 19*, pp. 2–4.

21 See, for example, eSafety, *Submission 2*, p. 4; Alcohol and Drug Foundation, *Submission 10*, p. 2; Reset Australia, *Submission 74*, p. 4.

22 Attorney-General's Department, *Submission 51*, p. 5.

> The UK-based Internet Watch Foundation reported that, 'Imagery of primary school aged children being coached to perform sexual acts online has soared by more than 1,000 percent since the UK went into lockdown during the pandemic.'[23]

Current Australian regulations and frameworks

8.23 The current regulation of online safety is spread across several different government agencies as outlined in Table 8.1.

Table 8.1 Regulatory Function—Government Agencies

Agency	Legislation	Function
Australian Competition and Consumer Commission	*Competition and Consumer Act 2010*	Competition and consumer issues
Office of the Australian Information Commissioner	*Privacy Act 1988*	Data and privacy issues
Australian Communications and Media Authority	*Broadcasting Services Act 1992*	Industry code relating to targeting of a person with disinformation and information
Attorney-General's Department	*Criminal Code Act 1995* *Telecommunications (Interception and Access) Act 1979* *Surveillance Devices Act 2004* *Privacy Act 1988*	Commonwealth criminal justice and law enforcement frameworks across multiple areas
eSafety Commissioner	*Online Safety Act 2021*	Regulatory function for online safety

Source: eSafety Commissioner, Submission 2, p. 1; Attorney-General's Department, Submission 51, p. 4.

eSafety Commissioner

8.24 The primary agency focused on online safety is eSafety. The *Online Safety Act 2021* (OSA), eSafety's enabling legislation, provides the regulatory functions for online safety, including administering complaints and investigations schemes for four types of online harms:

- cyberbullying of children;
- cyber abuse of adults;
- the non-consensual sharing of intimate images;

[23] Attorney-General's Department, *Submission 51*, p. 5.

- illegal or restricted online content.

8.25 eSafety also holds powers to regulate digital platforms' broader systems and processes.[24]

Mandatory industry codes

8.26 The OSA requires certain online industry sectors to develop mandatory industry codes to deal with class 1[25] and class 2[26] illegal and restricted content online.[27] These include providers of social media, email, messaging, gaming, dating, search engine and app distribution services, as well as internet and hosting service providers, manufacturers and suppliers of equipment used to access online services and those that install and maintain the equipment.[28]

8.27 The codes outline such things as measures towards ensuring industry participants take reasonable and proactive steps to prevent access or exposure to, distribution of and online storage of class 1A material.[29]

8.28 Other matters the codes address include:

- measures to facilitate consultation and cooperation with other industry participants around removal and disruption and restriction of class 1A and 1B material and associated accounts.
- ensuring communication and cooperation with eSafety with respect to the relevant material, including complaints.
- tools and information to help people avoid exposure to these materials.
- clear, accessible and effective reporting mechanisms and complaints mechanisms around handling of reports.
- the mechanisms to effectively respond to reports and complaints on report handling.

---

24 eSafety, *Submission 2*, p. 1.

25 Class 1 material is material that is or would likely be refused classification under the National Classification Scheme, see eSafety, *Illegal and Restricted online content*, www.esafety.gov.au/key-topics/Illegal-restricted-content (accessed 11 October 2023).

26 Class 2 material is material that is, or would likely be, classified as either: X18+ (or, in the case of publications, category 2 restricted), or R18+ (or, in the case of publications, category 1 restricted) under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old, see eSafety, *Illegal and Restricted online content*, (accessed 11 October 2023).

27 eSafety, *Submission 2*, p. 6.

28 eSafety, *Industry codes and standards*, www.esafety.gov.au/industry/codes (accessed 6 July 2023).

29 eSafety, *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms*, www.esafety.gov.au/sites/default/files/2023-09/Consolidated-Industry-Codes-of-Practice-Head-Terms-12-September-23.pdf (accessed 15 September 2023).

- publication of an annual report on compliance with the codes.[30]

8.29 Following assessment by eSafety, the codes will be registered if they meet statutory requirements, or eSafety may determine an industry standard if requirements are not met by the proposed code.[31] Once registered, compliance with the codes is mandatory and enforceable.[32] eSafety will have powers to investigate breaches and direct platforms to comply, with civil penalties, enforceable undertakings and injunctions available to ensure compliance.[33]

8.30 eSafety has so far registered six industry codes to deal with class 1 content for:

- social media services
- app distribution services
- hosting services
- internet carriage services
- equipment
- internet search engine services.

8.31 The obligations contained in these codes will come into effect on 16 December 2023,[34] except the Internet Search Engine Services code which will come into effect on 12 March 2024.[35]

8.32 eSafety is drafting industry standards for Electronic Services and Designated Internet Services in consultation with industry and the public as the proposed codes did 'not provide appropriate community safeguards for users in Australia'.[36]

8.33 A second phase of industry codes will follow, focusing on class 2 material and measures to prevent children accessing high-impact age-inappropriate content that can be harmful.[37]

---

30 eSafety, *Consolidated Industry Codes of Practice for the Online Industry (Class 1A and Class 1B Material) Head Terms*, (accessed 15 September 2023).

31 eSafety, *Industry codes and standards*, (accessed 6 July 2023).

32 eSafety, *Submission 2*, p. 6.

33 eSafety, *Online industry asked to address eSafety's concerns with draft codes*, www.esafety.gov.au/newsroom/media-releases/online-industry-asked-address-esafetys-concerns-draft-codes-0 (accessed 15 September 2023).

34 eSafety, *Industry codes and standards*, (accessed 6 July 2023).

35 eSafety, *Online industry asked to address eSafety's concerns with draft codes*, (accessed 15 September 2023).

36 eSafety, *Industry codes and standards*, (accessed 6 July 2023).

37 eSafety, *Industry codes and standards*, (accessed 6 July 2023).

Regulated reporting requirements: Basic Online Safety Expectations

8.34 The OSA also introduced the Basic Online Safety Expectations (BOSE) which outline the Australian Government's expectations that social media, messaging and gaming service providers and other apps and websites will take reasonable steps to keep Australians safe.[38]

8.35 eSafety can establish mandatory reporting requirements for online service providers to report how they are meeting the BOSE such as protecting children from age-inappropriate content or proactively minimising unlawful material or activities. The reporting obligation is enforceable, backed by civil penalties and other mechanisms (see Box 8.2 for an example).[39]

8.36 Since the OSA commenced, eSafety has issued 12 BOSE reporting notices focussed on the steps being taken by platforms to prevent, detect and remove child sexual exploitation and abuse on their services.[40] Statements summarising these responses can be found on eSafety's website.[41]

8.37 eSafety's world-first report, *Basic Online Safety Expectations (BOSE): Summary of industry responses to the first mandatory notices*, found that some of the world's biggest technology companies needed to do more to tackle child sexual exploitation and abuse material.[42]

Box 8.2 Findings of non-compliance: Google and Twitter (X)

eSafety found Google and Twitter (now X Corp.) failed to comply with non-periodic notices given on 22 February 2023, contravening paragraph 56(2)(b) and section 57 of the *Online Safety Act 2021*.

Google

- Google failed to answer several questions in response to the notice, including providing generic information where specific information was sought.
- Google was issued a formal warning, notifying it of its failure to comply, and warning against non-compliance in the future.

[38] eSafety, *Basic Online Safety Expectations*, www.esafety.gov.au/industry/basic-online-safety-expectations (accessed 6 July 2023).

[39] eSafety, *Basic Online Safety Expectations*, (accessed 6 July 2023).

[40] eSafety, *Submission 2*, p. 7.

[41] eSafety, *Responses to transparency notices*, www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices (accessed 6 July 2023).

[42] UNICEF, *Submission 14*, p. 7.

Twitter (X)

- eSafety considered Twitter's failure to comply more serious. Twitter failed to provide any response to some questions, and provided some responses that were incomplete and/or inaccurate.
- eSafety issued a service provider notification to Twitter, confirming its non-compliance, and an infringement notice for $610 500.

Source: eSafety, Responses to transparency notices, *www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices (accessed 6 July 2023).*

Safety by Design

8.38 eSafety also promotes online safety measures through its Safety by Design initiative. Safety by Design encourages industry to anticipate potential harms and implement risk-mitigating and transparency measures throughout the design, development and deployment of a product or service.

8.39 The initiative promotes online safety through three guiding principles:

- Service provider responsibility – that platforms are responsible for the safety of users.
- User empowerment and autonomy – that users should be empowered with safety tools and provided with autonomy.
- Transparency and accountability – that platforms should be transparent and held accountable for their actions.[43]

The Attorney-General's Department

8.40 The Attorney-General's Department is responsible for the Commonwealth's criminal justice and law enforcement frameworks in relation to child sexual exploitation and abuse. Its focus includes combating CSAM. It operates under powers enforced by the following Acts:

- *Criminal Code Act 1995*;
- *Telecommunications (Interception and Access) Act 1979*;
- *Surveillance Devices Act 2004*; and
- *Privacy Act 1988* (Privacy Act).[44]

8.41 The Attorney-General's Department also works with domestic and international agencies to combat CSAM. Examples of recent collaborative work include:

- The Australian Government's signing of the agreement on the US *Clarifying Lawful Overseas Use of Data Act* in December 2021.[45]

---

43 eSafety, *Submission 2*, p. 7.

44 Attorney-General's Department, *Submission 51*, pp. 4–5.

45 Ms Lucinda Longcroft, Director of Government Affairs and Public Policy, Google, *Proof Committee Hansard*, Parliamentary Joint Committee on Law Enforcement, 10 August 2023, p. 4.

- The Australian Federal Police and AUSTRAC's partnership on 'Operation Huntsman' to combat sexual extortion in Australia.[46]
- The Attorney-General's Department's work with digital platforms such as Google to procure information on CSAM investigations.[47]

Age Verification Roadmap

8.42 In March 2023, eSafety submitted a roadmap on age verification to the Australian Government for consideration. It included complementary measures to prevent and mitigate harm to children from online pornography.

8.43 The roadmap makes a number of recommendations for Government, reflecting the multifaceted response needed to address the harms associated with Australian children accessing pornography.[48]

Measures implemented by Big Tech

8.44 Many large digital platforms highlighted their commitments to promoting online child safety.

8.45 Meta submitted it recognises its responsibility to young people and invests heavily in it. Meta has many default protections for young people, including restricting advertisers to only be able to target young people by age and location. Ms Mia Garlick, Regional Director of Policy, Meta, stated that:

> Since 2016 we've invested over US$16 billion. Really it's in our commercial interest to invest in safety and security, because people will only continue to use our services if they feel welcome and safe.[49]

8.46 Mr Kyle Andeer, Vice President, Products and Regulatory Law, Apple Inc., stated Apple provides a range of tool for parents to help kids safely use Apple devices. These include parent controls that:

> … empower parents to decide exactly which apps can be downloaded on their kids' devices. It allows parents to block or limit specific consent, features or websites, including explicit content. It allows parents to block apps from accessing their children's most personal information, including their contacts, photos and even their location. Parents can help protect their kids from what they see and send by setting up communication safety on their kids' devices. This feature uses privacy friendly on-device machine learning to analyse photos and videos. If your kid receives or attempts to

---

46 Attorney-General's Department, *Submission 51*, p. 5.

47 Ms Lucinda Longcroft, Director of Government Affairs and Public Policy, Google, *Proof Committee Hansard*, Parliamentary Joint Committee on Law Enforcement, 10 August 2023, p. 4.

48 eSafety, 'Age verification', www.esafety.gov.au/about-us/consultation-cooperation/age-verification#roadmap-and-background-report, (accessed 27 November 2023).

49 *Proof Committee Hansard*, 22 August 2023, p. 17.

> send photos or videos that might contain nudity, we warn them, give them an opportunity to stay safe and offer to connect them to a trusted adult.[50]

8.47 Microsoft submitted it invests in child safety across four pillars:

- Platform architecture – Microsoft recognises design of platforms impacts safety and is working to embed safety by design principles across consumer services.
- Content moderation – Microsoft publishes and enforces clear policies, such as its Code of Conduct Agreement which states users should not engage in any activity that exploits, harms, or threatens to harm children.
- Culture – Microsoft believes in creating safe and inclusive communities, which includes providing users and families with the tools and information to support their engagement, provide choices about the content and users with whom they interact, and raising awareness of online safety risks.
- Collaboration – Microsoft states a collaborative approach between regulators, industry and civil society is critical.[51]

8.48 Google stated it is an industry leader in fighting child sexual abuse, including using proprietary technology to deter, detect and report offences, and remove material on its platforms. It also partners with NGOs and industry on programs to share technical expertise and develop and share tools to help organisations fight CSAM, and works with law enforcement.[52] Further, Google stated it is working to implement the new codes under the Online Safety Act, and alongside BOSE, have an effective protection framework.[53]

Concerns with the current regulatory framework

Fragmentation

8.49 As highlighted above, the committee notes that there are a number of government bodies with a function in children's online safety.

8.50 In its submission, the Office of the Australian Information Commissioner outlines that 'the different harms that can arise in the online environment have resulted in intersections between regulatory spheres in regulating digital platforms, which highlights the importance of regulatory cooperation and coordination'.[54]

---

50 *Proof Committee Hansard*, 3 October 2023, p. 6.

51 Microsoft, *Submission 47*, pp. 13–14.

52 Google, *Submission 49*, p. 11.

53 Google, *Submission 49*, p. 14.

54 Office of the Australian Information Commissioner, *Submission 61*, p. 1.

Regulatory gaps

8.51 Several submissions highlighted that fragmentation of regulations has resulted in regulatory gaps.

8.52 Reset Australia commented that issues surrounding children's rights, especially privacy, engagement with harmful communities and data, are currently overlooked:

> Our framework focuses on a narrower understanding of online safety that does not adequately reflect the full scope of the risks children and young people face online. That is, when Australian children and young people engage with the digital world, many of the risks they encounter currently sit outside our regulatory system.[55]

8.53 The committee was advised, for example, that the current legislative framework is limited in its capacity to comprehensively address the issue of reducing harmful digital marketing practices.[56]

8.54 eSafety's remit under the OSA addresses criminal and antisocial online behaviours and seriously illegal content. The committee was advised that there has been less Australian Government investment in addressing online safety aspects that arise from the design of digital platforms, such as contact risks.[57]

Effectiveness of BOSE

8.55 BOSE provides eSafety with the power to compel online service providers to produce compliance reports, thus enhancing transparency of the actions digital platforms are taking to ensure user safety. BOSE also encourages platforms to maintain a focus on safety concerns.[58]

8.56 However, while eSafety's primary report indicated technology companies needed to do more to tackle child sexual exploitation and abuse material,[59] eSafety has no powers to compel changes to the way platforms operate.

8.57 The Australian Research Alliance for Children and Youth noted that 'the inability to enforce the BOSE is insufficient in preventing online harm from occurring … any impetus derived from reputational damage caused by the

---

55 Reset Australia, *Submission 74*, p. 4.

56 See, for example, Foundation for Alcohol Research and Education, *Submission 33*, p. 9; UNICEF, *Submission 14*.

57 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 14.

58 Australian Research Alliance for Children and Youth (ARACY), *Submission 21*, [p. 2].

59 UNICEF, *Submission 14*, p. 7.

disclosure [is] inconsequential because of the lack of market pressures to conform.'[60]

Ineffective self-regulation

8.58 Submitters commented that voluntary or co-regulatory approaches are insufficient for appropriately regulating technology companies.[61]

8.59 The Alcohol and Drug Foundation stated:

> The existing regulatory system, relying largely on voluntary, industry-managed codes and practices, has proven to be ineffective in protecting the community from the negative impact of unhealthy marketing. The industry's clear conflict of interest means that the industry-led processes will never restrict alcohol marketing in a genuinely effective manner. Existing codes do not adequately restrict alcohol companies from marketing on digital platforms that are heavily used by children, and there are concerning examples of alcohol advertising directed to children online.[62]

8.60 Dr Jessie Mitchell, Advocacy Manager, the Alannah & Madeline Foundation, stated, while participating in consultation to develop the Online Safety Act Industry Codes, the foundation found 'there was not a clear commitment to pursuing common global standards of best practice in upholding children's safety'.[63]

8.61 Reset Australia also argued the weakness of co-regulation is demonstrated by the limited protections in Australia as compared to other children's codes in the United Kingdom (UK), Ireland and California. Reset Australia recommended not registering co-regulatory codes in future, and progressively replacing self or co-regulatory codes with mandatory regulations.[64]

8.62 The Human Rights Law Centre commented:

> Co-regulation is inappropriate for such a powerful and high-risk sector, in which business models frequently come into conflict with community needs and the public interest. In the European Union, introduction of the *Digital Services Act* was driven by growing recognition that self- and co-regulatory models are inadequate and ineffective.[65]

---

60 ARACY, *Submission 21*, [p. 2].

61 See, for example, Ms Alice Dawkins, Executive Director, Reset.Tech Australia, *Proof Committee Hansard*, 26 July 2023, p. 17; Mr Mark Nottingham, *Submission 37*, p. 5; Human Rights Law Centre (HRLC), *Submission 50*, p. 9; Obesity Policy Coalition, *Submission 19*, p. 2.

62 Alcohol and Drug Foundation, *Submission 10*, p. 2.

63 *Proof Committee Hansard*, 26 July 2023, p. 13.

64 Reset Australia, *Submission 74*, p. 15.

65 HRLC, *Submission 50*, p. 9.

Globally inconsistent controls

8.63 The committee notes online safety is a global concern. Australia does not appear to have aligned safety standards for Australian children with the rights of children overseas or emerging best practice. The committee heard:

> … this is a transnational world where children and young people are living digitally across all of these platforms globally.[66]

8.64 Several submitters argued various codes, in force in international jurisdictions, such as in the UK, California and Ireland, provide higher protections for children than Australia (See Box 8.3 for more information on two of these codes).[67]

8.65 The Alannah & Madeline Foundation commented that Big Tech is currently taking a market-by-market approach and applying different standards in different jurisdictions.[68] Ms Davies provided an example:

> … there are different standards for the privacy default setting in Australia, which is 16, and in other jurisdictions which are regulated independently, where the default setting is 18. There are different standards for collecting geolocation data.[69]

8.66 Dr Mitchell added:

> Something we experienced recently was the opportunity to take part in the consultation to information the development of industry codes under Australia's Online Safety Act. While we value the opportunity to take part, we did come away with the belief that there was not a clear commitment to pursuing common global standards of best practice in upholding children's safety.[70]

8.67 Ms Davies elaborated that this approach is 'disingenuous' and allows platforms to act based on what they think they will get away with rather than employing high safety settings by default.[71]

8.68 eSafety and UNICEF also emphasised that existing international regulatory instruments, such as the UK Age Appropriate Design Code, recognise the

---

66 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13.

67 See, for example, Reset Australia, *Submission 74*, p. 15; Alannah & Madeline Foundation, *Submission 41*, p. 8.

68 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 12.

69 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 12.

70 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13.

71 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 12.

importance of services being able to identify which of their users are children and young people so they can create safe, private and appropriate online experiences for them.[72]

The Age Appropriate Design Code (UK)

8.69 Dr Mitchell compared the different approaches between Australia and the UK in relation to online safety:

> When we contrast what the new industry codes will require for digital platforms in Australia compared to what's expected of them in the UK under their children's code, we can see that there are some lower standards being accepted in Australia than would be accepted in the UK.[73]

8.70 Dr Mitchell highlighted the important considerations that have been included in the UK's Age Appropriate Design Code (Children's Code):

> Under the UK children's code, services that are likely to be accessed by someone under 18 have to have fairly comprehensive, high privacy settings by default, whereas in the Australian situation both the definition of 'children' and the definition of 'privacy' are narrower. Children became defined as 'under 16' and the high privacy settings focus on preventing contact with strangers but not necessarily stopping inappropriate handling of children's data—like in geolocation data, for example.[74]

8.71 The committee heard about the positive changes resulting from introduction of the UK Children's Code:

> Following its introduction, we did see a number of positive changes being made by digital platforms that were operating there. As a few examples, you had Instagram introducing prompts to encourage children to take a break from scrolling, Google making SafeSearch their default browsing mode for children and YouTube autoplay being turned off. While we can't directly attribute that to operating in a country that had a more rigorous code, the timing is suggestive.[75]

Box 8.3 International approaches to children's codes

The Age Appropriate Design Code (UK)

The UK Children's Code came into force on 2 September 2020. It is enforced by the UK Information Commissioner. The Code is derived from the principles in the UK Data Protection Act and European Union General Data

---

72 eSafety, *Submission 1*, p. 13; UNICEF, *Submission 14*, pp. 4–5.

73 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13.

74 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13.

75 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 14.

Protection Regulation, including data minimisation, purpose limitation, and data protection by design and default.

The code mandates that all online services 'likely to be accessed by children' provide data security for children such as by:

- providing a high level of privacy by design and default;
- explaining the nature of the service in child-friendly language;
- requiring data use to be in the child's best interests; and
- not using children's data to recommend harmful material.[76]

California Age Appropriate Design Code Act (US)

This Act, passed on 15 September 2022, aims to keep children safe online by requiring companies to consider privacy and protection of children in the design of any digital product or service that children are likely to access.[77] It also restricts data collection and profiling of children, requires high privacy settings for children by default, and prohibits the use of nudge techniques to encourage children to weaken their privacy protections.[78] On 19 September 2023, the US District Court, Northern District of California, San Jose Division granted an injunction that prohibited the California Attorney General from enforcing the Act until ordered otherwise by the court as it likely violates the First Amendment of the US Constitution.[79]

Strengthening Australia's framework

8.72 A range of measures were proposed to the committee in response to the current challenges of regulating online safety.

Current processes

8.73 The Tech Council of Australia supported a wait-and-see approach allowing time to observe and evaluate the impact of the recent reforms.[80]

---

[76] 5 Rights Foundation, *Demystifying the Age Appropriate Design Code*, https://5rightsfoundation.com/uploads/demystifying-the-age-appropriate-design-code.pdf (accessed 28 June 2023).

[77] 5 Rights Foundation, *We Need to Keep Kids Safe Online: California has the Solution*, https://5rightsfoundation.com/uploads/California-Age-Appropriate-Design-Code_short-briefing.pdf (accessed 28 June 2023); *The California Age-Appropriate Design Code Act 2022* (US).

[78] 5 Rights Foundation, *We Need to Keep Kids Safe Online: California has the Solution*, (accessed 28 June 2023).

[79] Adi Robertson, *Court blocks California's online child safety law*, 19 September 2023, www.theverge.com/2023/9/18/23879489/california-age-appropriate-design-code-act-blocked-unconstitutional-first-amendment-injunction (accessed 21 November 2023).

[80] Tech Council of Australia, *Submission 63*, p. 14.

8.74 The current online safety framework will be assessed through a legislated independent review of the operations of the OSA, to commence by January 2025.

8.75 Department of Infrastructure, Transport, Regional Development, Communications and the Arts advised this review timeframe allows for a proper assessment of the operations and weaknesses of the OSA, consideration of emerging international approaches, and is the appropriate mechanism to consider amendments.[81]

8.76 Many submitters were in favour of implementing additional regulatory measures to protect children without delay.[82]

Support for the Privacy Act Review

8.77 As discussed in Chapter 5: Data, many submitters raised broad support for the proposed amendments under the Privacy Act Review.[83]

8.78 The Privacy Act Review report puts forward proposals to strengthen protections for children, such as encouraging entities to consider 'whether the collection, use or disclosure of personal information is in the best interests of the child'. It also proposes prohibitions on direct marketing and targeting to children, and trading children's data.[84]

8.79 eSafety highlighted, as part of the Attorney-General's Department review of the *Privacy Act 1988*, it proposed the creation of an Australian Children's Online Privacy Code, to be modelled on the UK Age-Appropriate Design Code, with eSafety being consulted during the development.[85]

8.80 Reset.Tech supported the proposals as being 'sound. They're justified, and they should be heartily supported by anyone with an interest in these issues'.[86]

---

81 Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Submission 9*, p. 6.

82 See, for example, Reset Australia, *Submission 74*, p. 19; Mr John Livingstone, Advocacy Manager, UNICEF Australia, *Proof Committee Hansard*, 26 July 2023, p. 26; Obesity Policy Coalition, *Submission 19*, p. 1; Alannah & Madeline Foundation, *Submission 41*, p. 3; ARACY, *Submission 21*, [p. 3]; Children and Media Australia, *Submission 53*, p. 1; Uniting Church of Australia, *Submission 52*, p. 1; Cancer Council Australia, Submission 5, [p. 2].

83 See, for example, ACCAN, *Submission 20*, p. 37; DIGI, *Submission 65*, p. 1; Mr Roger Somerville, Head, Australia and New Zealand Public Policy, Amazon Web Services, *Proof Committee Hansard*, 3 October 2023, p. 4.

84 Office of the Australian Information Commissioner, *Submission 61*, p. 4.

85 eSafety, *Submission 2*, p. 13; UNICEF, *Submission 14*, pp. 4–5.

86 Ms Alice Dawkins, Executive Director, Reset.Tech Australia, *Proof Committee Hansard*, 26 July 2023, p. 17.

Education

8.81 UNICEF recommended any emerging regulations should be accompanied by greater education efforts:

> The emerging standards for age assurance are embracing the full range of options on offer. These need to be coupled with education to understand the value of privacy-preserving age assurance options and the role they can play in improving online safety for children, along with a broad multi-faceted approach to protecting children online beyond age assurance.[87]

8.82 The Tech Council of Australia suggested Kindergarten to Year 12 education should include e-safety courses from on topics such as cyberbullying, online privacy, digital footprints, online scams and safe online practices.[88]

A strong regulator

8.83 The committee heard that any regulation should be overseen by an independent public regulator[89] and be adequately resourced so it can be 'sufficiently muscular'.[90]

8.84 Reset Australia submitted the risks to sector require strong enforcement because they are:

- High impact, and include significant public health and community safety concerns
- Significant to the community, and the public has an appetite for the certainty of robust regulations
- Unable to be adequately dealt with by lighter touch regulations. Digital platforms have demonstrated a track record of systemic compliance issues, including multiple breaches of existing legislation and a generally anaemic response to self-regulation

> This warrants a pivot towards primary and subordinate legislation and regulation for the sector. Alongside strengthening existing regulation, regulators need to be resourced and enabled to enforce this, and joined up in ways that do not reproduce the issue-by-issue approach hampering current legislative remedies.[91]

8.85 The Alannah & Madeline Foundation argued that regulators need adequate resources and access to high-quality, up-to-date information about new and emerging developments in digital technology:

---

87 UNICEF, *Submission 14*, p. 7.

88 Tech Council of Australia, *Submission 63*, p. 14.

89 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 12.

90 Ms Alice Dawkins, Executive Director, Reset.Tech Australia, *Proof Committee Hansard*, 26 July 2023, p. 17. Also see CPRC, *Submission 60*, p. 5.

91 Reset Australia, *Submission 74*, p. 3.

> Legislation and regulations are only as good as a system's ability to enforce them consistently and reasonably. We urge the committee to reflect on the capacity of our national regulators such as the eSafety Commissioner and the Office of the Information Commissioner. Even at the level of individual complaint-handling, pressure on regulators is growing. For example, in the year between 2020-21 and 2021-22, eSafety received a 65% increase in reports of child cyber bullying and a 55% increase in reports of image-based abuse.
>
> Moreover, these regulators are negotiating with large international digital platforms with immense wealth and lobbying power. This poses challenges for regulators - for example, legislation may allow for digital platforms to be fined for certain practices, but regulators still need the resources to pursue these cases, especially if platforms decide to contest them.[92]

8.86 Dr Mitchell commented on the UK as an example:

> … the experience in the UK has also been that constant vigilance is needed. Certainly, there are still digital platforms there that are not operating to the standards of the code. So, whenever there's a new form of regulation introduced, it's very much an ongoing commitment that that regulator needs to have the resourcing, the expertise and the teeth to be able to monitor and enforce what they've introduced.[93]

New regulation

8.87 Reset Australia and UNICEF recommended new mandatory online safety codes should be implemented to bring Australia into line with comparable jurisdictions like the UK and California.[94]

8.88 Evidence recommended any new or revised regulation, such a children's code, include specific features such as:

- obligations to ensure data is processed in children's best interests;[95]
- writing privacy collection and consent notices in child friendly language;[96]
- banning collection of data for children under 18 (unless specifically necessary for the provision of that service);[97]

---

92 Alannah & Madeline Foundation, *Submission 41*, p. 9.

93 Dr Jessie Mitchell, Advocacy Manager, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 14.

94 Reset Australia, *Submission 74*, p. 19; Mr John Livingstone, Advocacy Manager, UNICEF Australia, *Proof Committee Hansard*, 26 July 2023, p. 26.

95 Mr John Livingstone, Advocacy Manager, UNICEF Australia, *Proof Committee Hansard*, 26 July 2023, p. 26.

96 Mr John Livingstone, Advocacy Manager, UNICEF Australia, *Proof Committee Hansard*, 26 July 2023, p. 26.

97 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13.

- banning or limiting the use of children's data for targeted advertising or other content;[98]
- banning children from contact with unknown adults that they know from their user profile are over the age of 18 and have not been explicitly tagged as friends or contacts; [99] and
- prohibiting the tracking, profiling, monitoring or targeting of children for commercial purposes.[100]

Best interests of the child

8.89 Some submissions recommended new regulations should be implemented that follow 'the best interests of the child' principle.[101] A proposal in the *Privacy Act Review Report 2022* recommended enshrining a principle that recognises the best interests of the child.[102]

8.90 UNICEF suggested application of the principle requires an assessment of the specific context and should have regard for all children's rights, including their rights to:

- seek, receive and impart information;
- be protected from harm; and
- have their views given due weight.[103]

8.91 It would also need to ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.[104]

8.92 Reset.Tech submitted best interests should be considered in data collection and processing:

> This means that where profiling, behavioural advertising or other uses are not clearly in young people's best interests, it should not be allowed … We also believe that children and young people should also have more control and say in how data is collected and used, where it is in their best interests and not too much has been collected … Lastly, as a principle, we believe that children and young people should have the right to delete their data. We would like to see clear and simple ways developed that young people can

---

98 See, for example, Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13; Reset Australia, *Submission 74*, p. 21; Ben Blackburn Racing, *Submission 1*, p. 9; Foundation for Alcohol Research and Education, *Submission 33*, p. 5.

99 Ms Sarah Davies, Chief Executive Officer, Alannah & Madeline Foundation, *Proof Committee Hansard*, 26 July 2023, p. 13.

100 Foundation for Alcohol Research and Education, *Submission 33*, p. 11.

101 See, for example, UNICEF, *Submission 14*, p. 4; Reset.Tech, *Submission 31*, p. 3; Alannah & Madeline Foundation, *Submission 41*, p. 3.

102 Attorney-General's Department, *Submission 51*, p. 17.

103 UNICEF, *Submission 14*, p. 4.

104 UNICEF, *Submission 14*, p. 4.

ask for their data to be deleted, including for advertising and profiling if it is collected.[105]

[105] Reset.Tech, *Submission 31*, p. 3.

Chapter 9
Emerging challenges

AI and the Metaverse

Overview

9.1 This chapter explains potential risks and proposed regulations for emerging technologies, with a focus on the artificial intelligence (AI) and the metaverse.

Artificial intelligence

9.2 Artificial intelligence is a broad term with no single agreed definition. AI algorithms guide how AI learns, adapts and make decisions. The Department of Industry, Science and Resources (DISR) explained AI as follows:

> Artificial intelligence (AI) refers to an engineered system that generates predictive outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.
>
> Machine learning are the patterns derived from training data using machine learning algorithms, which can be applied to new data for prediction or decision-making purposes.
>
> Generative AI models generate novel content such as text, images, audio and code in response to prompts.[1]

AI potential

9.3 Submissions highlighted the opportunities in technological growth offered by AI. For example, Microsoft advised it:

> … strongly believes in the potential for AI, particularly the recent advances in generative AI, to become a powerful tool for advancing critical thinking, stimulating creative expression, and discovering insights amid complex data and processes.[2]

9.4 The Tech Council of Australia also emphasised that Australia should seek to 'be a leader in best practice regulation of AI'. It noted that Australia should:

> … capitalise on the opportunities and new innovations presented by the use of these technologies, while mitigating the risks and potential harms. This includes being an active contributor to the international standards process. Any interventions should be complemented by measures to build

---

1 Department of Industry, Science and Resources (DISR), *Safe and Responsible AI: discussion paper*, p. 5.

2 Microsoft, *Submission 47*, p. 10.

awareness and capability among the public and private sectors to develop, use and govern algorithmic systems responsibly.[3]

Risks

9.5 While there are many potential benefits to the use of AI, stakeholders raised various concerns about the risks associated with this technology.

9.6 Evidence to the committee highlighted concerns about AI risks are consistent with the risks of algorithm use more generally. Social harm risks including unauthorised use of data for profiling, potential for increasing inaccurate and untruthful content, targeting and manipulation of users, inadvertent exclusion of local content and cultural material, and perpetuation of bias and discrimination are some of the concerns raised.

9.7 The committee notes digital platforms have implemented their own policies and systems striving for responsible AI.[4]

Growth of generative AI

9.8 The Gradient Institute explained that generative AI 'refers to a type of AI that is capable of creating new data or content, such as images, music, text, or videos'.[5]

9.9 The Office of the eSafety Commissioner (eSafety) outlined the following examples of generative AI applications in its Generative AI position statement:

- text-based chatbots, or programs designed to simulate conversations with humans, such as Anthropic's Claude, Bing Chat, ChatGPT, Google Bard, and Snapchat's My AI
- image or video generators, such as the Bing Image Creator, DALL-E 2, Midjourney, and Stable Diffusion
- voice generators, such as Microsoft VALL-E.[6]

9.10 eSafety highlighted how generative AI has rapidly improved thanks to recent advancements including 'the availability of more training data, enhanced artificial neural networks with larger datasets and parameters, and greater computing power'.[7]

9.11 For example, the Gradient Institute advised the new generation of chatbots based on generative AI are increasingly capable. These AI are:

---

3 Tech Council of Australia, *Submission 63*, p. 10.

4 See, for example, Microsoft, *Submission 47*, pp. 10–11; Meta, *Submission 69*, pp. 51–52; Amazon Web Services (AWS), *Submission 46*, p. 4.

5 Gradient Institute, *Submission 30*, p. 2.

6 Office of the eSafety Commissioner (eSafety), *Generative AI – position statement*, www.esafety.gov.au/industry/tech-trends-and-challenges/generative-ai (accessed 30 October 2023).

7 eSafety, *Generative AI – position statement*, (accessed 30 October 2023).

> … able [to] sustain coherent, human-like conversations with users that include answering queries, writing poetry, solving riddles, summarising ideas and reasoning about the emotional states of others.[8]

9.12 In a different use of generative AI, Amazon outlined how it is using a range of AI globally including creating customer reviews of products in their stores. Noting this system may not be operating in Australia yet, Mr Michael Cooley, Director, Public Policy Australia, Amazon Australia, advised:

> The system is actually creating those reviews based on other reviews so as to highlight different elements that customers are looking for when they're searching for products, whether that be low price or convenience or high utility.[9]

9.13 The committee noted the 2022 European Union's (EU) Europol agency's report that estimated that by 2026 about 90 per cent of online content will either be generated or manipulated by generative AI.[10]

Generative AI Risks

9.14 The committee heard that AI also brings with it a range of uncertainties.

9.15 The Australian Publishers Association, for example, noted that '[t]he potential impact of AI on book publishing, authorship, and copyright is only now just being thought through'.[11]

9.16 Submissions noted the growth in generative AI has the potential to amplify the risks seen in automated decision making (ADM) and traditional algorithms. eSafety commented:

> Companies are moving quickly to develop and deploy their own generative AI technologies. This may lead to not enough attention being paid to risks, guardrails, or transparency for regulators, researchers, and the public.[12]

Consolidation of market dominance

9.17 The committee was advised that generative AI has the potential to solidify the market dominance of digital platforms. The Gradient Institute explained:

> Generative AI is so resource intensive that it is almost exclusively the domain of Big Tech companies. Not only do big tech companies have the required expertise, computing power, and data to build these models, they have the platforms from which to deploy them.
>
> We believe that just as today, most interactions with content are moderated by Big Tech through social media, in the future most interactions with

---

8 Gradient Institute, *Submission 30*, p. 2.

9 *Proof Committee Hansard*, 22 August 2023, p. 5.

10 Senator Shoebridge, *Proof Committee Hansard*, 22 August 2023, p. 20.

11 Australian Publishers Association, *Submission 56*, p. 4.

12 eSafety, *Generative AI – position statement*, (accessed 30 October 2023).

> artificial personas will also be moderated through Big Tech. It is also clear that giving generative AI models more data and more computing power makes them much more capable, entrenching the existing advantages of Big Tech companies.[13]

9.18 Digital Rights Watch (DRW) similarly paints a picture of a Big Tech dominated market:

> Many economists have warned that AI will drive wages down, increase inequality and consolidate power in the hands of ever fewer corporations. But this is only true of AI developed, owned and led by private companies in the pursuit of profit.
>
> Machine learning and AI could prove to have many social and economic benefits, but only if the technology is governed democratically for the benefit of all. Decisions about how such finite computing resources are allocated is not something that can be left in the hands of a few private companies.[14]

Profiling

9.19 As discussed in Chapter 5: Data, the significant quantities of data captured by digital platforms can be consolidated to form detailed profiles of individual users including personal details, browsing habits and even geographical location.

9.20 Digital platforms utilise this data to train their AI learning systems.[15] For example, one submission outlined:

> Facebook's AI learning system, 'FBLearner Flow', ingests trillions of data points every day, from which its algorithmic models can make more than 6 million predictions per second.[16]

9.21 The committee was advised that, like personalisation of recommender systems and traditional algorithms, the use of data to personalise online experiences and prioritise content will have the same flow-on risks and social harm concerns. For example, the Gradient Institute noted:

> … the amount of personal data that Big Tech companies have about individuals may enable them to personalise generative AI chatbots more effectively, further increasing their manipulation capabilities.[17]

---

13 Gradient Institute, *Submission 30*, p. 3.

14 Digital Rights Watch (DRW), *Submission 68*, p. 19.

15 Mr Joshua Zubak, *Submission 27*, pp. 1–2.

16 Mr Joshua Zubak, *Submission 27*, p. 1.

17 Gradient Institute, *Submission 30*, p. 3.

Content risks

9.22 The committee was also warned about the risk of generative AI resulting in an increase of inaccurate and untruthful content.

9.23 Submissions advised that generative AI will likely increase the amount of inaccurate material online. The Australian Library and Information Association and National and State Libraries Australasia warned:

> Generative AI by its nature is not directed towards finding "truth" or "accuracy". And there is a significant risk that as the internet is populated by AI-generated content that this will become a self-referencing spiral as early mistakes are fed back into training data and reinforced.[18]

9.24 They further noted:

> Generative AI will introduce significant efficiencies and advances. It also is almost inevitably going to increase the amount of "bullshit" found online. As multiple commentators have noted over the years, the primary differential between bullshit and a lie is that someone who lies knows the truth and choses to conceal it, whereas bullshit is characterised by a disinterest in whether something is true or not.[19]

9.25 The use of generative AI in search engines has raised concerns about factual inaccuracy, a lack of source referencing and the potential for misinformation to be spread. DRW highlighted digital platforms continue to release generative AI to the market without addressing these concerns:

> In early 2023, controversy arose regarding the use of OpenAI's large language model chat bot, ChatGPT, to write articles. Microsoft's expanded partnership with OpenAI has seen ChatGPT technology already rolled out in their search engine Bing, and Google has since announced that it will be rolling out a chatbot named Bard to provide responses to some Google search queries.[20]

Identification of AI-created material

9.26 Stakeholders expressed concern around the identification of material created by generative AI and sought information on how big tech was approaching this challenge, including the options for disclosing and watermarking AI generated content.

9.27 Ms Kate Reader, General Manager, Digital Platforms Branch, the Australian Competition and Consumer Commission, noted:

> … transparency is one of the important things we consider will be valuable for consumers, and a watermark would certainly help, particularly in the

---

18 Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA), *Submission 57*, pp. 5–6.

19 ALIA and NSLA, *Submission 57*, pp. 5–6.

20 DRW, *Submission 68*, p. 28.

> scam space but also more generally in relation to understanding how content is produced.[21]

9.28 eSafety similarly expressed support for watermarking of AI generated material, advising:

> … the benefits of watermarking would probably go beyond online safety. I suspect they would be very useful in terms of protecting consumers from misleading material and dealing with any concerns with news quality et cetera. But that was something that I think was raised in eSafety's 'Tech trends position paper' on generative AI, which was released last week.[22]

9.29 Meta provided a commitment that its generative AI products within Australia will have watermarking features consistent with commitments made to the US Biden administration.[23] However, Meta was unable to provide an indicative timeframe for implementation, stating:

> Some of our additional tooling will most likely only be available in the US initially but our intention is to ensure that things are applied consistently across the platform.[24]

Manipulation through synthetic relationships

9.30 The advanced capabilities of generative AI raised further concerns around the ability to manipulate consumers on a more emotional level through artificial relationships.[25]

9.31 The Gradient Institute advised that with the ability 'to sustain coherent, human-like conversations with users that include answering queries, writing poetry, solving riddles, summarising ideas and reasoning about the emotional states of others', generative AI can be used to create synthetic personas. Users may form emotional bonds with synthetic personas leaving themselves vulnerable to manipulation by the entity in control of the chatbot.[26] The Gradient institute explained:

> The chatbot might, for example, be designed to convince the user to use certain products, or to subscribe to a particular political belief. These preferences and beliefs could be integrated into the chatbot's persona, making it difficult for users to even recognise the intentions of the chatbot's owners.[27]

---

21 *Proof Committee Hansard*, 22 August 2023, p. 36.

22 Ms Morag Bond, Executive Manager, Industry Regulation and Legal Services, eSafety, *Proof Committee Hansard*, 22 August 2023, p. 36.

23 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 21.

24 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 21.

25 eSafety, *Generative AI – position statement*, (accessed 30 October 2023).

26 Gradient Institute, *Submission 30*, p. 2.

27 Gradient Institute, *Submission 30*, pp. 2–3.

Current regulatory framework

9.32 A number of existing regulatory measures specifically capture AI design and development activity.

9.33 eSafety continues to promote the Safety by Design initiative which 'puts user safety and rights at the forefront of design and development of online products and services' and should apply to AI developments. eSafety advised:

> The online industry can take a lead role by adopting a Safety by Design approach. Safety by Design is built on three principles: service provider responsibility, user empowerment and autonomy, and transparency and accountability. Technology companies can uphold these principles by making sure they incorporate safety measures at every stage of the product lifecycle.[28]

9.34 In addition to a prevention approach, including education programs and resources, eSafety provides regulatory protections. The *Online Safety Act 2021* (OSA) 'provides eSafety with a range of powers and functions to address online safety issues, including those related to generative AI'.[29] eSafety noted:

> eSafety's four complaints-based investigations schemes do capture AI-generated images, text, audio, and other content which meets the legislative definitions of:
>
> - class 1 material (such as CSEA material and terrorist and violent extremism content) and class 2 material (such as pornography)
> - intimate images produced or shared without consent (sometimes referred to as 'revenge porn')
> - cyberbullying material targeted at a child
> - cyber abuse material targeted at an adult.[30]

9.35 Basic Online Safety Expectations reporting requirements include questions about the use of AI tools to detect illegal and harmful content.[31] This could be expanded in future to require service providers to report on the reasonable steps they are taking to ensure the safety of their generative AI functionalities.[32]

9.36 One proposed industry code developed under the OSA for internet search engine services was redrafted 'to capture proposed changes to search engines to incorporate generative AI features' with the aim of addressing risks associated

---

28 eSafety, *Generative AI – position statement*, https://www.esafety.gov.au/industry/tech-trends-and-challenges/generative-ai (accessed 30 October 2023).

29 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 25.

30 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 25.

31 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 25.

32 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 25.

with the use of generative AI to generate class 1 material prior to being registered.[33]

9.37 Additionally, the committee was advised that one of the Digital Platform Regulators Forum's key strategic priorities is a focus on understanding and assessing the benefits, risks and harms of generative AI.[34]

9.38 Further, DISR has published Australia's AI Ethics Principles guiding businesses and governments to undertake responsible AI design, development and implementation, ensuring it is 'safe, secure and reliable'.[35] The principles are a voluntary framework, intended to complement existing AI regulations and practices. The principles are:

- Human, societal and environmental wellbeing: AI systems should benefit individuals, society and the environment.
- Human-centred values: AI systems should respect human rights, diversity, and the autonomy of individuals.
- Fairness: AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.
- Privacy protection and security: AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.
- Reliability and safety: AI systems should reliably operate in accordance with their intended purpose.
- Transparency and explainability: There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them.
- Contestability: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
- Accountability: People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.[36]

Recent consultations and studies

9.39 A range of recent studies and consultation has been undertaken in the field of AI furthering discussion and knowledge in this emerging area.

---

33 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 2.

34 Ms Elizabeth Hampton, Deputy Commissioner, Office of the Australian Information Commissioner, *Proof Committee Hansard*, 22 August 2023, p. 27.

35 DISR, *Australia's AI Ethics Principles*, www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles (accessed 31 October 2023).

36 DISR, *Australia's AI Ethics Principles*, (accessed 31 October 2023).

9.40 The committee noted DISR conducted consultation into AI and ADM regulations in 2022.[37]

9.41 DISR also recently conducted a consultation process on safe and responsible AI considering 'what the Australian Government can do to support the safe and responsible use of AI'. The consultation, which closed on 4 August 2023, is assessing:

- voluntary approaches, like tools, frameworks and principles
- enforceable regulatory approaches, like laws and mandatory standards.[38]

9.42 In 2019 the Australian Government published an Artificial Intelligence Roadmap (the Roadmap). The Roadmap was co-developed by CSIRO's Data61 and the then Department of Industry, Innovation and Science and 'identifies strategies to help develop a national AI capability to boost the productivity of Australian industry, create jobs and economic growth, and improve the quality of life for current and future generations'.[39]

Guiding the future of AI development

Cooperation and consultation

9.43 Stakeholders highlighted the essential need for international collaboration in the regulation of generative AI in addition to collaboration among existing local regulators. Indeed, Australia is involved in international forums and discussions:

> eSafety is actively involved in bilateral and multilateral discussions on emerging technologies, including through the Global Online Safety Regulators Network, to promote Australia and eSafety's perspectives on online safety regulatory issues.[40]

9.44 Various submissions discussed the need for engagement with government, both domestically and internationally.

---

37 DISR, *Positioning Australia as a leader in digital economy regulation (automated decision making and AI regulation*, May 2022.

38 DISR, *Responsible AI in Australia: have your say*, 1 June 2023, www.industry.gov.au/news/responsible-ai-australia-have-your-say (accessed 31 October 2023).

39 CSIRO, *Artificial Intelligence Roadmap*, *'Artificial Intelligence: solving problems, growing the economy and improving our quality of life'*, www.csiro.au/en/research/technology-space/ai/artificial-intelligence-roadmap (accessed 31 October 2023).

40 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 22.

9.45 Amazon noted that it was working with the Australian and other governments to grapple with issues relating to AI such as ethical guidelines and policy controls.[41]

9.46 Meta also advised it has been engaging with DISR on the safe and responsible AI in Australia consultation process.[42]

9.47 The Gradient Institute advised:

> The Australian Government should seek to establish an expert advisory committee with diverse and relevant expertise on AI risks and AI safety, drawing broadly from industry, government, academia, the nonprofit sector and the broader civil society, to monitor the rapidly evolving AI risks and provide ongoing advice to the Government on how Australia should best respond to those risks.[43]

9.48 Microsoft also highlighted the need for skilled technological leaders. It advised:

> Australia, its allies, and other democratic societies will need multiple and strong technology leaders to help advance AI, with broader public policy leadership and cooperation on topics including data, AI supercomputing infrastructure and talent.[44]

Considerations

9.49 A number of principles and values need to be considered when designing AI governance frameworks.

9.50 The Consumer Policy Research Centre (CPRC) advised of six key principles 'critical to include in AI and ADM architecture to ensure improved consumer outcomes.' These are accessibility, accountability, agency, transparency, understandability and explainability, and sustainability. It stated:

> We recommend that the Government also prioritise the development of innovation enablers to support technology that will create genuine benefits for all Australians. Innovation enablers should include:
>
> - investing in and enabling AI and ADM innovation in the not-for-profit sector to demonstrably improve community outcomes and welfare, and
> - implementing regulatory sandboxes to enable the safe testing and learning environment prior to deploying AI and ADM-enabled products and services at scale.[45]

9.51 However, DRW noted the risks of regulatory sandboxes:

---

41 Mr Michael Cooley, Director, Public Policy Australia, Amazon Australia, *Proof Committee Hansard*, 22 August 2023, p. 5.

42 Ms Mia Garlick, Regional Director of Policy, Meta, *Proof Committee Hansard*, 22 August 2023, p. 21.

43 Gradient Institute, *Submission 30*, p. 4.

44 Microsoft, *Submission 47*, p. 11.

45 Consumer Policy Research Centre, *Submission 60*, p. 4.

> Regulatory sandboxes can be a dangerous experiment, even those for good reasons. A better approach might be pre-emptive regulation or co-governance frameworks, like those suggested by Fairwork in their model standards for the fair implementation of artificial intelligence.[46]

9.52 UNICEF advised the committee that AI development must ensure the wellbeing of children in the AI world. It recommended the development of AI systems needs to be guided 'to ensure they are child-centred, protecting children, providing equitably for their rights, and empowering them to participate in an AI world'.[47]

9.53 The OECD published guiding principles on AI in May 2019 'which includes human-centred values and fairness, transparency and explainability, robustness, security and safety, inclusive growth and sustainable development, and accountability'.[48]

9.54 The committee also noted support for risk-based regulatory models.[49] For example, Amazon Web Services stated:

> We support AI governance efforts that take a risk-based approach to addressing the responsible use of AI, such as Australia's AI Ethics Principles, the OECD's AI Principles, and Singapore's AI Governance Framework.[50]

The case for regulation

9.55 The committee was advised that a regulatory approach to generative AI was essential.

9.56 The Gradient Institute advised 'measures to mitigate the risks of generative AI manipulation are required urgently'.[51] Noting Big Tech companies are 'competing to develop, deploy and monetise generative AI in general, and chatbots in particular', the Gradient Institute highlighted:

> … the scale of the risk, and the previous failure of market forces to control AI-driven manipulation by Big Tech in social media, imply the need for strong regulation of generative AI manipulation.[52]

---

46 DRW, *Submission 68*, p. 32.

47 UNICEF, *Submission 14*, p. 11.

48 eSafety, *Submission 2*, p. 10.

49 See for example, eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 22; AWS, *Submission 46*, p. 4.

50 AWS, *Submission 46*, p. 4.

51 Gradient Institute, *Submission 30*, p. 3.

52 Gradient Institute, *Submission 30*, p. 3.

International approaches

9.57 eSafety outlines in its AI position statement the myriad of international approaches to generative AI, from voluntary principles and standards to legislation and mandatory requirements:

- voluntary principles and governance frameworks (India)
- AI governance frameworks, third-party testing and verification technology (Singapore)
- application of existing consumer safety and data regulations and the signing of pledges around self-regulatory principles (US)
- audits, risk and impact assessments and pre-launch disclosure requirements for 'high-risk AI' (Canada, UK and South Korea)
- new and enforceable rules, including supervision powers (China)
- dedicated AI legislation (EU, Canada, South Korea, Brazil)
- intermediate bans on generative AI technology (Italy).[53]

9.58 The committee was advised that the 'newly published AI Risk Management Framework from the U.S. Institute of Standards and Technology offers a helpful roadmap for AI governance'.[54] Microsoft stated:

> We encourage federal and local governments to leverage its contents to help organisations identify and address the potential risks of AI systems, encouraging interoperability with publicly developed best practices.[55]

Dedicated Legislation

9.59 eSafety highlighted the EU's Digital Services Act 'provides harmonised rules on AI, outlining its risk- based approach to the regulation of AI'.[56]

9.60 Further, eSafety advised the committee that the EU Artificial Intelligence Act is the first law on AI proposed by a major regulator.[57] The proposed law:

> … assigns applications of AI to three risk categories: first, applications and systems that create an unacceptable risk, such as government-run social scoring are banned; second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements; lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.[58]

---

53 eSafety, *Tech Trends Position Statement – Generative AI*, August 2023, p. 21.

54 Microsoft, *Submission 47*, p. 11.

55 Microsoft, *Submission 47*, p. 11.

56 eSafety, *Submission 2*, p. 10.

57 eSafety, *Submission 2*, pp. 9–10.

58 eSafety, *Submission 2*, p. 10.

The metaverse

9.61 The metaverse is a concept that is still evolving, and companies mean different things when referring to it. Generally, it refers to the concept of an immersive online world where people can gather to socialise, work or play.[59]

9.62 The Alannah & Madeline Foundation explained:

> There is no single, accepted definition of the 'metaverse' - indeed, many stakeholders don't use the term, preferring other framings such as 'immersive technologies' or 'extended reality'. As a generalisation, these technologies are understood to have the following features:
>
> - Realistic - 3D virtual environments which participants perceive as lifelike
> - Immersive - the participant feels partly or fully immersed in this space
> - Interactive - participants interact with their surroundings and other participants, engage in transactions, and create content
> - Interoperable or integrated - participants travel (fairly) seamlessly between virtual spaces, taking their virtual assets with them
> - 24/7 - digital spaces exist in real time and are 'always on'
> - Virtual economy - a digital economy powers the metaverse, with blockchain and cryptocurrencies enabling trade and purchase of digital items.[60]

9.63 eSafety commented on the potential benefits of new technologies such as the metaverse:

> Immersive technologies and emerging online environments, such as the metaverse, provide a range of opportunities – in entertainment, education, defence, health sciences and other fields. Being able to practise a skill virtually or to understand an experience from an unfamiliar point of view are valuable applications. Immersive experiences can also improve the quality of life and independence of people who are unable to access actual experiences for a variety of reasons, including disability, age, caring responsibilities, transport access or remoteness, and can help people build empathy by experiencing a virtual world from different perspectives.[61]

Potential harms

9.64 All harms relating to digital platforms examined in the preceding chapters of this report also apply to, and may be amplified in, the metaverse.

9.65 Evidence specifically discussing potential harms arising from and being in the metaverse are discussed below.

---

[59] Merriam-Webster, *What is the 'metaverse'?*, 30 October 2021, www.merriam-webster.com/wordplay/meaning-of-metaverse (accessed 30 October 2023).

[60] Alannah & Madeline Foundation, *Submission 41*, p. 11.

[61] eSafety, *Submission 2*, p. 15.

Data and wellbeing concerns

9.66 Submissions raised concern about the large amount of data likely to be collected in the metaverse.[62] Excess collection and collation of personal data could lead to an increase in scams, identity theft and fraud. Risks of data collection and aggregation are elaborated on in Chapter 5: Data.

9.67 Data collection in the metaverse may include collection and aggregation of sensitive biometric information, such as eye movements, voice recordings, measurement of movements, heart rate, fingerprints, location and behaviour of users, adding additional risks around profiling, targeted marketing, fraud and data breaches.[63]

9.68 The Foundation for Alcohol Research and Education (FARE) commented on the risks to wellbeing from metaverse data collection:

> The monitoring of biometric data such as heart rate, eye movement and pupil dilation, which are integrated into the development of immersive visual reality technology for functionality purposes could be used to provide real-time psychological insights for marketing and retail purposes. For alcohol and other addictive products, this could mean that addictive tendencies and stressors could be detected and used to target marketing and encourage the purchase and use of harmful and addictive products like alcohol.[64]

9.69 Targeted marketing of harmful products is an issue for consumers across all digital platforms. Submissions raised concerns that data collection in the metaverse may be highly targeted.[65]

9.70 FARE argued that this targeting may be exacerbated in the metaverse:

> However, the promotion and sale of alcohol in the Metaverse will be even more engaging tha[n] that available through the digital platforms discussed in the above sections of this submission as we see e-commerce transition to i-commerce (immersive commerce). This has implications for both the effect of alcohol marketing and also for the increasing availability of alcohol in the community. The engaging nature of alcohol promotion and sale in the Metaverse is likely to have greater influence on people's attitudes toward and purchasing and use of alcoholic products. Research with Australian adolescents and young adults indicates that engaging with digital marketing for unhealthy food and beverages is associated with consumption of unhealthy food and beverages, and that engaging with this

---

62 See, for example, Foundation for Alcohol Research and Education (FARE), *Submission 33*, p. 14; eSafety, *Submission 2*, p. 15; Alannah & Madeline Foundation, *Submission 41*, p. 12.

63 See, for example, FARE, *Submission 33*, p. 14; eSafety, *Submission 2*, p. 15; Alannah & Madeline Foundation, *Submission 41*, p. 12.

64 FARE, *Submission 33*, p. 14.

65 Cancer Council, *Submission 5*, [p. 2].

> marketing has a stronger impact than exposure alone (i.e., as was previously the case with traditional media advertising).[66]

9.71 The Alannah & Madeline Foundation was concerned the metaverse could exacerbate the wellbeing concerns already being observed from increased digital engagement in the community such as loneliness, disassociation, desensitisation, dysregulated behaviours, body image problems, and social and political polarisation.[67]

Criminal behaviour

9.72 Stakeholders were concerned that the metaverse could be used to engage in harmful or criminal behaviour, such as grooming, sexual abuse, bullying, discrimination, threats, defamation, identity theft, assault, cyber-attacks and scams.[68]

9.73 eSafety commented on the potential for significant harms in the metaverse:

> eSafety is concerned that these technologies can be used for cyberbullying, grooming children for online sexual abuse, and image-based abuse. Further, forms of assault might be experienced virtually including through a haptic suit. Augmented realities could also be used to fake a sexually explicit three-dimensional image or video of a real person and interact with it without their consent. While a virtual experience may be considered private due to being physically isolated, there is a risk that an intimate image or video created in that environment could then be livestreamed, stored, or shared without consent.[69]

9.74 The Centre for AI and Digital Ethics submitted that the potential for scams is higher with new technology developments:

> The mystique of new technology and ambiguity around regulation exposes Australians to scams and fraud-much as what happened with cryptocurrencies and NFTs [non-fungible token]. Virtual investment properly offers another easy backstory for scammers to tell their marks … The Australian government should expect a wave of fraud related to virtual investment property schemes because of the similarities with the cryptocurrency market. The Australian Competition and Consumer Commission 's report on Scam Activity stated that cryptocurrency investment scams were the "main driver" of the sharp 35% increase in investment scam losses in 2021 from the previous year, with Australians reporting $99 million lost to these scams. Given the growing interest in virtual reality, it is likely that similar fraudulent activities will occur in this market, posing a significant risk to Australian investors.[70]

---

66 FARE, *Submission 33*, p. 14.

67 Alannah & Madeline Foundation, *Submission 41*, p. 12.

68 See, for example, eSafety, *Submission 2*, p. 15; Alannah & Madeline Foundation, *Submission 41*, p. 12.

69 eSafety, *Submission 2*, p. 15.

70 Centre for AI and Digital Ethics, *Submission 23*, [p. 7].

Current regulatory framework

9.75 Activities by digital platforms expanding into the metaverse are encapsulated by existing regulations in relation to safety, privacy, competition, and consumer requirements as explored in previous chapters. There is no metaverse specific legislation.

Proposed solutions

When to implement regulation

9.76 Many submissions argued that regulation capturing operation and use of the metaverse should be implemented now, rather than waiting until metaverse technology is more developed.[71]

9.77 The CPRC recognised the need for immediate regulation:

> We are beyond the waiting game now when it comes to developing adequate consumer protections for products and services in the digital economy. It is clearly evident that a self-regulatory or self-assessed approach is no longer adequate in addressing the risks posed to consumers by large and powerful digital platforms. We need the Federal Government to be proactive and not wait for Australians to endure harm first before creating safeguards for them.[72]

9.78 Mr Mark Nottingham, expert advisor to the United Kingdom Competition and Markets Authority's Digital Markets Unit, argued that it is best to implement regulation now, while the metaverse is still being designed, 'since making incompatible changes to technical architectures at scale is notably difficult'.[73]

9.79 Similarly, the Alannah & Madeline Foundation remarked:

> We believe it is important for legislators and regulators to be on the 'front foot' with regard to new digital technologies. Many decision-makers took years to respond to developments like social media and smartphones; arguably this delay contributed to the many concerns that exist nowadays in relation to children's use of technology.[74]

9.80 The Centre for AI and Digital Ethics recommended regulators 'take a proactive approach [to] a) policing violations of existing consumer protection law and b) protecting competition as firms explore virtual reality offerings'. It added:

> However, because virtual reality products show genuine potential to become pervasive in civic life, it is critical that regulators ensure that

---

71 See, for example, Children and Media Australia, *Submission 53*, p. 4; Alannah & Madeline Foundation, *Submission 41*, p. 10; Mr Mark Nottingham, *Submission 37*, p. 6.

72 CPRC, *Submission 60*, p. 8.

73 Mr Mark Nottingham, *Submission 37*, p. 6.

74 Alannah & Madeline Foundation, *Submission 41*, pp. 10–11.

> competition concerns are adequately policed and that we learn the last decade's lesson limits of platform self-governance.[75]

Broad legislation

9.81 Submissions supported broad risk or principle-based legislation to capture the metaverse and other new technologies as they emerge.[76]

9.82 Children and Media Australia argued the metaverse is:

> … likely to evolve rapidly, posing challenges for law and regulation in keeping up. This is all the more reason to craft regulations that strike at the heart of the risks posed, rather than addressing particular platforms or practices.[77]

9.83 The Alannah & Madeline Foundation supported 'safety by design' and suggested regulatory models be crafted in a way that they can capture new technologies. Regulation should be:

- high-level enough to remain relevant as new digital technologies emerge, such as immersive technologies or 'extended reality' (aka the 'metaverse')
- Support investment in research and policy development concerning the likely societal, economic and legislative implications of immersive technologies emerging via pathways like the 'metaverse'. Any policy and legislation developed in response should be informed by expertise on the rights of the child and should treat the best interests of the child as the primary consideration in relation to the handling of children's data by digital platforms.[78]

9.84 The Australian Research Alliance for Children and Youth (ARACY) recommended consideration of its evidence-based wellbeing framework, The Nest, which offers a guide for navigating the dimensions of the metaverse from a child's perspective and providing a foundation for safety-by-design processes and indicators of success.[79] It commented:

> Taking this approach can foster innovative solutions to potential harms or risks without necessarily stifling development and maximising the opportunities of the Metaverse. In addition, ongoing, real-time exploration of the hopes for the Metaverse by users as well as their attitudes to potential

---

75 Centre for AI and Digital Ethics, *Submission 23*, [p. 7].

76 See, for example, CPRC, *Submission 60*, p. 8; Children and Media Australia, *Submission 53*, p. 4; Australian Research Alliance for Children and Youth (ARACY), *Submission 21*, [p. 2]; FARE, *Submission 33*, p. 5.

77 Children and Media Australia, *Submission 53*, p. 4.

78 Alannah & Madeline Foundation, *Submission 41*, p. 5.

79 ARACY, *Submission 21*, [p. 2].

> harms must be taken into consideration, as this can enable a less reactive approach to regulatory interventions.[80]

9.85 ARACY added:

> We consider that modelling a process and associated regulatory framework similar to the development and approval of new drugs and medical technologies, or even vehicle safety testing, would be a beneficial starting point. The required testing and reporting on safety-by-design components for Metaverse developments and the ethics considerations necessary for testing will assist in embedding the question 'just because we could, should we?' in research and development. A regulatory framework will subject all companies operating in this space to the same time frames and requirements prior to going to market.[81]

9.86 Similarly, FARE argued in favour of proactive and systematic regulatory measures for the metaverse and other emerging technologies that include the following principles:

> - A primary consideration of preventing harm from digital platform business activities, and
> - Minimum standards that require [that] digital platforms do not act in ways that put people using platforms at risk of harm, including to their health and wellbeing.[82]

International collaboration

9.87 Submissions suggested international cooperation between governments and companies is important to ensure adequate and consistent regulation.[83]

9.88 ARACY supported a global framework:

> An international regulatory framework could be developed and regularly updated through an international multidisciplinary body. This could fall under the auspices of the International Telecommunications Union with each member state implementing the regulations through their national bodies, for example, the eSafety Commission in Australia. The international regulatory framework would then provide the basis for developing national regulations and legislations. A multidisciplinary body should also be appointed to monitor the regulations and to determine any changes to them over time. Enforcement could continue, in Australia, under the eSafety Commission or affiliated body.[84]

9.89 Blockchain Australia also indicated there is a need for legislative agreements across borders and added:

---

80 ARACY, *Submission 21*, [p. 4].

81 ARACY, *Submission 21*, [p. 4].

82 FARE, *Submission 33*, p. 5.

83 See, for example, ARACY, *Submission 21*, [p. 4]; Blockchain Australia, *Submission 45*, [p. 13.]

84 ARACY, *Submission 21*, [p. 4].

A key component will be intelligence gathering and collaboration with the tech firms involved in developing these experiences. This emphasises the need to build partnerships with Telco companies, which possess the infrastructure through which attacks are perpetrated. Developers must be included in the security process and need precision training on the vulnerabilities that they are likely to face. Governments need to start developing approaches to defend against threats now, such as the controls to remove bad actors and user education.[85]

[85] Blockchain Australia, *Submission 45*, [p. 13].

Chapter 10
The way forward

Overview

10.1 This chapter explores evidence received about regulatory fragmentation. It goes on to outline the committee's views on the evidence discussed throughout this report and make recommendations.

Regulatory fragmentation

10.2 Submitters raised concerns that the current digital platforms sphere involves duplicated and overlapping regulations, and there is a need for a coordinated approach to digital regulation.[1]

10.3 BSA – The Software Alliance (BSA) suggested 'the Committee consider the broader issue of how to reduce regulatory overlap, including by promoting improved coordination between regulators, policymakers, and the private sector'.[2]

10.4 The Tech Council of Australia stated regulation:

> … should aim to deliver a more coordinated and cohesive approach to digital regulation that enables long-term growth of the Australian technology sector in the national interest, including by avoiding overly broad or piecemeal approaches to regulation, which our research has found to be a key barrier to innovation and capturing the benefits of new technologies.[3]

10.5 Significant regulatory gaps were also highlighted in evidence to the committee. For example, the committee questioned Digital Platforms Regulators Forum (DP-REG) members about which agency held responsibility for protecting Australians from spending on unused subscription fees. The DP-REG members were unable to point to an agency that would hold that remit.

10.6 Senator Shoebridge asked:

> Isn't this one of the problems in this whole space? There's no lead agency. There's no-one who's ultimately responsible. It must frustrate you no end, which is one of the reasons you've brought together this informal forum. There's just no lead agency, is there?[4]

---

1 See, for example, BSA – The Software Alliance, *Submission 32*, p. 2; Tech Council of Australia (TCA), *Submission 63*, p. 4; Australian Information Industry Association, *Submission 16*, [p. 3]; Tech Policy Design Centre, *Submission 22*, p. 1.

2 BSA – The Software Alliance, *Submission 32*, p. 3.

3 TCA, *Submission 63*, p. 4.

4 *Proof Committee Hansard*, 22 August 2023, p. 33.

10.7 Ms Elizabeth Hampton, Deputy Commissioner, Office of the Australian Information Commissioner (OAIC), responded:

> I don't agree that it's the frustration around a lack of a lead agency that caused us to coalesce and come together. Instead, we've reflected on the fact that we each have an important different lens to bring to a set of issues, and it's the coordination of those different lenses that results in a really good outcome for Australians.[5]

10.8 In response to committee concerns that there is no agency with ultimate responsibility when regulatory gaps are identified, Ms Creina Chapman, Deputy Chair, the Australian Communications Media Authority, explained:

> The gap is not in the regulators; the gap is not in the fact that there is not a regulator that has responsibility for it. If there is a gap, it is a legal gap.[6]

Proposed solutions

Upskill and empower existing regulators

10.9 Submissions recommended upskilling existing regulators, such as the Australian Competition and Consumer Commission (ACCC) or OAIC, so they have the adequate skills and resources to regulate the behaviour of digital platforms.[7]

10.10 The Consumer Policy Research Centre stated regulators need specific expertise to regulate digital platforms:

> Monitoring and surveillance by regulators in this complex environment needs a diverse workforce that not only understands the implications of the law but also the technical architecture on which these business models are built upon. Experts such as data scientists, artificial intelligence engineers, information security analysts and other technical professionals need to be in the mix to support upstream regulation and mitigate the risk to consumers, potentially before widespread harm has occurred.[8]

10.11 Similarly, the Human Rights Law Centre (HRLC) supported a comprehensive regulatory framework that includes 'broad information-gathering and enforcement powers for an independent, well-resourced and integrated

---

5 *Proof Committee Hansard*, 22 August 2023, p. 33.

6 *Proof Committee Hansard*, 22 August 2023, p. 33.

7 See, for example, Centre for AI and Digital Ethics, *Submission 23*, [p. 3]; CHOICE, *Submission 54*, p. 3; Tech Policy Design Centre, *Submission 22*, p. 1; Consumer Policy Research Centre, *Submission 60*, p. 6; Australian Small Business and Family Enterprise Ombudsman, *Submission 39*, p. 3.

8 Consumer Policy Research Centre, *Submission 60*, p. 6.

regulator'.[9] The HRLC told the committee this regulator should be empowered and have robust information-gathering powers.[10]

Better coordination between regulators and policy makers

10.12 Evidence to the committee also recommended the creation of a new model of coordination between existing regulators and policy makers.[11]

10.13 .au Domain Administration Ltd (auDA) told the committee that closer engagement with stakeholders is needed at all stages of policy development. It advocated for coordinated efforts between regulators, policy makers, the private sector, technical community, academia, and civil society. It recommended:

> … all relevant regulators and government departments actively participate in a multi-stakeholder policy development approach. This would help to avoid siloes and overlapping consultation processes facilitated by different government entities and drive greater certainty amongst industry and consumers.[12]

10.14 Similarly, BSA stated DP-REG is comprised of only regulators, with policy makers and industry representatives absent from the conversation. It recommended considering the Australian National University's Tech Policy Design Centre's (ANU Tech) proposed model to increase involvement from industry representatives and independent technical expertise. BSA argued:

> The increased involvement of industry representatives will provide the government with access to independent technical expertise and a regular platform for consultations. More importantly, it will discourage taking a reactionary approach when addressing emerging concerns and ultimately will pave the way for a more certain regulatory environment.[13]

10.15 ANU Tech's proposed 'Tech policy coordination model' includes the following layers of coordination:

- The Tech Policy Ministerial Coordination Meeting is the peak Ministerial coordination body in the Australian tech-ecosystem. Its objective is to facilitate cross-portfolio Ministerial coordination before tech policy proposals are taken to Cabinet.
- The Tech Policy Council is the peak senior officials' coordination body in the Australian tech-ecosystem. Its objective is to improve coordination among and between policymakers and regulators.

---

9 Human Rights Legal Centre (HRLC), *Submission 50*, p. 5.

10 HRLC, *Submission 50*, p. 11.

11 See, for example, Tech Policy Design Centre, *Submission 22*, p. 2; Communications Alliance, *Submission 58*, p. 7; Tech Council of Australia, *Submission 63*, p. 5.

12 .au Domain Administration Ltd (auDA), *Submission 26*, p. 8.

13 BSA – The Software Alliance, *Submission 32*, p. 7.

- The Tech Regulators Forum is the peak regulator coordination body in the Australian tech-ecosystem. Its objective is to improve coordination among tech regulators.[14]

10.16 auDA supported ANU Tech's model as it 'does not change any existing mandates of Ministers, departments or agencies, but helps cultivating coordination at all stages of tech policy development'.[15]

10.17 The Australian Information Industry Association noted ANU Tech's proposal and similarly recommended establishing a Council of Tech Regulators which:

> … would work to a similar model as the Council of Financial Service Regulators and be comprised of authorities such as the eSafety Commissioner, the Australian Information Commissioner, the Digital Transformation Agency, the Department of Home Affairs, Treasury, the Attorney General's Department and the Australian Cyber Security Centre. The Council would ensure that, as far as possible, regulation is streamlined and rationalised to mitigate overregulation, red tape, duplicative reporting requirements and parallel consultation timeframes. Breaking down silos and ensuring that in respect of technology – the all-pervasive, innovative and value-creating engine at the heart of the economy – the left hand of government knows what the right is doing as far as regulation and reporting is concerned, and regulatory impost is contained as far as possible.[16]

Parliamentary committee

10.18 The HRLC recommended a dedicated Parliamentary committee on digital matters be established to acknowledge the ongoing attention required on emerging tech issues and policy coordination across Government.[17]

10.19 A joint submission from multiple research organisations similarly proposed Parliament establish a Joint Standing Committee on Digital Affairs. They stated:

> A dedicated standing Committee would allow for a better allocation of time, resources and expertise and help develop a more sophisticated understanding of digital and technology policy. Existing portfolio committees are overworked and their broad remits mean that they neither have the capacity nor time to proactively interrogate emerging tech issues.[18]

A digital platforms specific body

10.20 Some submissions raised support for a new digital platforms specific body.

---

14 Tech Policy Design Centre, *Submission 22*, p. 2.

15 auDA, *Submission 26*, pp. 5–9.

16 Australian Information Industry Association, *Submission 16*, pp. 4–5.

17 HRLC, *Submission 50*, p. 9.

18 Joint submission from Digital Rights Watch, Electronic Frontiers Australia, Tech Policy Design Centre, Centre for New Industry, Professionals Australia and Australia Institute, *Submission 62*, [p. 1]. Also see Digital Rights Watch, *Submission 68*, p. 40.

10.21 Ben Blackburn Racing recommended consideration of 'the introduction of a new Australian Government agency which could bring more independence to oversight of the influence and decision-making structures of Big Tech companies and their impacts in Australia'.[19]

10.22 Mr Rupert Taylor-Price, Chief Executive Officer, Vault Cloud, discussed how there is no clear regulator in the digital platforms space, and there needs to be one:

> It's a bit like when you get on a plane. To some degree, you don't have to worry too much about who's providing you that service. You know that it's a well-regulated industry. You know that there's a degree of safety by getting on that plane. That's what CASA and other regulators in that space affect in the outcome that they get for their citizens. In the technology space, say that you didn't like the way an algorithm had worked for you in some way on one of these platforms. How do you deal with that? If you go to a bank, you go to APRA. If you get on a plane, you go to CASA. Who do you go to as a citizen when you have an issue with a technology platform?[20]

10.23 The Law Institute of Victoria recommended:

> … the introduction of a new government regulatory authority, or the establishment of a collaborative team across existing regulatory bodies, tasked with overseeing the regulation of Big Tech companies specifically … [it] would need to be sufficiently resourced in order to provide any meaningful opportunity for appropriate regulation.[21]

10.24 Ms Kate Pounder, Chief Executive Officer, Tech Council of Australia, stated the US National Institute of Standards and Technology (NIST) could be examined as a model that brings together competition, consumer and data issues. NIST is an agency of the US Department of Commerce, that produces standards and guidelines with expertise. Ms Pounder stated:

> … often in these new areas, particularly when technology is moving fast, there's not a high degree of expertise. So I think centralising that in one body, which can provide expert guidance to governments and work fairly rapidly to get standards and guidance material out, is vital. It can take a science based and evidence based model. Often the work of NIST ends up being utilised in other markets. I think there's also an opportunity for Australia to simply leverage that a bit better and aim for coherence with some of the guidelines that come out there. It often tends to happen in the private sector, because an Australian company that's successful in the tech sector will be selling globally, so they might look to those guidelines and try to adhere to them.[22]

---

19 Ben Blackburn Racing, *Submission 1*, p. 9.

20 *Proof Committee Hansard*, 26 July 2023, p. 22.

21 Law Institute of Victoria, *Submission 12*, [pp. 3–4].

22 *Proof Committee Hansard*, 27 July 2023, p. 44.

10.25 Digital Rights Watch recommended a Minister for Digital Capabilities be appointed.[23]

Committee view

10.26 This section provides the committee's view on key themes and concerns raised throughout this inquiry and the committee's recommendations.

Regulation

10.27 Throughout this report and particularly earlier in this chapter, evidence was presented that the current regulatory system is not working effectively. Regulation of digital platforms is split across various agencies, in some cases with competing priorities.

10.28 The committee found that the current legislative and regulatory framework is not sufficient to ensure positive outcomes for consumers and competition. In short, it is fragmented.

10.29 The committee acknowledges the importance of well-resourced and appropriately skilled regulators to ensure adequate enforcement efforts achieve the desired outcomes. The committee is concerned that upskilling existing regulators alone will not resolve regulatory gaps or provide the expertise needed to address emerging competition and consumer risks.

10.30 Stakeholders highlighted that despite the market power of Big Tech and potential for harm, digital platforms are not regulated like other significant industries, such as banks, telecommunications providers and airlines. The committee considers that a new regulatory regime could address fragmentation and bolster regulatory efficacy.

10.31 Evidence to the committee also highlighted the need for better coordination between regulatory bodies and policymakers. Improved coordination would streamline legislation and regulatory efforts. Further, a coordinating body would give consumers and digital platforms certainty about where to turn to when issues arise.

10.32 Accordingly, the committee recommends a new coordination body be established, which does not alter or acquire the day-to-day functions of the four main DP-REG agencies but coordinates collaboration efforts, common responsibilities and tasks.

Recommendation 1

10.33 The committee recommends that the Australian Government establish a digital platforms coordination body.

---

23 Digital Rights Watch, *Submission 68*, p. 40.

Competition

10.34 Chapters 3 and 4 considered issues that have arisen due to the concentrated market power of Big Tech. The committee heard evidence that the dominant market power of Big Tech has allowed these firms to engage in anticompetitive behaviours and exploit power imbalances to the detriment of small businesses and consumers.

10.35 A range of submitters told the committee that the market power of Big Tech allows these firms to engage in anticompetitive tying and self-preferencing. These practices make it difficult for other companies, particularly small businesses, to compete, resulting in reduced competition, less choice for consumers and increased prices.

10.36 The committee has heard that Big Tech platforms may impede consumers from switching products or services through tying practices that lock consumers in to one provider.

10.37 Submissions raised concerns that app store providers tie the use of app store services to the use of their in-app payment (IAP) services. App stores take up to a 30 per cent commission on every IAP and restrict app-developers from providing their own IAP mechanisms.

10.38 The committee is concerned that the tying of IAPs creates a barrier to entry for competitors and limits the choices available to consumers. Further, the committee believes there is a lack of transparency in how commission fees are determined, and how app stores use the IAP data they collect.

10.39 Furthermore, the committee has heard that regulation of near-field communication mobile device components and mobile wallets is needed to ensure consumers have similar rights against large digital platforms compared to regulated financial institutions that provide payment services.

10.40 Other jurisdictions such as the European Union (EU) and South Korea have introduced measures that require major app store operators such as Apple and Google to unbundle the use of their proprietary in-app payment systems from the use of app distribution services.

10.41 Accordingly, the committee supports introduction of legislation that will address anti-competitive tying by Big Tech platforms to ensure a level and competitive playing field.

Recommendation 2

10.42 The committee recommends that the Australian Government introduce legislation to prevent anti-competitive practices through the bundling of payment services and products by large digital platforms.

10.43 The committee is concerned that self-preferencing conduct may be anti-competitive and create barriers to entry for small businesses.

10.44 Multiple submissions called for regulation that tackles anti-competitive self-preferencing by gatekeeper companies and referred to international approaches that could be adopted. For instance, the United Kingdom (UK) has proposed a pro-competition regime for digital markets. This regime will include measures to address anti-competitive self-preferencing by requiring digital platforms to not influence competitive processes or outcomes in a way that unduly self-preferences a platform's own services over that of its rivals.

10.45 The committee is of the view that there needs to be greater transparency on the part of large digital platforms regarding the practice of self-preferencing their own products.

10.46 The committee believes this warrants mandatory public disclosure by large international platforms when they engage in self-preferencing behaviour for their own products on app-stores and other digital markets. Furthermore, large digital platforms should disclose aggregate information on the data collected from customers and business users for reasons other than the app review process.

Recommendation 3

10.47 The committee recommends that the Australian Government require mandatory disclosure by large digital platforms of self-preferencing conduct.

Dispute resolution

10.48 In Chapter 4, the committee considered consumer redress options within the digital economy. While Big Tech firms invest in a range of mechanisms to prevent and minimise problems for consumers, a significant number of problems and disputes are unable to be resolved within existing systems.

10.49 Internal dispute resolution mechanisms provided by digital platforms are an important first point of redress. However, consumers encounter many difficulties navigating these mechanisms and the power imbalance between Big Tech providers and consumers is evident.

10.50 The committee supports the introduction of mandatory digital platform internal dispute resolution standards.

Recommendation 4

10.51 The committee recommends the Australian Government implement mandatory dispute resolution requirements for large digital platforms via regulation.

10.52 Judicial escalation of disputes with digital platforms is generally not financially accessible for most consumers, nor expeditious enough to address problems before serious harm occurs. Small businesses and consumers are therefore

reliant on a regulator choosing to prosecute their case; however, regulators such as the ACCC focus their resources on systemic issues.

10.53 The committee is concerned that consumers are left with no realistic escalation options once business-to-business dispute resolution, perhaps with the assistance of an independent advocate or mediator, has been exhausted.

10.54 The committee considers the proposal for a judicial escalation option akin to a state-level small claims tribunal has merit.

Recommendation 5

10.55 The committee recommends the Australian Government establish a tribunal for small disputes with digital platforms.

Transparency

10.56 Chapters 5 and 6 highlighted concerns about transparency of data use by Big Tech, including by algorithms and in automatic decision-making.

10.57 Data collection by digital platforms occurs on a grand scale, often without explicit consent from users. Data brokers aggregate data to on-sell for commercial use, such as targeted advertising. Submissions raised concerns that consumer data can be used for profiling and discrimination, without consumers being aware that their data was collected.

10.58 The committee suggests measures be implemented to ensure customers are aware of what personal data is being collected by digital platforms and what it is used for. A greater effort should be made by digital platforms and the Australian Government to ensure personal data of individuals is adequately protected.

10.59 The committee proposes implementation of a public data reporting regime requiring Big Tech firms to:

- provide details of the targeting criteria for advertising and data determining which users are exposed to particular ads; and
- provide key metrics on demographic data collected for the purposes of targeting advertising, particularly children's data.

10.60 The committee notes that the EU Digital Services Act requires platforms that display advertising material on their online interfaces to ensure users can identify, for each advertisement displayed, that the information is an advertisement, who the advertisement is on behalf of and the parameters selecting recipients of the advertisement.[24] Some digital platforms have

[24] Guide to the Digital Services Act, *Article 24 – Online advertising transparency*, https://digitalservicesact.cc/dsa/art24.html (accessed 21 November 2023).

responded to this by creating an online repository of advertisers.[25] This model could be considered by the government.

10.61 Mandatory reporting of data collection by digital platforms should be modelled on the obligations imposed on superannuation funds to disclose certain information in notices for annual members' meetings.

10.62 Chapter 6 discussed concerns that algorithms used by digital platforms may not operate in a way that adequately supports community values, such as fairness, accuracy, privacy and user safety.

10.63 Evidence supported international approaches to strengthen the transparency of algorithmic use by digital platforms. In particular, the UK and the EU have implemented transparency standards for the use of algorithmic tools.

10.64 Large digital platforms should be subject to data access obligations and transparency measures which extend to algorithms used for content recommendation and for targeted marketing.

10.65 The committee supports the development of a risk-based regulatory framework by the proposed digital platforms coordination body. The framework should place the onus on digital platforms to identify risks created by their use of algorithms and outline how they will address those risks.

Recommendation 6

10.66 The committee recommends the Australian Government implement a requirement for designated digital platforms to report advertising material via a public register, based on turnover, and that it implement mandatory reporting on algorithm transparency, data collection and profiling by very large platforms, particularly identifying what personal data is collected and how it is used.

10.67 The committee notes the Privacy Act Review proposal to create a right of data erasure.

10.68 Submissions highlighted that individuals have limited rights when it comes to how their data is used. A right to erase personal data would give individuals more control over their own information when engaging with digital platforms.

10.69 The committee notes any right of erasure must extend beyond an individual's ability to delete data, such as photos or posts, which they have voluntarily shared online to also encompass biographical, geolocation, browsing habits, 'likes' and other data surreptitiously collected and collated by digital platforms.

---

[25] For example, *Google Ads Transparency Centre*, https://adstransparency.google.com/?region=AU (accessed 21 November 2023).

Recommendation 7

10.70 The committee recommends that the Australian Government regulate an individual's right to delete personal data.

Children's data

10.71 As highlighted in Chapter 8, children's online data collection raises particular security and personal risks. Evidence suggested that the changes in digital platforms' practices required to protect children online will only occur when mandatory codes with penalties for non-compliance are introduced and enforced.

10.72 The committee considers that additional regulation of children's data protection and privacy rights is necessary. The committee recommends implementing a mandatory code for the protection of children online, addressing regulatory fragmentation and aligning the rights of Australian children with international jurisdictions.

Recommendation 8

10.73 The committee recommends the Australian Government legislate for mandatory industry codes on the collection, use and retention of children's data.

Senator Andrew Bragg
Chair
Liberal Senator for New South Wales

Government Senators' additional comments

Introduction

1.1 Government senators provide these additional comments recognising the sufficient exploration of the policy issues and evidence in the majority committee report.

1.2 We extend our thanks to all submitters and witnesses to this inquiry. This has been a broad inquiry, and the expertise and views provided to the inquiry are appreciated.

1.3 It is evident that digital platforms need to better address their market power, influence, and conduct. Regrettably, many digital platforms are resistant to meeting the expectations of the public and policy makers. It is important that digital platforms consider consumer and market impacts of their operations and remedy clear issues when they are presented with them.

1.4 Government senators are of the view that a whole of government response to the regulation of digital platforms is the most efficient way to address digital platforms power, influence and wide impact on the economy and consumers.

1.5 Importantly, this whole of government response is already underway. Significant reforms are being progressed by the government through the Australian Competition and Consumer Commission's (ACCC) Digital Platform inquiries and the Attorney-Generals' Review of the *Privacy Act 1988* (Privacy Act). Other initiatives from across government portfolios complement these reforms.

1.6 Regulation of digital platforms is a policy matter being addressed globally, and it is important reforms pursued domestically—where appropriate — align with developments internationally. Government senators are of the view that lessons from overseas should be considered and applied to reforms in Australia as part of the whole of government approach.

1.7 Government senators look forward to further reforms being progressed that regulate the conduct of digital platforms, particularly with the protection of consumers in mind.

1.8 Since coming to government, reforms have been progressed that go to the heart of the challenge of regulating digital platforms—protecting consumers, modernising existing laws and regulations, and acting collaboratively with industry to address issues. Some of these significant reforms include:

- Consultation on the ACCC's Digital Platforms Services regulatory reform recommendations.[1]
- Modernising the Privacy Act including consultation on the outcomes of the Attorney-General's Department's Review of the Privacy Act.[2]
- Consultation on an exposure draft bill to provide the Australian Communications and Media Authority (ACMA) with new powers to hold the digital platforms to account and improve efforts to combat harmful misinformation and disinformation.[3]
- Increasing funding for the eSafety Commissioner and the Office of the Australian Information Commissioner to support their work regulating digital platforms activities.[4]
- A ban on unfair contract terms which came into effect on 3 November 2023, a recommendation of the ACCC.[5]
- Consultation on options to address unfair trading practices, a recommendation of the ACCC.[6]
- Consultation on the 'Supporting responsible AI' discussion paper and commitments from the Hon Ed Husic MP, Minister for Industry and Science to 'work with the international community to ensure AI is developed with the right guardrails in place'.[7]
- Consultation and subsequently the announcement of the Strategic Plan for Australia's Payments System.[8]
- A Prominence Framework to support access by consumers to free-to-air television services on connected television devices.[9]

---

1 The Treasury, *Digital Platforms— Consultation on Regulatory Reform*, 20 December 2022, https://treasury.gov.au/consultation/c2022-341745 (accessed 24 November 2022).

2 Australian Government, 'Government Response: Privacy Act Review Report', 28 September 2023.

3 The Hon Michelle Rowland MP, Minister for Communications, 'New ACMA powers to combat harmful online misinformation and disinformation', *Media Release*, 20 January 2023.

4 Office of the Australian Information Commissioner, 'OAIC welcomes additional Budget funding', *Media Release*, 9 May 2023.

5 The Hon Julie Collins MP, Minister for Small Business, The Hon Andrew Leigh MP, Assistant Minister for Competition, Charities and Treasury, 'Unfair contract terms banned from today', 9 November 2023.

6 The Treasury, *Unfair trading practices - Consultation Regulation Impact Statement*, 31 August 2023, https://treasury.gov.au/consultation/c2023-430458 (accessed 24 November 2022).

7 Department of Industry, Science and Resources, 'Supporting responsible AI: discussion paper', 1 June 2023; The Hon Ed Husic MP, Minister for Industry and Science, 'Australia signs the Bletchley Declaration at AI Safety Summit', *Media Release*, 3 November 2023.

8 The Treasury, *A Strategic Plan for Australia's Payments System*, 7 June 2023.

9 The Hon Michelle Rowland MP, Minister for Communications, 'First steps underway toward a new local TV prominence framework', *Media Release*, 10 August 2022.

- Consultation on strengthening the Basic Online Safety Expectations (BOSE) Determination established under the *Online Safety Act 2021*, including the best interest of the child being a primary consideration for all services used by children.[10]
- Industrial relations reform in the Fair Work Legislation Amendment (Closing Loopholes) Bill 2023 which addresses 'gig economy' workers who work through digital platforms.[11]
- An industry code of practice for dating platforms as an outcome of the National Roundtable on Online Dating Safety.[12]
- Reform to the National Classification Scheme to reflect the modern media environment as well as updated Guidelines for the Classification of Computer Games.[13]
- Involving technology companies in the Australian Government Digital Identity System (AGDIS) consultation.

1.9 While there are existing competition, consumer, corporation, taxation, privacy, online safety laws as well as recent reforms made by the government that provide further consumer and market protections, work on the whole of government approach to reforms should continue in order to keep pace with technological developments.

Response to majority committee report recommendations

1.10 This Senate Economics Reference Committee Inquiry has significant parallels to the findings and recommendations of the ACCC's inquiries, which are being consulted on and developed by the government, and the Review of the Privacy Act which is also being implemented by the government.

1.11 Government senators are of the view the government should continue to prioritise the findings and recommendations of the ACCC and the Privacy Act Review, a sentiment shared by many witnesses to the inquiry.

1.12 Government senators are of the view that the government should also continue to understand and learn from regulation pursued in other jurisdictions, and integrate this with domestic regulation where appropriate.

---

10 The Hon Michelle Rowland MP, Minister for Communications, 'Albanese Government takes major steps forward to improve online safety', *Media Release*, 22 November 2023.

11 The Hon Tony Burke MP, Minister for Employment and Workplace Relations, 'World-leading legislation to protect gig workers', *Media Release*, 31 August 2023.

12 The Hon Michelle Rowland MP, Minister for Communications, 'Update on the National Roundtable on Online Dating Safety', *Media Release*, 26 March 2022; Michelle Rowland, Minister for Communications, 'Government demands dating sites do better by Australians', *Media Release*, 18 September 2022.

13 The Hon Michelle Rowland MP, Minister for Communications, 'Changes to modernise Australia's Classification Scheme on their way', *Media Release*, 5 September 2023.

1.13 Government senators provide the following commentary on the recommendations included in the majority committee report.

Policy coordination is already happening

Commentary on Recommendation 1

The committee recommends that the Australian Government establish a digital platforms coordination body.

1.14 Evidence to the committee was clear that the four key regulators of the digital platforms—ACCC, eSafety Commissioner, ACMA, Office of the Australian Information Commissioner Information—meet regularly and share their knowledge, work, and priorities for the benefit of each regulator.

1.15 Together, their work as the Digital Platform Regulators' Forum (DP-REG) facilitates collaboration, knowledge sharing and a greater consideration of how existing and emerging competition, consumer, privacy, safety, and data issues interact and could be addressed.

1.16 This coordination is already happening, and it complements the whole of government approach the government is taking while recognising the requirements for the regulators to maintain their independence and pursue their respective responsibilities and priorities.

1.17 Government senators are of the view that it is unclear what a coordination body would add when there already exists cross-government coordination. It is also unclear how the regulators' independence could be managed from a legal perspective given they are established by statutes as independent agencies with different responsibilities.

1.18 Acknowledging this, there are always merits in further collaboration between the departments, agencies and regulators that oversee digital platforms which should be considered.

1.19 In considering options to increase alignment, the government should also explore opportunities to incorporate the learnings and experiences of international counterparts as well.

1.20 Similarly, if pursued, the government should appropriately facilitate the involvement of third parties in such a body to represent the views of consumers, workers, and industry in the coordination of digital platform regulation.

Competition and consumer policy reform is underway

Commentary on Recommendation 2 and Recommendation 3

The committee recommends that the Australian Government introduce legislation to prevent anti-competitive practices through the bundling of payment services and products by large digital platforms.

The committee recommends that the Australian Government require mandatory disclosure by large digital platforms of self-preferencing conduct.

1.21 The ACCC's Digital Platforms Inquiry between 2017 and 2019 and the Digital Platform Services inquiry from 2020 until 2025 is the most significant Australian inquiry into online platforms to date. This industry analysis, consultation, engagement with stakeholders and institutional understanding of how consumers and competition laws are enforced and applied to digital platforms are significant.

1.22 The ACCC's fifth interim report 'Digital platform services inquiry— September 2022 interim report— Regulatory reform' recommended regulatory options to address the harms that digital platforms can have to consumers, competition, and small business.

1.23 The ACCC is clear that they consider the bundling of products and services, self-preferencing, impediments to consumer switching and interoperability, and exclusive pre-installation and default arrangements, among other conduct by the digital platforms, as potentially anti-competitive.

1.24 Importantly, the ACCC have recommended that the government consider options to address these issues through a code framework that can be assessed clearly and objectively, and with industry and stakeholders to ensure it targets specific competition issues.

1.25 The Treasury has commenced consultation on the recommendations in the ACCC's fifth interim report to seek views and options for regulatory reform. The government is considering the ACCC's recommendations, undertaking consultation , and has a view to ensuring Australia maintains a competitive and well-regulated digital economy.

1.26 Government senators note that in progressing ACCC recommendations, it is important that instances of anti-competitive practices that cause consumer detriment and harm are prioritised.

1.27 These competition and consumer issues presented by the digital platforms are being addressed globally.

1.28 In the European Union, the Digital Markets Act (DMA) addresses market power and the Digital Services Act (DSA) addresses digital platforms' services.

1.29 Digital platforms operate globally and bring consumers together in a global marketplace. While there remains a sovereign responsibility to regulate in the national interest and in the interest of domestic consumers and markets, the challenge of addressing the powers and influence of digital platforms also remains a global challenge .

1.30 Government senators believe it is important that the government collaborate with and look to the world's initiatives to further regulate in accordance with international developments.

Dispute resolution is a critical next step

Commentary on Recommendation 4 and Recommendation 5

> ***The committee recommends the Australian Government implement mandatory dispute resolution requirements for large digital platforms via regulation.***
>
> ***The committee recommends the Australian Government establish a tribunal for small disputes with digital platforms.***

1.31 Recommendations 4 and 5 both address dispute resolution and have been considered together.

1.32 The ACCC recommended targeted measures to protect users, including through a mandatory process for dispute resolution to be established internally by the digital platforms. They recommended accessibility, timeliness, accountability, having the ability to escalate to a human, and transparency as critical features of such a scheme.

1.33 Government senators are strongly of the view that consumers must have access to internal dispute resolution services and that regulators are empowered to ensure dispute resolution services of the digital platforms are effective and meet consumer expectations.

1.34 Government senators look forward to the government progressing reforms on this important aspect of consumer protection, a recommendation of the ACCC and consulted on by Treasury.

1.35 Consideration of the best options for a potential external dispute resolution scheme should follow consideration of internal dispute resolution requirements and oversight processes to ensure that consumers have access to adequate internal dispute resolution as a priority.

Transparency is the right approach

Commentary on Recommendation 6

> ***The committee recommends the Australian Government implement a requirement for designated digital platforms to report advertising material via a public register, based on turnover, and that it implement mandatory reporting on algorithm transparency, data collection and profiling by very large platforms, particularly identifying what personal data is collected and how it is used.***

1.36 Transparency is an important regulatory tool that governments should utilise to impose obligations and operational changes to digital platforms. When digital platforms need to be open, accountable, and transparent their systems and services improve.

1.37 Some digital platforms do not recognise the need for regulations such as these, assert that self-regulation is an appropriate and sufficient approach, and avoid compliance with regulations, and fail to provide the level of transparency the community expects.

1.38 The merits of this recommendation and its usefulness should be considered in conjunction with other information gathering and reporting obligations that are already imposed on platforms.

1.39 Consideration should also be given to opportunities to extend or develop powers that already exist such as the compulsory information-gathering powers under section 155 of the *Competition and Consumer Act 2010*.

1.40 The Government is now considering refinements to the proposed Combatting Misinformation and Disinformation Bill based on the public consultation and submissions that were made, and a bill is expected to be introduced in 2024.

1.41 Government senators look forward to the implementation of this bill and believe it will improve transparency about what digital platforms are doing in relation to misinformation and disinformation, including the systems and processes that platforms have in place.

1.42 Importantly, these reforms from the government will build on and strengthen obligations in the voluntary disinformation code from the Digital Industry Group Inc. (DIGI) which launched in 2021.

1.43 Driving transparency is an important part of Australia's online safety approach. The Basic Online Safety Expectations (BOSE) Determination, established under the *Online Safety Act 2021*, sets out the Government's minimum safety expectations of online service providers for protecting Australian users. In November 2023, the Minister for Communications announced consultation to strengthen the BOSE Determination, to ensure these protections are fit-for-purpose in a rapidly evolving online environment.[14]

The government is making significant reforms to privacy and data use

Commentary on Recommendation 7 and Recommendation 8

The committee recommends that the Australian Government regulate an individual's right to delete personal data.

The committee recommends the Australian Government legislate for mandatory industry codes on the collection, use and retention of children's data.

[14] The Hon Michelle Rowland MP, Minister for Communications, *Online Safety (Basic Online Safety Expectations) Amendment Determination 2023*, www.infrastructure.gov.au/have-your-say/online-safety-basic-online-safety-expectations-amendment-determination-2023 (accessed 22 November 2023).

1.44 The review by the Attorney-General's Department of the *Privacy Act 1988* was instigated by the ACCC's 2019 Digital Platforms Inquiry final report and commenced by the previous government in 2020.

1.45 This work was not completed by the previous government and has since been progressed by the Labor Government. On 28 September 2023, the government agreed or agreed in-principle to the majority of the review's recommendations.

1.46 The government is now progressing the implementation of these reforms, conducting impact analysis, working with stakeholders and considering transition periods for legislative reform.[15]

1.47 Notably, in pursing privacy reforms ahead of the review being finalised, the government secured passage of legislation in the parliament to significantly increase penalties for repeated or serious privacy breaches. The Attorney-General stated that 'Companies which fail to take adequate care of customer data will face much higher penalties'. This is an essential factor of the legislative framework that is being progressed to ensure that companies and platforms have an obligation to protect their users' data.

1.48 Government senators note the government has agreed in-principle as part of the Privacy Act Review that individuals should have greater transparency and control over their personal information, particularly a right to:

- Request an explanation of what personal information is held and what is being done with it through an enhanced right to access.
- Challenge the information handling practices of an entity and require the entity to justify how its information-handling practices comply with the Privacy Act.
- Require an entity to delete (or de-identify) personal information through a right to erasure.
- Request correction of online publications over which an entity has control.
- Require search engines to de-index certain online search results.[16]

1.49 Government senators also note the government has agreed to develop a Children's Online Privacy code that would apply to online services that are likely to be accessed by children, as well as a proposal to prohibit the targeting of children under eighteen by digital platforms unless it was in their benefit such as preventing children from seeing age-sensitive advertisements.[17]

---

15 The Hon Mark Dreyfus KC, MP, Attorney-General, 'Albanese government to strengthen privacy protections', *Media Release*, 28 September 2023.

16 Australian Government, 'Government Response: Privacy Act Review Report', 28 September 2023.

17 Australian Government, 'Government Response: Privacy Act Review Report', 28 September 2023.

1.50 In developing the code, the Australian Government should address concerns around the collection, use and retention of children's data and the rights of users and consumers to have greater control over their data.

Senator Jess Walsh
Deputy Chair
Senator for Victoria

Senator Jana Stewart
Member
Senator for Victoria

Appendix 1
Submissions and additional information

1 Ben Blackburn Racing
2 eSafety Commissioner
3 SBS
4 Australian Broadcasting Corporation
5 Cancer Council Australia
6 NSW Small Business Commissioner
7 Digital Transformation Agency
8 Australian Competition and Consumer Commission
- Attachment 1

9 Department of Infrastructure, Transport, Regional Development, Communications and the Arts
10 Alcohol and Drug Foundation
11 Alcohol Change Australia
12 Law Institute of Victoria
13 Association of Heads of Independent Schools of Australia
14 UNICEF Australia
15 Screen Producers Australia
16 Australian Information Industry Association
17 Free TV Australia
18 Blockchain & Digital Assets Pty Ltd
19 Obesity Policy Coalition
20 Australian Communications Consumer Action Network (ACCAN)
21 Australian Research Alliance for Children and Youth
22 Tech Policy Design Centre
23 Centre for AI and Digital Ethics
24 Australian Communications and Media Authority
25 Gesellschaft für Freiheitsrechte e.V.
26 auDA
27 Mr Joshua Zubak
28 Australian Institute of Company Directors
29 Reddit
30 Gradient Institute
31 Reset.Tech Australia
32 BSA | The Software Alliance
33 Foundation for Alcohol Research and Education
34 Digital Platform Regulators Forum
35 Developers Alliance
36 Irish Council for Civil Liberties

37 Mr Mark Nottingham
38 Vault Cloud
39 Australian Small Business and Family Enterprise Ombudsman
40 Dr Janine Arantes
41 Alannah & Madeline Foundation
42 Professor Toby Walsh
43 Commercial Radio & Audio
44 Australian Muslim Advocacy Network
45 Blockchain Australia
46 Amazon Web Services
47 Microsoft
48 Amazon Australia
49 Google
50 Human Rights Law Centre
51 Attorney-General's Portfolio
52 Uniting Church of Australia (Synod of Victoria and Tasmania)
53 Children and Media Australia
54 CHOICE
55 Australian Media Literacy Alliance
- Attachment 1
- Attachment 2
- Attachment 3

56 Australian Publishers Association
57 Australian Library and Information Association and National and State Libraries Australasia
58 Communications Alliance
59 Council of Small Business of Australia
60 Consumer Policy Research Centre
61 Office of the Australian Information Commissioner
62 Joint submission from DRW, EFA, TPDC, CNI, PA and CRT
63 Tech Council of Australia
64 DoorDash
65 Digital Industry Group Inc. (DIGI)
66 Australian Medical Association
67 Airwallex
68 Digital Rights Watch
69 Meta
70 Apple
71 Commonwealth Bank
72 OVHcloud
73 Match Group
74 Reset Australia
75 Mr Cian Byrne

76 Optus
77 Epic Games

Answer to Question on Notice

1 UNICEF-001: answers to written questions on notice asked by Chair Senator Andrew Bragg - UNICEF AI Policy Guidance & Children Privacy Code (received 09 August 2023).

2 ACCC-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg & Senator David Shoebridge during a public hearing on 22 August 2023 - ACCC Enforcement Staff Numbers and live investigations in relation to dark patterns (received 06 September 2023).

3 ACMA-001: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Enforcement of Online Gambling (received 05 September 2023).

4 ACMA-002: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Enforcement action in relation to online gambling (received 05 September 2023).

5 ACMA-003: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Enforcement and disruption options (received 05 September 2023).

6 ASBFEO-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 26 July 2023 - Digital Platforms Issue Response (received 18 August 2023).

7 DHA-001: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Scope and inclusions in the ChatGPT questionnaire (received 05 September 2023).

8 DHA-002: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Summary of ChatGPT information entered by Home Affairs Employees (received 05 September 2023).

9 DHA-003: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 22 August 2023 - Enforcement mechanisms in relation to critical infrastructure assets (received 05 September 2023).

10 eSafety-001: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - TikTok on Government Devices (received 05 September 2023).

11 Microsoft-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg, Senator David Shoebridge, and Senator Jana Stewart during a public hearing on 22 August 2023 - Multiple Responses (received 05 September 2023).

12 DTA-002: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Notifiable attack contact clauses (received 05 September 2023).

13 Joint ACCC, ACMA, OAIC, eSafety-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 22 August 2023 - Joint Response (received 08 September 2023).

14 Meta-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg & Senator David Shoebridge during a public hearing on 22 August 2023 - Scams and Whistleblower allegations (received 12 September 2023).

15 OAIC-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 22 August 2023 - Enforcement Capacity and Enforcement Actions (received 08 September 2023).

16 DHA-004: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Cyber Breaches (received 26 September 2023).

17 DHA-005: answers to spoken questions on notice asked by Senator David Shoebridge during a public hearing on 22 August 2023 - Current accredited data centre and cloud providers (received 26 September 2023).

18 Amazon-001: answers to spoken questions on notice asked by Chair Senator Bragg, Senator Shoebridge, and Senator Stewart during a public hearing on 22 August 2023 - Multiple Subjects (received 25 September 2023).

19 AWS-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 3 October 2023 - Australian Financial Revenue from Public Cloud (received 10 October 2023).

20 ISGA-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 3 October 2023 - Regulatory Architecture in the EU (received 6 October 2023).

21 Airwallex-001: answers to spoken questions on notice asked by Chair Senator Andrew Bragg during a public hearing on 3 October 2023 - Competition Dynamics (received 18 October 2023).

Appendix 2
Public hearings and witnesses

Wednesday, 26 July 2023
Sydney Masonic Centre
66 Goulburn St, Sydney

Match Group

- Mr Mark Buse, Senior Vice-President, Head of Global Government Relations and Policy

Australian Institute of Company Directors

- Ms Laura Bacon, Senior Policy Adviser
- Mr Simon Mitchell, Senior Policy Adviser

DoorDash

- Mrs Rebecca Burrows, General Manager
- Ms Rachel Murphy, Director, Head of Policy and Government Relations

Alannah & Madeline Foundation

- Ms Sarah Davies, Chief Executive Officer
- Dr Jessie Mitchell, Advocacy Manager

Reset.Tech Australia

- Ms Alice Dawkins, Executive Director

Vault Cloud

- Mr Rupert Taylor-Price, Chief Executive Officer,

UNICEF Australia

- Mr John Livingstone, Advocacy Manager

Rob James Consulting

- Mr Rob James, Principal Consultant and Chief Executive Officer

Australian Small Business and Family Enterprise Ombudsman

- The Hon. Bruce Billson
- Dr Craig Latham, General Council

Tech Council of Australia

- Ms Katherine (Kate) Pounder, Chief Executive Officer

Centre for AI and Digital Ethics

- Dr Shaanan Cohney, Senior Lecturer, School of Computing Information Systems, Private capacity; and Researcher
- Professor Jeannie Marie Paterson, Professor of Consumer Law, Director
- Dr Sarita Rosenstock, Lecturer, School of Computing Information Systems, Private capacity; and Researcher

Australian Communications Consumer Action Network (ACCAN)

- Dr Gareth Downing, Deputy Chief Executive Officer

Tuesday, 22 August 2023

Committee Room 2S3
Parliament House, Canberra

Amazon Australia

- Mr Michael Cooley, Director, Public Policy Australia
- Mr David Howarth, Senior Manager Economic Policy Australia
- Ms Mariko Lawson, Manager, Public Policy Australia

Microsoft

- Ms Belinda Dennett, Corporate Affairs Director

Digital Transformation Agency

- Mr Chris Fechner, Chief Executive Officer
- Mr Peter Rymasz, Director, Hardware, Software and Digital Marketplaces

Meta

- Ms Mia Garlick, Regional Director of Policy

Australian Competition and Consumer Commission

- Mr Tom Leuner, Executive General Manager, Mergers, Exemptions and Digital
- Ms Kate Reader, General Manager, Digital Platforms Branch

eSafety Commissioner

- Ms Morag Bond, Executive Manager, Industry Regulation and Legal Services

Australian Communications and Media Authority

- Ms Creina Chapman, Deputy Chair

Office of the Australian Information Commissioner

- Ms Elizabeth Hampton, Deputy Commissioner

Department of Home Affairs

- Mr Peter Anstee, Acting First Assistant Secretary, Digital Security Policy
- Mr Hamish Hansford, Deputy Secretary, Cyber and Infrastructure Security

Tuesday, 3 October 2023

Committee Room 2S1
Parliament House, Canberra

Amazon Web Services

- Mr James Barton, Senior Corporate Counsel
- Mr Roger Somerville, Head, Australia and New Zealand Public Policy

Apple Inc.

- Mr Kyle Andeer, Vice President, Products and Regulatory Law

Google

- Ms Lucinda Longcroft, Director, Government Affairs and Public Policy, Australia and New Zealand

Free TV Australia

- Mr Ross Mitchell, Director, Broadcasting Policy

Nine Entertainment

- Mr Ben Campbell, Director, Digital Advertising and Data Products

ANU Tech Policy Design Centre

- Professor Johanna Weaver, Director

Airwallex

- Mr Luke Latham, General Manager, Australia and New Zealand
- Mr Nalin Natrajan, Financial Partnerships Manager
- Mr Sumukh Rudrapatna, Product Lead

International Social Games Association

- Mr Luc Delany, Chief Executive Officer