AUSTRALIAN COMPETITION & CONSUMER COMMISSION

# Digital Platform Services Inquiry

## Interim report

September 2020

accc.gov.au

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601



ACCC 09/20_20-22

ISBN 978 1 920702 53 3

www.accc.gov.au

# Contents

# Glossary

| Term | Description |
|---|---|
| **5G** | Fifth generation technology standard for wireless networks |
| **ACCC** | Australian Competition and Consumer Commission |
| **ACL** | Australian Consumer Law |
| **ACMA** | Australian Communications and Media Authority |
| **Ad tech** | Ad tech is a common abbreviation for 'advertising technology'. It refers to intermediary services involved in the automatic buying, selling and serving of some types of display advertisements |
| **Ad Tech Inquiry** | On 10 February 2020, the Australian Government directed the ACCC to conduct an inquiry into markets for the supply of digital advertising technology services and digital advertising agency services |
| **AI** | Artificial intelligence—the ability of computer software to perform tasks that are complex enough to simulate a level of capability or understanding usually associated with human intelligence |
| **Algorithm** | A sequence of instructions that performs a calculation or other problem-solving operation when applied to defined input data. In this report 'algorithm' generally refers to the algorithms used by platforms to rank and display content on their services |
| **Android Advertising ID** | A type of persistent identifier used for advertising purposes which uniquely identifies a mobile device, allowing an individual's behaviour to be tracked over time |
| **APIs** | Application programming interface—tools for building software that interacts with other software, for example, how apps interact with operating systems |
| **AR** | Augmented reality—technology that uses the existing environment and overlays new information on top of it, to experience existing reality in a heightened way |
| **Biometric data** | Data derived from biometric information, which includes any features of an individual's face, fingerprints, iris, palm, signature or voice |
| **Bundeskartellamt** | German Federal Cartel Office |
| **Clickwrap agreements** | Online agreements that use digital prompts and which typically allow users to 'accept' to the terms and policies by clicking 'I Agree' or a similar icon |
| **CMA** | Competition and Markets Authority, UK |
| **Crawling** | The process by which search engines systematically and continuously search the internet for new pages and add them to their index of known pages so they can be surfaced in search results |
| **Data practices** | The collection, use and disclosure of user data |

| Term | Description |
|---|---|
| **Direction** | Ministerial direction from the Australian Government to the ACCC on 10 February 2020 to conduct an inquiry into markets for the supply of digital platform services |
| **DPI** | Digital Platforms Inquiry—conducted by the ACCC into digital search engines, social media platforms and other digital content aggregation platforms, and their effect on media and advertising services markets |
| **DPI Final Report** | The final report for the Digital Platforms Inquiry, published on 26 July 2019 |
| **Dynamic competition** | Competition resulting from the potential for development of innovative products and services that allow a competitor to enter and/or expand in a market |
| **EC** | European Commission |
| **Economies of scale** | Cost advantages obtained by a supplier, where average costs decrease with increasing scale |
| **EU** | European Union |
| **Ex ante regulation** | Market intervention that seeks to identify problems beforehand and shape behaviour |
| **FTC** | Federal Trade Commission, United States |
| **GDPR** | General Data Protection Regulation (EU) |
| **IoT** | Internet of Things—the use of internet-connected technology in physical devices that have not traditionally featured such technology, such as cars, household appliances and speakers. This allows these devices to collect, share and make use of data |
| **IP address** | Internet Protocol address—a numeric address assigned to each device connected to a local network or the internet via the Internet Protocol |
| **Knowledge Graph** | Google's database of facts about people, places and things, compiled from a variety of sources that provide factual information (including public sources and data licensed from providers) |
| **Multi-homing** | The practice of using more than one supplier of the same type of service |
| **Natural language processing/ natural language generation** | Technology that allows computer software to collect, analyse, interpret and produce ‘natural’ language in the form of text and speech |
| **Network effects** | The effect whereby the more users there are on a platform, the more valuable that platform tends to be for their users |
| **Non-proprietary online private messaging services** | Online private messaging services that can be downloaded and used across devices and operating systems, and services that have a primary focus on offering a service through which users can communicate with each other |
| **OAIC** | Office of the Australian Information Commissioner |
| **OECD** | Organisation for Economic Cooperation |

| Term | Description |
|---|---|
| **OneBox** | A separate display box within Google search results that allows Google to include results from its other search products (e.g. carousel from Google Shopping or nearby locations from Google Maps) within its standard Google search |
| **Online private messaging services** | Services that enable users to communicate privately with friends, family members, colleagues and other contacts, one-to-one and/or with a group in real-time and in various forms such as text, voice or video |
| **Organic search results** | The provision of a set of hyperlinks on a search engine results page, considered by the search engine's algorithm as responsive to a user's search query |
| **Personal information** | Defined within the Privacy Act as<br>'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:<br>• whether the information or opinion is true or not, and<br>• whether the information or opinion is recorded in a material form or not' |
| **Personalised pricing** | A form of price discrimination whereby different consumers may receive different prices, set using information about their characteristics and what a business thinks they are willing to pay |
| **Price discrimination** | Similar goods are sold by a firm at different prices (or at prices that are in different ratios to marginal cost) |
| **Privacy Act** | *Privacy Act 1988 (Cth)* |
| **Proprietary online private messaging services** | Online private messaging services that are only available on one mobile operating system |
| **RCS** | Rich Communication Services—a communication protocol between network operators and smartphones that aims to replace standard SMS services, to send and receive messages. RCS provides users with the ability to send and receive messages over a data network and provides an enhanced form of messaging, with multimedia support, typing indicators and group chat functionality, among other features |
| **SDK** | Software Development Kit—a third-party software component that is used to develop applications |
| **Search engines** | Software systems designed to search for information on the World Wide Web, generally returning a curated, ranked set of links to content websites |
| **SMS** | Short Messaging Service |
| **Social media platforms** | Online services that allow users to participate in social networking, communicate with other users, and share and consume content generated by other users (including professional publishers) |
| **Specialised search** | Search engines that specialise in different types of search. For example, Expedia provides vertical search services for travel |
| **Sponsored search results** | Advertisements shown on a search engine results page |

| Term | Description |
| --- | --- |
| **Standalone online private messaging services/standalone services** | Online private messaging services whose primary function is to provide a personal means of communication between people (such as Facebook Messenger, WhatsApp, iMessage) |
| **Sunk costs** | Costs that are incurred and cannot be recovered in any way |
| **Third party data** | Information from an entity that does not have a direct relationship with the person the data has been collected about. Common types of third party data that may be purchased by websites or advertisers include purchasing history, geographic data and sociodemographic data |
| **Third party script** | Web applications offered by developers and organisations that can be embedded into websites to provide certain functionality, such as for analytics or advertising purposes. |
| **Voice assistant** | A digital assistant that uses voice recognition, speech synthesis and natural language processing to provide a service through a particular application or device, and can perform tasks or services for an individual based on commands or questions. Examples include Google Assistant, Siri and Alexa |
| **VR** | Virtual reality—technology that offers a digital recreation of a real life setting and replicates a real or imagined environment |
| **Wake word** | A phrase that allows users to activate and engage with a voice assistant on a smart device, for example ‘Hey Google’ |

# Executive Summary

## Introduction

In 2020, when Australians have had to live more of our lives online than ever before, the importance of digital platforms has never been clearer. The central role platforms perform for businesses and for individuals means that the actions or inaction of platforms have a significant impact on our daily lives and the operation of many businesses.

In December 2019, the Government announced that the ACCC would have a role for five years to monitor digital platform services[1] and their impacts on competition and consumers. As part of this role, the ACCC is to provide the Australian government with six-monthly reports on digital platform services.

This is the first six-monthly report and it looks at competition and consumer issues associated with online private messaging services, updates previous findings reached by the ACCC as regards social media and online search services and also identifies some common concerns across different types of platforms.

Following reports will focus on other types of digital platform services as set out here.

## Online private messaging

### Facebook and Apple are two of the largest suppliers of standalone online private messaging services in Australia

Online private messaging services encompass a range of services, including text, audio and video messaging services[2], and are offered by a wide variety of platforms. Based on the information available to the ACCC, Facebook and Apple are two of the largest suppliers of standalone online private messaging services[3] (standalone services) in Australia.[4]

Facebook supplies two standalone services: Facebook Messenger and WhatsApp, which are available for use across Android and Apple devices.[5] In June 2020, Facebook Messenger had an estimated 14.7 million monthly active users. Facebook-owned WhatsApp had an estimated 8 million monthly active users.[6]

Apple supplies two standalone services: iMessage and FaceTime, which are available to users of Apple devices. FaceTime is a video and voice calling app and iMessage is a feature of Apple's preinstalled messaging app (Messages) that is enabled by default in the app. While Apple's Messages can be used to send SMSs to all types of devices that have the ability to receive SMSs, the iMessage service provides online private messaging with additional features, including the ability to send and receive photos, group chats and read receipts. The ACCC understands that Apple's iMessage has an estimated range of 6 million

---

1 Digital platform services covered by this direction include internet search engine services (including general search services and specialised search services), social media services, online private messaging services (including text messaging; audio messaging and visual messaging), digital content aggregation platform services, media referral services and electronic marketplace services.

2 'Online private messaging services' are defined in section 4 of the Direction to the Digital Platform Services Inquiry. As they are 'online' services, they exclude services which do not rely on data networks, such as SMS.

3 A standalone service is a service where the primary function of the service is to provide users with the ability to communicate with others. Some standalone online private messaging services focus on one particular form of communication, such as video calling, while others may provide a number of ways to communicate. Certain standalone online private messaging services are only available on one operating system (for example, Apple's iMessage), while others can be downloaded and used across different operating systems and devices (such as Facebook Messenger and Zoom).

4 Based on estimates from Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Unique Audience. Chapter 2 discusses estimates of active users of iMessage.

5 Instagram, which is owned by Facebook, also provides a private messaging function to their users. However, for this report the ACCC has not considered it as a standalone service since private messaging is part of Instagram's broader social media offering.

6 Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Unique Audience.

to 12 million daily active users in Australia.[7] The ACCC also understands that usage of FaceTime is significant, with a recent ACMA consumer survey finding that 33 per cent of online Australian adults had used FaceTime in the six months prior to June 2020.[8]

## Facebook has a significant competitive advantage over suppliers of other standalone services

Standalone services are not generally interoperable; messages or calls from one service cannot be sent to, or received by, another service. This gives rise to identity-based network effects. The more a user's friends, family, colleagues and acquaintances use the service, the more attractive that service is to the user.

The significant size of each of the user bases of Facebook Messenger and WhatsApp, and the presence of these network effects, gives Facebook a significant competitive advantage over smaller suppliers of standalone services in Australia. In order to attract individual users away from Facebook, rival standalone services need to attract some or many of the user's friends, family, colleagues and acquaintances to their service.

While Apple's standalone services are used by a significant number of Australians, their use is limited to users of Apple devices. For users wanting to communicate with users of other devices, Apple's services are not an effective alternative to Facebook Messenger and WhatsApp. This limits the competitive constraint that Apple's services impose on Facebook Messenger and WhatsApp.

Other types of standalone services, such as those focused on video-calling (for example Zoom) or business customers (rather than consumers), also do not appear to be viable alternatives for many users of Facebook's standalone services due to the differentiated nature of the offerings and/or their smaller user bases.

Accordingly, the ACCC considers that Facebook has a degree of freedom from competitive constraints in the supply of standalone services.

## The competitive constraints that Facebook Messenger and WhatsApp impose on iMessage are most likely to be stronger than the constraint iMessage imposes on Facebook Messenger

The ACCC has also considered the competitive constraints on iMessage given estimates indicating its widespread use in Australia and the default position it holds on Apple devices.

The significant size of iMessage's user base and the presence of identity-based network effects provides it with a significant competitive advantage over smaller standalone services. This advantage is likely to be enhanced by the default position that iMessage holds on Apple devices.

As iMessage is only available on Apple devices, it would be costly for non-Apple users to switch from Facebook Messenger or WhatsApp to iMessage as doing so involves acquiring an Apple device. However, it is relatively inexpensive for Apple users to switch away from iMessage to Facebook Messenger or WhatsApp. As a result, the competitive constraints imposed on iMessage by Facebook Messenger and WhatsApp are most likely stronger than the constraint iMessage imposes on Facebook Messenger and WhatsApp.

## COVID-19 and isolation requirements have contributed to the growth of online private messaging and other services, including Zoom

Use of online private messaging services and, in particular, video conferencing platforms such as Zoom, have grown significantly during the COVID-19 pandemic as workplaces and

---

7 Information provided to the ACCC.

8 ACMA, Trends in online behaviour and technology usage – ACMA consumer survey 2020, September 2020, p. 9.

schools moved to remote access and people turned to alternatives to face-to-face communication.

TikTok, a music video sharing platform, typically considered a type of social media platform[9], has also seen rapid growth. This may be attributed to both its popularity amongst younger users and also the impact of COVID-19, as users turn to online activity as a means to spend leisure time and stay connected.

The ACCC will monitor the growth of online private messaging services and social media platforms, including growth as a result of COVID-19, during the Inquiry.

## Social media and search

### Google remains dominant in search and Facebook remains dominant in social media

Google Search has over 95 per cent of the supply of search services in Australia.[10] Facebook's social media services, Facebook and Instagram, are the most used social media platforms, with the majority of time spent by users on its platforms and no social media services appearing to provide a meaningful constraint.[11]

### Increasing numbers of consumers are choosing platforms that differentiate on the basis of privacy protections

DuckDuckGo's global daily average search traffic increased by around 61 per cent between June 2019 and June 2020, growing from 39.1 million searches to 62.9 million searches.[12] Research conducted by DuckDuckGo indicates that people are taking 'meaningful action to improve their privacy protections'.[13] This action may in part explain its substantial growth, although DuckDuckGo's share of general search in Australia remains small.[14]

### Facebook's and Google's significant share of online advertising expenditure is increasing

Based on information provided to the ACCC, for a typical AU$100 spent by advertisers on online advertising in 2019, $53 went to Google, $28 to Facebook[15] and $19 to all other websites and ad tech. This is an increase to both Google and Facebook from $49 and $24 respectively in 2018.[16]

Advertising expenditure has been impacted by the COVID-19 pandemic, but it remains to be seen how this and other events will affect the longer term advertising revenue of online advertising services in Australia, including the services offered by the major platforms.

---

9 Social media platforms are online services that allow users to participate in social networking, communicate with other users, and share and consume content generated by other users (including professional publishers). Many social media platforms, including TikTok, also have private messaging functionality.

10 Statcounter, Search engine market share, accessed 22 September 2020.

11 Nielsen Digital Panel, June 2020, All demographics, PC, Smartphone and Tablet, Total time spent. Appendix B discusses the proportion of time spent by Australians on selected social media platforms.

12 DuckDuckGo, DuckDuckGo Traffic, accessed 22 September 2020.

13 DuckDuckGo, New DuckDuckGo research shows people taking action on privacy, 3 October 2019, accessed 22 September 2020.

14 Statcounter, Search engine market share, accessed 22 September 2020.

15 The ACCC notes that advertising revenue figures for Facebook relate to the amount of advertising revenue from customers in Australia based on the location of the invoiced party (which may differ from the country in which the advertisements are shown). The ACCC understands that these figures are not recorded in the ordinary course of business by Facebook and are not audited, verified or otherwise reported on. As such, the ACCC considers that these are approximate estimates of relevant advertising revenue attributable to Australia for Facebook.

16 ACCC estimates, based on information provided to the ACCC. Figures are not comparable to information provided in the Final Report of the Digital Platforms Inquiry due to changes in calculation methodology. As with all estimates, there is a potential that this may under or overstate the actual market share of each firm or the total size of the market.

## Potential consumer concerns

### Consumers, as well as small businesses, are impacted by a greater number of sponsored search results on mobile devices

Google provides organic results in response to search queries and, depending on the search, sometimes provides sponsored results. Over time, Google has introduced OneBoxes and the Knowledge Graph, among other features, to search result pages.

The ACCC examined the extent to which the use of different devices may impact the display of Google search results to consumers by comparing the results on handheld mobile devices with desktop devices (including laptops). It found that, for a retail product search, there was a higher proportion of sponsored results as the first result on mobile devices compared to desktop devices, and that organic search results were often less visible to consumers searching on a mobile device.

Given that a significant proportion of Google searches in Australia are conducted on mobile devices[17] and that consumers often focus their attention on the highest ranking search results[18], a higher proportion of sponsored results on these devices can reduce the ability of consumers to obtain information through search that best suits their needs. It also increases the need for businesses to use Google's search advertising tools to reach consumers (rather than relying on clicks to organic links).

### Australians' online activity is being extensively tracked, with large platforms including Facebook and Google key recipients of this data

The ACCC's commissioned and internal analysis indicates that, in addition to information collected while users are on their platform, a number of businesses, including large platforms that provide online private messaging, social media and search, can obtain user data through their role providing advertising and other services to websites and mobile applications.

The ACCC's website analysis found Google and Facebook had the largest presence in online tracking, with Google and Facebook's third party scripts[19] present on over 80 per cent and 40 per cent respectively of 1000 popular websites in Australia. Amazon and Microsoft tracking were present on nearly 30 per cent and almost 20 per cent of websites respectively.

Commissioned research by AppCensus on the top 1000 popular Android mobile applications (apps) in Australia[20] observed that platforms such as Google and Facebook and advertising services providers have the potential to receive a range of user information from apps because of the prevalence of their software development kits (SDKs) within apps.[21] AppCensus observed that Google's SDKs were identified in 92 per cent of all apps analysed and Facebook's SDKs in 61 per cent of apps.[22] Almost two thirds of apps analysed were

---

17 See chapter 4.

18 Competition and Markets Authority, Online Search: Consumer and Firm Behaviour, 7 April 2017, p. 86.

19 ACCC analysis. Third party scripts are offered by developers and organisations, and can be embedded into websites to provide certain functionality, such as for analytics or advertising purposes. The ACCC's analysis indicated that the vast majority of Google and Facebook's scripts were tracking scripts.

20 Based on ranking and active users, the top 1000 most popular Android apps analysed consisted of top apps on the Google Play Store across all categories and at least 100 top apps in both the Fitness and Health categories ('Health apps') and in the Education, Games and Animation and Comics categories that are targeted to children aged 13 and under ('Kids apps').

21 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii. SDKs are third party software components that are bundled with an app to provide a particular functionality such as providing the primary features of the app and/or collecting and sending data for the purposes of advertising and analytics. AppCensus noted that the prevalence of popular SDKs provides a metric for potential data collection from apps.

22 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. iii–iv. AppCensus also found that Google's SDKs for advertising or analytics purposes were identified in 91 per cent of apps analysed, and Facebook's advertising and analytics SDKs in 62 per cent of apps analysed. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 24.

observed by AppCensus to have the ability to transmit user information to Facebook, regardless of whether those users have Facebook accounts.[23]

In addition to the presence of SDKs in apps, AppCensus observed that a range of platforms and advertising services providers were being sent data from apps during testing.[24] The research showed that Facebook received data from approximately 40 per cent of all apps analysed.[25] Other platforms such as Google, Twitter and Amazon were observed to be receiving user data from around 10 per cent, 8 per cent and 4 per cent of the apps respectively.[26]

The types of user data observed being collected and transmitted by apps varied, ranging from user advertising identifiers[27] and location information[28], to accessing sensitive user information, such as audio recordings, access to a user's camera as well as health data.[29] In some cases, AppCensus observed apps transmitting a resettable advertising identifier alongside other identifiers[30], which would allow apps to continue tracking the same user, even if that user chose to reset the advertising identifier.[31]

In relation to online private messaging services, the ACCC's review of terms and conditions found that, even if the content of messages between users is private, a number of platforms confirm they may collect a range of other data from users, including their location, account and device information and other online activities.

### New products and services, including voice assistants, and augmented and virtual reality services, allow for an increased ability to collect data on consumers

Voice assistants and new technologies facilitate the growing collection of data by platforms—every month more than 500 million people globally are using Google Assistant across smart phones, TVs, cars, smart displays and other devices.[32] Platforms operated by Google, Amazon and others have the ability to collect voice recordings or transcripts of interactions with voice assistants.[33] The extent of tracking and data collection is likely to continue as large platforms acquire and expand into new technologies, including connected

---

23 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 27.

24 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. vi–viii. The testing period was from June-July 2020 and conducted on devices within Australia.

25 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. vi.

26 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. vi, 33. These figures may understate the extent to which data is accessed and received by apps. Further information is provided at section 4.1 and section 5 of the report. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. 13, 65–68.

27 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. ii, 9. An identifier is a unique number that uniquely identifies a mobile device and can be used to track users over time and across services.

28 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 16.

29 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. 38–43. In particular, see figure 15 and 16 which show the percentage of apps analysed which requested access to sensitive user information (labelled by Android as 'dangerous' permissions) and used these permissions during the testing period. Android describes 'dangerous' permissions as covering 'areas where the apps wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of others apps. For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant permission to the app'. See Android, Permissions overview, accessed 22 September 2020. This is further discussed in chapter 4.

30 The Android Advertising ID is a resettable advertising identifier, meaning that users are able to go through the system settings to reset it to a new value. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 9. AppCensus indicated that 32 per cent of apps observed transmitted other identifiers alongside the Android Advertising ID. AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. v.

31 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. v.

32 M Bronstein, A more helpful Google Assistant for your every day, *The Keyword (Google Blog)*, 7 January 2020, accessed 22 September 2020.

33 This can be set as the default or through consumers opting in, however, some services provide an option to delete these recordings. See for example, Google, Data security and privacy on devices that work with Assistant, Google Nest Help, accessed 22 September 2020. Amazon, Alexa and Alexa Device FAQs, accessed 22 September 2020. Amazon, Alexa Privacy Settings, accessed 22 September 2020.

devices with voice activated and voice recognition services, and augmented and virtual reality.

### Most Australians have limited understanding of the data practices they consent to and the majority view third party use as a misuse

Most consumers are unclear on what they are consenting to and express concern over tracking online. Recent research indicates that less than 10 per cent of consumers have a very good understanding of how their personal information is used once they give consent[34] and more than 4 in 5 consider it to be a misuse for an organisation to ask for information that is not relevant to the purpose of the transaction or to monitor and record their online activities without their knowledge.[35]

The ACCC notes that similar findings in the Digital Platforms Inquiry Final Report led to the ACCC's recommendation for changes to privacy law and the Australian Consumer Law to ensure consumers can exercise choice and control that align with their privacy preferences. The ACCC continues to support these recommendations and notes the Government Response and Implementation Roadmap for the Digital Platforms Inquiry generally supported or in principle supported these recommendations.

### Platforms need to do more to address scams on their platforms

The extensive data collected by platforms can include data that identifies (or infers) an individual's vulnerabilities, which places vulnerable consumers at particular risk of being targeted by scammers. The ACCC has found scams on platforms are increasing. In the period January 2018 to June 2020, scam reports to Scamwatch involving search, social media and online private messaging platforms resulted in reported losses of $87 million. This is likely to significantly undervalue loss as many consumers do not report scams. A number of the reports relate to known celebrity scams or lotto frauds, some of which have been continuing in a similar form for many years.

The ACCC considers that all platforms should do more to remove scam activity on their services and provide redress to consumers, where appropriate. Scammers are clever, flexible and innovative, and platforms are in the best position to identify persistent and emerging scams and other threats and act to minimise these harms to their users.

The ACCC remains of the view that effective dispute resolution mechanisms to address complaints and disputes to digital platforms are needed, and the establishment of an independent ombudsman is important to address these harms. The ACCC notes that the Government supported these recommendations in principle in its Government Response and Implementation Roadmap for the Digital Platforms Inquiry.

## Platform terms disadvantage small businesses and are potentially unfair

Australian businesses, particularly small businesses, increasingly rely on a range of platforms to reach Australian consumers online. However, the ACCC has found that the platforms' terms and conditions relevant to small businesses, which must be accepted by default, often leave small businesses at a significant disadvantage.

A review of multiple platforms' standard terms for businesses that seek to advertise on them has found common terms which could be unfair for small businesses. While it may be reasonable in some circumstances for platforms to remove content or suspend/terminate accounts, the terms often provide extremely broad discretion to exercise such powers. Terms also commonly limit the ability of businesses to address issues when they arise due to prohibitive dispute resolution clauses (for example terms requiring claims to be made in

---

[34] Deloitte, Australian Privacy Index 2020, accessed 22 September 2020, p. 7.
[35] OAIC, Australian Community Attitudes to Privacy Survey, September 2020, pp. 36–37.

the US or via international arbitration), confidentiality or publicity limitations, as well as clauses allowing platforms to vary terms without notice.

The terms that small businesses are required to adhere to in order to use platforms' services reflect the power imbalances that exist. As noted above, the ACCC remains of the view that platforms need to improve dispute resolution options for small businesses, as well as consumers, and reiterates its recommendations from the Digital Platforms Inquiry Final Report.

Further, while the application of certain standard terms to businesses may vary, the ACCC is particularly concerned about the potential impact on small businesses where terms have to be accepted by default, are heavily balanced in favour of platforms and do not provide sufficient recourse in the event of difficulties or disputes.

The ACCC notes the Digital Platforms Inquiry Final Report recommendation of a prohibition of unfair contract terms (with penalties applying to their use) and a prohibition of certain unfair trading practices. The ACCC continues to support these recommendations.

## Large platforms are expanding their ecosystems

Platforms such as Google, Facebook, Microsoft, Apple and Amazon continue to acquire businesses and develop new products and services that enable them to expand in existing and new markets.

The ACCC acknowledges the value that expanded digital ecosystems can bring to consumers.

However, the ACCC has concerns that growing ecosystems have the potential to affect competition where they extend the dominance of a platform in one market into adjacent markets, where a platform's complementary products and services could insulate their core service from future competition, and where it provides platforms with additional opportunities to gather data. The ACCC notes that similar concerns have been expressed by the UK's Competition and Markets Authority.[36]

The ACCC will monitor platform ecosystems, and their impact on competition, through the Inquiry.

## International scrutiny of platforms is escalating

The competition and consumer impacts of large digital platforms are an increasing focus for competition and consumer agencies, and for governments more broadly across the world.

One common concern identified across jurisdictions is the need for closer scrutiny of acquisitions by large platforms, particularly the practice of acquiring smaller businesses in neighbouring markets. Adequate ex-ante scrutiny of mergers and acquisitions is important as it is the key tool available to competition agencies to avoid the adverse consequences of market power. Both governmental and non-governmental reports have recommended changes to merger law and policy. The merger notification protocol, recommended in the Digital Platforms Inquiry Final Report, and which is subject to negotiation between the ACCC and large digital platforms, aims to ensure that the ACCC is informed and has adequate information to enable it to appropriately assess such acquisitions.

Many of the concerns recognised in this report and in the Digital Platforms Inquiry Final Report are global in nature. International collaboration and coordination is critical to address the position and conduct of major platforms, given the worldwide nature of many of these businesses.

---

[36] Competition and Markets Authority, Online platforms and digital advertising market study, 1 July 2020, Appendix E, pp. E2–E3.

The ACCC's Digital Platforms Branch is working closely with the equivalent teams being set up at many overseas competition and consumer agencies. As part of this cooperation, the ACCC will continue to assist in enhancing cross-border enforcement and, where appropriate, share information and align approaches to meet the same objectives.

# 1. Overview of online private messaging, search and social media services

On 10 February 2020, the Australian Government directed the ACCC to conduct an inquiry into markets for the supply of digital platform services[37] and digital advertising services supplied by digital platform service providers, and the data practices of both digital platform service providers and data brokers (the Inquiry). The Australian Government further directed the ACCC to provide an interim report by 30 September 2020 and every six months thereafter, and a final report by 31 March 2025.

The sectors that are the focus of the Inquiry include online private messaging, social media, internet search, electronic marketplaces, digital content aggregation platforms, media referral services and the digital advertising services provided by digital platform services, as well as data broker services. The Inquiry will examine:

- the intensity of competition in markets for the supply of digital platform services, with particular regard to the concentration of power, the behaviour of suppliers, mergers and acquisitions, barriers to entry or expansion and changes in the range of services offered by suppliers of digital platform services
- practices of suppliers in digital platform services markets which may result in consumer harm
- market trends that may affect the nature and characteristics of digital platform services, and
- developments in markets for the supply of digital platform services outside Australia.

**This first interim report focuses on platforms that provide online private messaging services (including text messaging, audio messaging and visual messaging).**

**It also updates the ACCC's previous analysis in relation to search and social media platforms and identifies competition and consumer issues common across these platforms.**

The second interim report (due March 2021) will examine app store marketplaces. Further information about the report can be found on the ACCC's website.

This chapter is structured as follows:

- **Section 1.1** provides an overview of online private messaging services, and
- **Section 1.2** provides an update on the usage of search and social media platforms (including their advertising services) since the ACCC's Digital Platforms Inquiry Final Report (DPI Final Report).

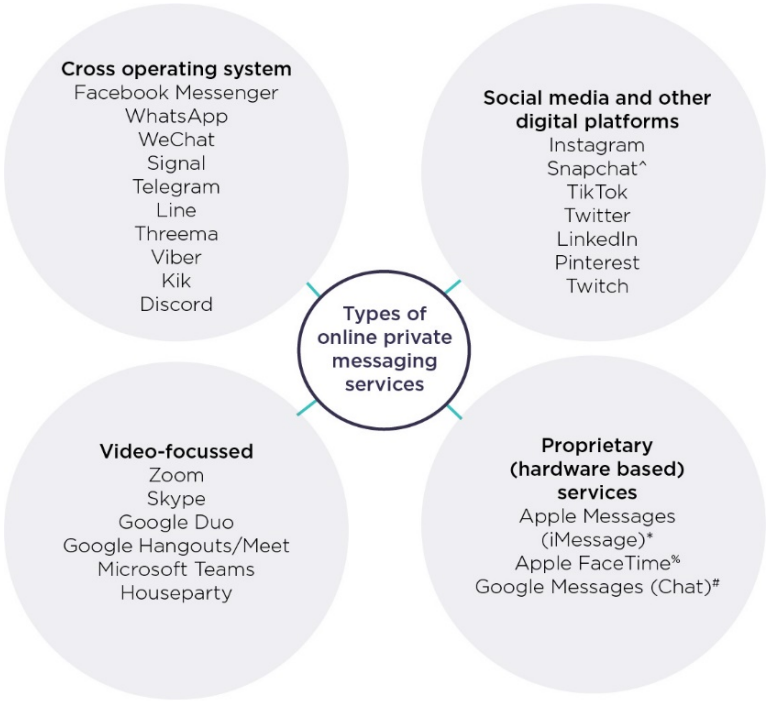
[37] Digital platform services covered by this direction include internet search engine services (including general search services and specialised search services), social media services, online private messaging services (including text messaging, audio messaging and visual messaging), digital content aggregation platform services, media referral services and electronic marketplace services.

## 1.1. Overview of online private messaging services

- **There is a wide range of online private messaging services available to Australian users, which Australians are increasingly using on an everyday basis. Online private messaging services are highly differentiated, offering different features and functionalities, and can be used by consumers for a number of different purposes.**
- **Use of online private messaging services, including Facebook Messenger and WhatsApp, has grown in recent times. For services such as Zoom, in particular, this is most likely as a consequence of COVID-19.**

Online private messaging services, which offer text, voice and video messaging, are an increasing facet of Australians' communications. While online private messaging services initially rose to prominence by offering a low-cost alternative to SMS, they have since evolved to offer more than just messaging, and some are 'multimedia hubs that support photos, videos, games, payments, and more'.[38] Figure 1.1 shows examples of widely used online private messaging services in Australia.

**Figure 1.1: Types and examples of online private messaging services offered in Australia**




Source: ACCC analysis.

^ The ACCC considers that Snapchat is an example of an online private messaging service and a social media platform, as its main function is the ability to send messages to other Snapchat users.

* The iMessage functionality on Apple's Messages provides the ability for users to send and receive messages using the Internet rather than mobile networks.

% Apple FaceTime is both a video-focused service and a service that is only available on the Apple iOS operating system.

\# The Chat feature on Google's Messages provides the ability for users to send and receive messages using the Internet rather than mobile networks.

[38] T Barot and E Oren, Guide to Chat Apps, 9 November 2015, accessed 22 September 2020.

Online private messaging services can be accessed by consumers on smartphones, tablets or computers[39], as well as wearable devices, such as smartwatches. Figure 1.1 shows that while online private messaging services provide the ability to communicate via text, voice and video, these platforms can differ in the features available to consumers. Some key differentiators are:

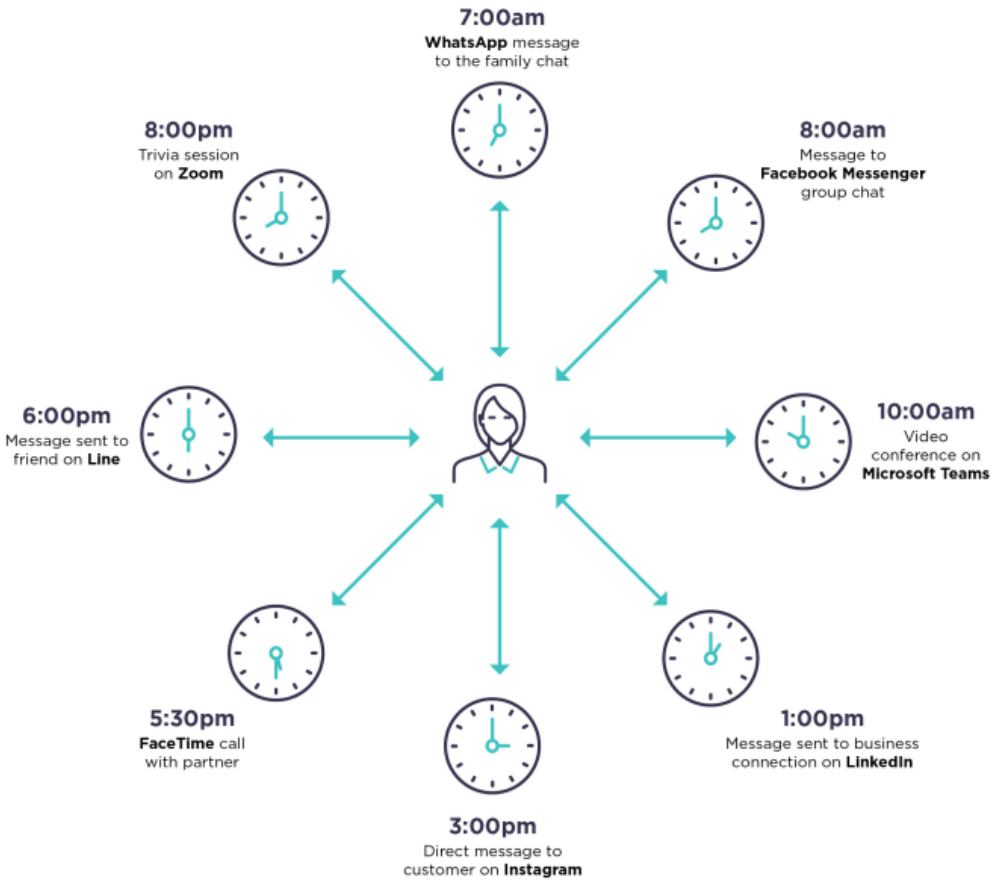
- **Allowing a user to message others on different operating systems (cross-operating system) or limiting a user to messaging certain users or devices (proprietary online private messaging)—**some online private messaging services, such as Facebook Messenger, WhatsApp and WeChat allow users to communicate with anyone who has downloaded the app, regardless of their operating system. However, other online private messaging services are only available to certain users. For example, the iMessage feature on Apple's Messages and the Chat feature on Google's Messages only allow communication between users of the same operating system (Apple's iOS or Google's Android).
- **Specialising in providing certain functionalities—**some online private messaging services focus on certain functionalities. For example, Zoom, which focuses on its video-calling functionality, has increased in popularity during the coronavirus pandemic (COVID-19). FaceTime only provides video and voice calling to Apple users.
- **Provision of the service as part of a broader offering—**some services have communication as their primary function (such as WhatsApp), while others may offer online private messaging as part of their broader offering of services. For example, social media platforms such as TikTok, Instagram and LinkedIn offer a direct messaging function, as well as other platforms providing different services such as Uber and Airbnb.
- **Price—**some services charge a subscription fee while others offer services for zero monetary price.[40] The varying business models for private messaging is further discussed in chapter 2.
- **Target audience—**some services target particular market segments. For example, Microsoft Teams and Zoom both have versions of their service that target business users (that is, users of the service for work/business purposes).[41] These provide greater functionality for business needs, including allowing users to join video and voice calls without creating a profile, higher video call participation limits, screen-sharing, scheduled meetings, and live support.

Consumers may use a variety of online private messaging services throughout their day. This is because, as noted above, online private messaging services differ in the features and functionalities offered and consumers may use multiple services for different purposes. The choice of service may also depend on who a consumer wants to communicate with and how they typically communicate with those other consumers. An example of how a consumer may use online private messaging services throughout a day is shown in figure 1.2.

---

39 ACCC, Communications sector market study final report, April 2018, p. 80.
40 This business model is discussed in further detail in ACCC, DPI Final Report, 26 July 2019, pp. 376–377.
41 These versions that target business users are often called 'enterprise' versions or packages.

**Figure 1.2: Example of a consumer's use of online private messaging services**




The ACCC also notes that other than online private messaging services, there are a large range of other forms of messaging services offered in Australia, including traditional SMS and Rich Communication Services.[42] The ACCC has previously recognised that online private messaging services provide a competitive constraint on SMS messaging services[43] and noted the growth of these services has followed a parallel decline in use of SMS services over time.[44]

A large and growing number of Australian consumers use online private messaging services. The Australian Communications and Media Authority (ACMA) estimated that as at June 2020, nearly 8 out of 10 Australian internet users used an app to communicate via messages, voice or video calls in the previous six months (compared to nearly 7 out of 10 Australian internet users doing the same in 2019).[45] The ACMA also estimated that 4 in 5 Australian adults started or increased their participation of video conferencing/calling since COVID-19 restrictions were introduced in March 2020.[46]

The ACMA research also noted that as at May 2019, younger users were more likely than older users to use online private messaging services, with 84 per cent of those aged 18–34

---

42 Rich Communication Services (RCS) is a communication protocol between network operators and smartphones that aims to replace standard SMS services to send and receive messages. RCS provides users with the ability to send and receive messages over a data network and provides an enhanced form of messaging, with multimedia support, typing indicators and group chat functionality, among other features. Google is introducing RCS functionality through the Chat feature of its Messages app.

43 ACCC, Communications sector market study final report, April 2018, p. 42.

44 ACCC, Mobile terminating access service declaration inquiry - 2018, 28 June 2019, p. 37.

45 ACMA, Trends in online behaviour and technology usage – ACMA consumer survey 2020, September 2020, p. 9.

46 ACMA, Trends in online behaviour and technology usage – ACMA consumer survey 2020, September 2020, p. 7.

using an app to send messages or make video or voice calls.[47] Further, recent research suggests that some younger demographics are spending less time on public methods of online communication, such as via traditional social media platforms like Facebook, and instead more on private channels to communicate, such as online private messaging services or social media platforms that offer a direct messaging function.[48]

For services that are standalone (that is, a service that provides online private messaging as its primary function; see section 2.1 for further information) and can be used across operating systems, Facebook Messenger is one of the most used online private messaging service in Australia, with an estimated 14.7 million monthly active users in June 2020, as well as WhatsApp, with 8 million monthly active users in the same time period.[49] Apple's iMessage is also widely used among Australians.[50]

The ACMA has also made similar observations regarding the significant use of Facebook Messenger and WhatsApp, reporting that in the 6 months prior to June 2020, 66 per cent of online Australian adults used Facebook Messenger and 39 per cent used WhatsApp. It also reported that 33 per cent of surveyed Australians reported used Apple FaceTime and 16 per cent used Apple iMessage in the same time period.[51] This survey data is discussed further in chapter 2.

Online private messaging services have also grown in importance during COVID-19 for consumers, with these services experiencing significant increases in usage during COVID-19.[52] Facebook reported in March 2020 that messaging increased by more than 50 per cent[53] and data and consulting firm Kantar's global survey of consumer attitudes and habits during COVID-19 found that WhatsApp has seen an overall 40 per cent increase in usage from the start of the pandemic up until April (when the survey was published).[54] Use of Zoom has also grown significantly, increasing from approximately 866 000 monthly active users in January 2020 to 5.6 million monthly active users in June 2020.[55]

The nature and extent of competition between online private messaging service providers is discussed in chapter 2.

---

47 ACMA, Communications Report 2018-19, 27 February 2020, p. 83.

48 See, for example, Global Web Index, Social Media by Generation, 2019, accessed 22 September 2020. Research suggests varied reasons for this move, qualitative research in 2019 suggested this could be attributed in part to concerns related to privacy and user preferences. See, for example, M Adorjan and R Ricciardelli, A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online, *Canadian Review of Sociology* Vol 56(1) February 2019; Edison Research, The Social Habit 2019, 30 May 2019, accessed 21 August 2020.

49 Nielsen Digital Content Ratings, Monthly Total, June 2020, P13+, PC, Smartphone, Tablet, Unique Audience.

50 Information provided to the ACCC.

51 ACMA, Trends in online behaviour and technology usage – ACMA consumer survey 2020, September 2020, p. 9.

52 Recent research by the eSafety Commissioner confirmed that COVID-19 has both influenced an increased use of video based online private messaging services, as well as the future intentions of users to continue their use after COVID-19. See eSafety Commissioner, Covid-19 impact on Australian adults' online activities and attitudes, June 2020, p. 10.

53 Facebook, Keeping our services stable and reliable during the COVID-19 outbreak, 24 March 2020, accessed 22 September 2020.

54 Kantar, COVID-19 Barometer: Consumer attitudes, media habits and expectations, 3 April 2020, accessed 22 September 2020. Kantar reported that it surveyed over 25,000 consumers in 30 markets between 14 March and 24 March 2020. See also Sarah Perez, Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic, TechCrunch, 27 March 2020, accessed 22 September 2020.

55 Nielsen Digital Content Ratings, Monthly Total, January 2020, June 2020, P13+, PC, Smartphone, Tablet, Unique Audience.

## 1.2. Update on search and social media services

- **Despite the entry of new platforms and expansion of existing platforms, consumers continue to spend a large proportion of their time on services owned and operated by Google and Facebook.**
- **While use of Google Search, Facebook, Bing and Snapchat have remained largely the same since 2019, use of DuckDuckGo and TikTok has grown; the growth of TikTok, in particular, may be partly due to the impact of COVID-19.**
- **Online advertising expenditure in Australia continues to increase and a growing proportion of expenditure is spent with Google and Facebook.**

This report examines general search services, social media services and the advertising services supplied on these platforms following their assessment in the DPI Final Report. The detailed analysis of these markets can be found at appendix B. The purpose of this analysis was to assist in determining the extent of any changes to the competitive conditions in these markets since the DPI Final Report in 2019.

In summary, the ACCC considers that Google continues to have substantial market power in the general search and search advertising markets, and that Facebook continues to have market power in social media and the overall supply of display advertising. However, the ACCC will continue to monitor changes through the course of the Inquiry, particularly for platforms subject to this Inquiry that are increasingly being used in Australia, such as TikTok.

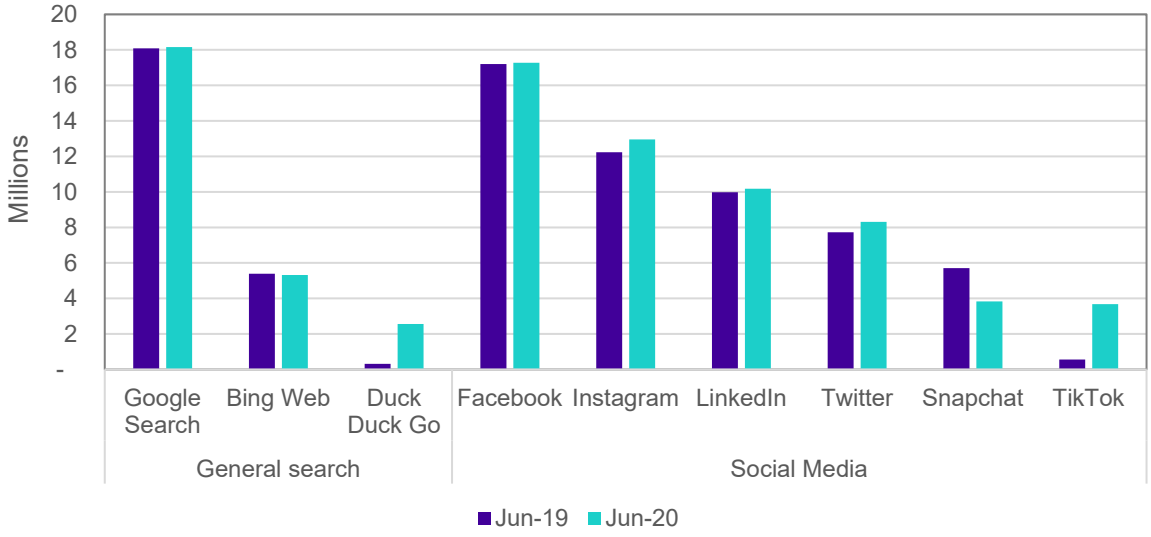
The remainder of this section considers recent trends in the use of search and social media services of consumers and advertisers.

### 1.2.1. Consumer use of social media and search services in Australia

Search and social media platforms are a part of the daily lives of many Australians, with users spending significant amounts of time each day on Google Search, Facebook, YouTube and Instagram.[56] Since May 2019, the number of unique monthly Australian users of platforms supplying general search and social media services has either remained roughly steady or grown (with the exception of Snapchat), as shown in figure 1.3.

[56] ACCC, DPI Final Report, 26 July 2019, p. 44.

**Figure 1.3: Use of search and social media platforms in Australia (June 2019 and June 2020)**




Source: Nielsen Digital Content Ratings, Monthly Total, June 2019, June 2020, P13+, PC, Smartphone, Tablet, Unique Audience.

Note: Figures shows number of monthly Australian unique users.

Since June 2019, there has been little growth in the number of unique monthly Australian users of the most popular search engines, such as Google Search, and established social media platforms such as Facebook. This may in part reflect that these platforms have been available to Australians for a number of years and, in the case of Google Search and Facebook, already have significant penetration in Australia, which may mean there is little room for further growth in user bases.

Some new and existing providers in social media and general search services have seen significant growth in users in Australia since 2019, in particular TikTok and DuckDuckGo. The growth of TikTok can likely be partly attributed to the impact of COVID-19 on Australians' online activity, as a means to spend leisure time and stay connected with friends and family.[57]

The increased use of DuckDuckGo may be due to an increasing preference of consumers for privacy protections in their use of online search services. Research conducted by DuckDuckGo indicated that people are taking 'meaningful actions to improve their privacy protections'[58] and that the substantial growth in DuckDuckGo traffic globally (an increase of worldwide daily average search queries from 39.1 million in June 2019 to 62.9 million in June 2020[59]) is indicative of this shift.[60] Rising consumer preference for privacy protections, including shifts from social media to online private messaging, is discussed further in chapter 3.

---

57 A survey by the eSafety Commissioner reported increases in the online use of social media and online private messaging services as a result of COVID-19. In particular, the survey reported that surveyed adults had increased their use of the internet to access social media for entertainment (25 per cent) and to make video calls with family and friends (23 per cent); 43 per cent of surveyed adults considered the internet to be essential to communicating and social interactions with family and friends; 69 per cent of surveyed adults intend to either maintain or increase their online activity to communicate and interact socially with family and friends. See eSafety Commissioner, COVID 19: Impact on Australian adults' online activities and attitudes, June 2020, pp. 3–5.

58 DuckDuckGo, New DuckDuckGo research shows people taking action on privacy, accessed 22 September 2020.

59 DuckDuckGo, DuckDuckGo Traffic, accessed 22 September 2020.

60 DuckDuckGo, New DuckDuckGo research shows people taking action on privacy, 3 October 2019, accessed 22 September 2020.

In addition to general search services, Australian consumers have turned to a range of platforms to increasingly conduct online transactions, some of which can be described as specialised search services.[61] In particular, since February 2019, platforms such as Amazon Australia have seen a marked increase in their use, growing from 8.1 million monthly active users in Australia to 10.3 million monthly active users in June 2020.[62] An examination of electronic marketplaces will be the subject of future reports for this Inquiry.

**Box 1.1: Emerging social media and search platforms**

Some emerging platforms in social media and search include:

- **TikTok**, a social media platform focused on the hosting and sharing of short-form videos between users. It has rapidly grown in Australia, rising from half a million unique users in May 2019 to almost 3.7 million unique users in June 2020.[63] TikTok is especially prevalent among younger users; Roy Morgan estimated that over a fifth of Australians in Generation Alpha (those born in 2006 until today) and about 14 per cent of Generation Z (born between 1991 and 2005) are now using TikTok.[64]
- **DuckDuckGo** is a search engine that does not collect, store or share users' personal information. DuckDuckGo also offers a privacy-focused browser and a search service extension that can be added to Google Chrome. In June 2020, it reported a daily average of 62.9 million queries entered on its search engine globally, an increase of 61 per cent from the daily average reported in June 2019.[65]
- **Amazon** is a multinational company that operates across a number of different industries, including e-commerce, cloud computing, online advertising services and streaming services. In particular, Amazon owns and operates Amazon Marketplace, a platform for end users and third party sellers to buy and sell goods. In December 2017, Amazon officially launched its Australian-specific e-commerce website. While there has been some growth in the use of the Amazon website[66], its position as a specialised search service (where users enter queries into Amazon's search engine to look for products) and its impact in Australia remains to be seen. Amazon's position as a supplier of online marketplaces will be considered in future monitoring reports.

Despite the entry and expansion of new and existing platforms, Google and Facebook owned and operated services continue to occupy a large proportion of consumers' time and remain an integral part of consumers' lives, as shown in figure 1.4.

---

61 ACCC, DPI Final Report, 26 July 2019, pp. 64–65; as noted in the report, specialised search services are restricted to providing information regarding an area of specialisation and typically provide certain features that are unavailable on generalised search services. Section 4 of the Direction covers specialised search services.

62 Nielsen Digital Content Ratings, Monthly Total, February 2019, June 2020, P13+, PC, Smartphone, Tablet, Unique Audience.

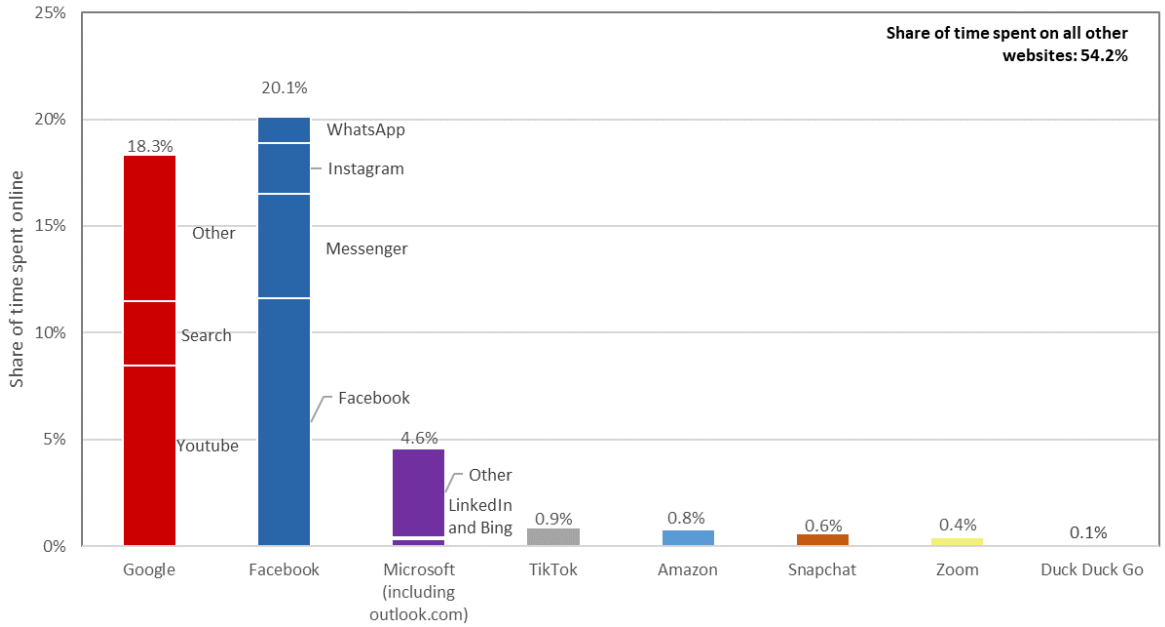
63 Nielsen Digital Content Ratings, Monthly Total, May 2019, June 2020, P13+, PC, Smartphone, Tablet, Unique Audience.

64 Roy Morgan, Over 1.6 million Australians already using TikTok, 24 February 2020, accessed 22 September 2020.

65 DuckDuckGo, DuckDuckGo Traffic, accessed 22 September 2020.

66 Data from Nielsen Digital Content Ratings reports growth in unique Australian monthly audience from 8.1 million in February 2019 to 10.3 million in June 2020.

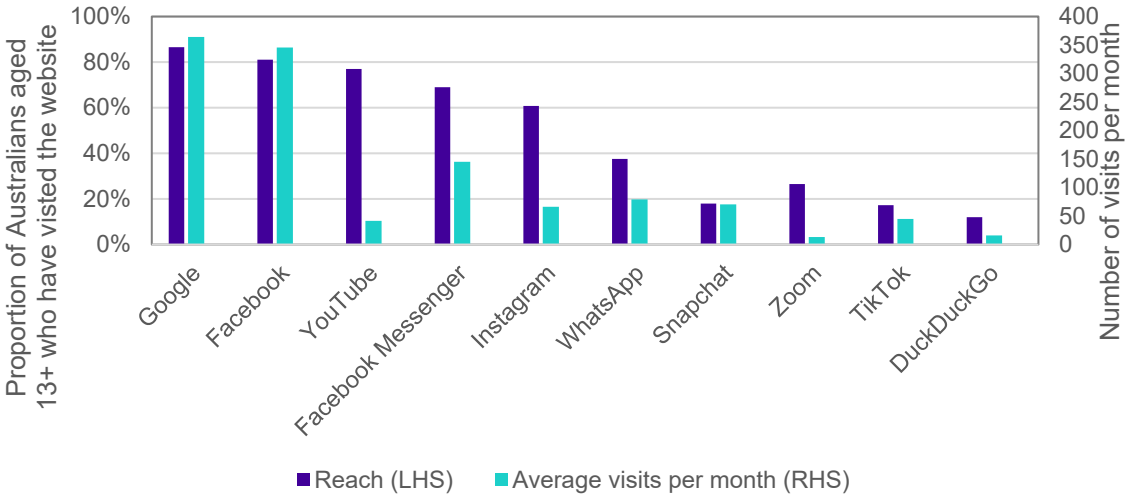
**Figure 1.4: Time spent on selected search, social media and messaging platforms in Australia (June 2020)**




Source: Nielsen Digital Panel, June 2020, All demographics, PC, Smartphone and Tablet, Total time spent. Note: Nielsen Digital Panel data does not capture use of iMessage, FaceTime or Google's Chat feature.

The continued prevalence of Google and Facebook services in the lives of Australians is also reflected in the reach (the proportion of Australians over 13 years who have visited a website) and the average number of daily visits to these sites. For example, figure 1.5 shows that approximately 80 per cent of Australian users aged over 13 years visited Facebook in a month, and that a user would typically access the platform an average of 345 times per month.[67]

**Figure 1.5: Digital engagement of Australians aged over 13 years with selected search, social media and messaging platforms (June 2020)**




Source: Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Active Reach and Average Frequency.

Note: Nielsen Digital Panel data does not capture use of iMessage, FaceTime or Google's Chat feature.

[67] Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Active Reach and Average Frequency.

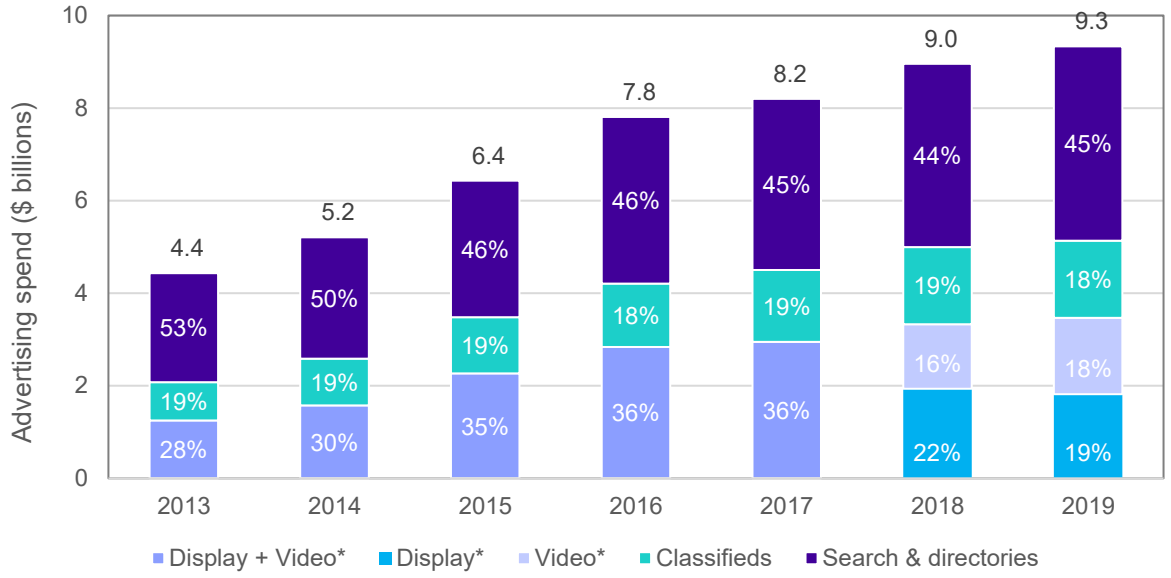
### 1.2.2. Search and display advertising expenditure in Australia

Online advertising is the key source of revenue for platforms that supply general search and social media services. The DPI Final Report found that Google was dominant in search advertising and that Facebook was dominant in the broad category of display advertising, noting that social media advertising was a specific kind of display advertising, displaying unique features. For the purpose of this report, online advertising is divided into three broad categories[68]:

- **search advertising**, which appear when a user performs a search query on a general search engine (such as Google and Bing) or a specialised search engine (such as Amazon or Expedia)
- **classified advertising**, which appear on general classifieds websites (such as Gumtree and Trading Post) or specific classifieds websites (such as Seek or Domain), and
- **display advertising**, which refers to all other types of online advertising, including advertising in banners or videos on webpages, in mobile apps, and alongside social media content.

As shown in figure 1.6 below, online advertising expenditure in Australia continues to grow. Across the various types of online advertising, video display advertising is reported as the fastest growing, experiencing 26.2 per cent growth in 2018[69] and increasing as a proportion of general display advertising, from 46 per cent to 53 per cent from the first quarter of 2019 to the first quarter of 2020.[70]

**Figure 1.6: Online advertising expenditure in Australia (2013 to 2019)**




* Video split out from general display for 2018 and 2019.

Source: PwC data, ACCC analysis.

Google, Facebook and YouTube (owned by Google) remain as the key sources of digital advertising inventory in Australia. In particular, expenditure on digital advertising services supplied by Google and Facebook appears to continue to grow, with PwC reporting that, 'beyond Google and Facebook, the rest of the online advertising market is in decline'.[71] This

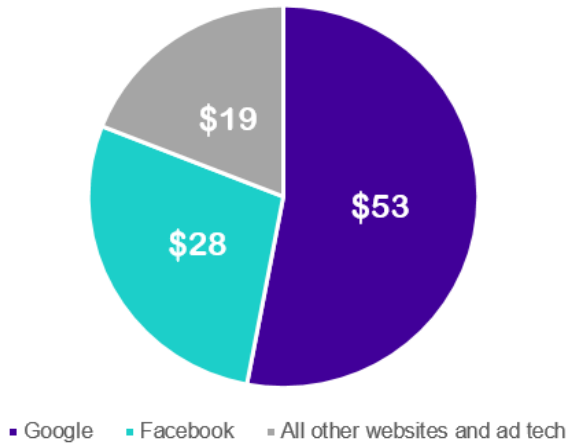
---

68 ACCC, Ad Tech Inquiry: Issues paper, 10 March 2020, p. 7.
69 PwC Australia, Australian Entertainment & Media Outlook 2019-2023, Internet Advertising, accessed 22 September 2020.
70 IAB Australia, Australian Online Advertising Expenditure Report for quarter ended 31 March 2020, p. 7.
71 PwC Australia, Australian Entertainment & Media Outlook 2019-2023, Internet Advertising, accessed 22 September 2020.

is also reflected in the proportion of advertising expenditure on Google and Facebook owned properties in Australia.

The ACCC notes that for a typical AU$100 spent by advertisers in 2018, $49 went to Google (including ad tech services), $24 to Facebook and $27 to all other websites and ad tech.[72] This trend has continued in the 2019 calendar year, with $53 to Google, $28 to Facebook[73] and $19 to all other websites and ad tech.[74]

**Figure 1.7: Breakdown of AU$100 spent by an advertiser in online advertising (excluding classifieds) in 2019**




Source: ACCC estimates, based on information provided to the ACCC. Figures are not comparable to information provided in the Final Report of the Digital Platforms Inquiry due to changes in calculation methodology.

The ACCC recognises that the advertising industry has been impacted by COVID-19, as spending throughout the economy slowed and expenditure in search and display advertising decreased in the first quarter of 2020.[75] Facebook advertising expenditure may also be impacted by a number of multinational advertisers which reportedly boycotted advertising on Facebook[76], but it remains to be seen how these and other events will affect the longer term advertising revenue of Google and Facebook owned and operated platforms, and also online advertising services in Australia more broadly.

---

72 Figures are not comparable to information provided in the Final Report of the Digital Platforms Inquiry due to changes in calculation methodology.

73 The ACCC notes that advertising revenue figures for Facebook relate to the amount of advertising revenue from customers in Australia, based on the location of the invoiced party (which may differ from the country in which the advertisements are shown). The ACCC understands that these figures are not recorded in the ordinary course of business by Facebook and are not audited, verified or otherwise reported on. As such, the ACCC considers that these are approximate estimates of relevant advertising revenue attributable to Australia for Facebook.

74 ACCC estimates, based on information provided to the ACCC. Figures are not comparable to information provided in the Final Report of the Digital Platforms Inquiry due to changes in calculation methodology. As with all estimates, there is a potential that this may under or overstate the actual market share of each firm or the total size of the market.

75 IAB Australia, Australian Online Advertising Expenditure Report for quarter ended 31 March 2020, p. 4.

76 In the announcement of its Q2 2020 results, Facebook noted that while its ad revenue has grown, 'the impact from certain advertisers pausing spend on our platforms related to the current boycott' will be reflected in its July trends: Facebook, Facebook reports second quarter 2020 results, 30 July 2020, accessed 22 September 2020.

# 2. Online private messaging services—competition assessment

- **Facebook and Apple are two of the largest suppliers of standalone online private messaging services in Australia.**
- **The significant size of the user base of Facebook Messenger and WhatsApp, and the presence of identity-based network effects, gives Facebook a significant competitive advantage over other suppliers of standalone online private messaging services in Australia. This advantage is likely to provide Facebook with a degree of freedom from competitive constraints in the provision of standalone online private messaging services.**
- **The significant size of iMessage's user base, coupled with the presence of identity-based network effects and the default position it holds on Apple devices, is also likely to provide it with a significant competitive advantage, particularly over smaller suppliers of standalone online private messaging services in Australia. However, these advantages are limited because iMessage is only available for Apple users. While Apple users can switch at a low cost to other standalone services such as Facebook Messenger and WhatsApp, non-Apple users would face higher costs in switching from other standalone services to iMessage.**

This chapter provides the ACCC's assessment of competition between suppliers of online private messaging services in Australia. This is the first time that the ACCC has examined these services in detail.

As discussed in chapter 1, there is a wide range of online private messaging services available to Australian users. Given the breadth of these services, the ACCC's competition assessment for this first report focuses on standalone online private messaging services (standalone services).

This chapter is structured as follows:

- **Section 2.1** describes standalone online private messaging services in Australia, their business models and usage of these services.
- **Section 2.2** discusses the competitive constraints on Facebook Messenger and WhatsApp, including from suppliers of similar online private messaging services, and barriers to entry and expansion in the supply of standalone online private messaging services in Australia.
- **Section 2.3** provides the ACCC's conclusion on the position of Facebook, through Facebook Messenger and WhatsApp, in the supply of these services.
- **Section 2.4** discusses the competitive constraints on Apple's iMessage feature on its Messages app (iMessage).
- **Section 2.5** provides the ACCC's conclusion on the position of Apple, through iMessage, in the supply of these services.

## 2.1. Standalone online private messaging services in Australia

As discussed in chapter 1, there are many suppliers of online private messaging services in Australia, offering differentiated products with a range of features and functionalities for different purposes. Broadly, online private messaging services can be offered as:

- **a standalone service**, where the primary function of the service is to provide users with the ability to communicate with others. Some standalone services focus on one particular form of communication, such as video calling, while others may provide a number of ways to communicate. Certain standalone services are only available on one operating system (for example, Apple's iMessage and FaceTime), while others can be downloaded and used across different operating systems and devices (such as Facebook Messenger and Zoom).
- **part of a broader offering**, where the ability to communicate with other users of the service is provided in addition to another service. For example, LinkedIn and Instagram both provide the ability for users to communicate with each other privately, in addition to their broader social media offering.

Standalone services are funded via a variety of different business models, including:

- advertising revenue—such as Facebook Messenger
- paid subscriptions—for example, Zoom, a business-focused service, offers a 'basic' plan for free and a 'business' plan for AU$27.99 per month per licence (which offers far more features than the 'basic' plan)[77]
- features offered on their apps—for instance, in addition to earning revenue from advertising, LINE also earns revenue from the sale of stickers, 'character goods' and e-commerce, among other digital services[78]
- sale of devices—services that are available only on specific operating systems or devices, such as iMessage and FaceTime, may be monetised through the sale of the devices on which they are available
- grants and donations—for instance, Signal is a non-profit company, funded through grants and donations.[79]

Figure 2.1 provides a snapshot of the usage of the most popular standalone services available in Australia (excluding iMessage, FaceTime and Google's Chat feature, which, similar to iMessage, provides users of the Google's Messages app with the ability to send and receive messages over the Internet, discussed further in box 2.1), based on monthly active users and time spent. As the ACCC was unable to access a single, consistent set of usage information across all major standalone services, box 2.1 below separately provides information on the usage of iMessage, FaceTime and Google's Chat feature in Australia.

Figure 2.1 shows that the time spent by Australians aged 13 years and over on Facebook Messenger and WhatsApp, when compared with other services, is significant, with:

- approximately two in three Australians using Facebook Messenger every month and spending, on average, 5 hours 41 minutes on the platform per month[80], and

---

77 Zoom, Choose a plan, accessed 22 September 2020.

78 LINE, Announcement of Additional Information of Summary of Consolidated Financial Results for the Six Months Ended June 30, 2020, 29 June 2020, p. 14.

79 Signal's website states that its service is 'Free for Everyone. Signal is an independent non-profit. We're not tied to any major tech companies, and we can never be acquired by one either. Development is supported by grants and donations from people like you'. See Signal, Signal, accessed 22 September 2020.

80 Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Active Reach and Average Time Spent.

- approximately one in three Australians using WhatsApp (owned by Facebook) and approximately one in four Australians using Zoom on a daily basis. While users spend an average of 2 hours 54 minutes on WhatsApp per month, Australians spend on average 1 hour 16 minutes a month on Zoom.[81]

In addition, Facebook Messenger and WhatsApp have also increased their monthly active user base over time while many other online private messaging services have seen their user base stagnate or only increase in recent months, as shown in figure 2.3 below.

The usage of iMessage and FaceTime in Australia is also significant. The ACCC understands that Apple's iMessage has an estimated range of 6 million to 12 million daily active users in Australia.[82] Further, a recent ACMA consumer survey found that that 33 per cent of online Australian adults used FaceTime in the six months to June 2020.[83]

Based on the information available to the ACCC, Facebook (through Facebook Messenger and WhatsApp) and Apple (through iMessage and FaceTime) are two of the largest suppliers of standalone services in Australia.

**Box 2.1: Usage of proprietary standalone services in Australia**

Apple and Google have proprietary apps that are only available on their respective operating systems. Apple's Messages is the default messaging app on iPhones, and iMessage is a feature of this app that is enabled by default. iMessage is also accessible on Apple laptops and tablets. FaceTime is a video and voice calling app on Apple mobile devices, and is pre-installed on those devices. Google's Messages is the default messaging app on certain Android devices, and similar to iMessage, has a 'Chat' feature that is available on some Android devices.

While users of Apple's Messages and Google's Messages can use these apps to send messages through the current standardised text messaging protocol, SMS, to all types of devices that have the ability to receive SMS, the iMessage and Chat features provide enhancements over SMS within the same app. These enhancements include enabling users to send and receive photos or videos, hold group chats and see read receipts. As such, the iMessage and Chat features bring the functionality of Apple and Google's default messaging apps closer to that of other popular standalone services such as Facebook Messenger and WhatsApp. However, these enhancements can only be used in messages between users who have these features enabled, and may be limited further to users who are using the same app. For example, an Apple user can only use iMessage to communicate with other iMessage users.

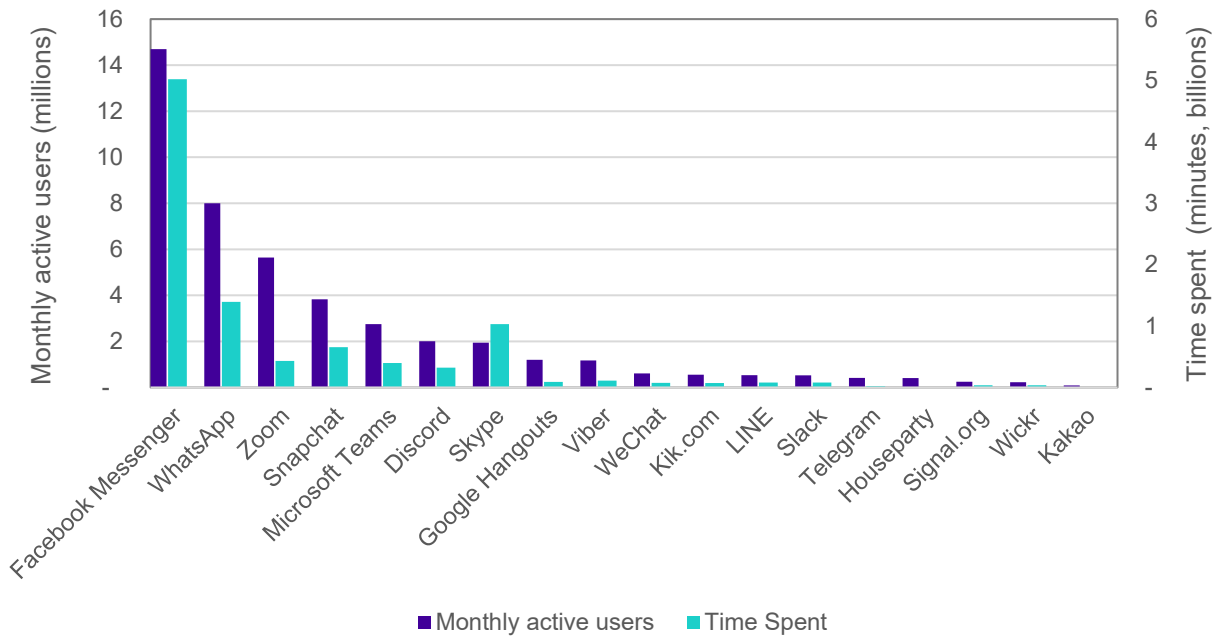
Similar to iMessage, FaceTime also only allows Apple users to video or voice call other FaceTime users. Estimates of iMessage and FaceTime use vary, and are based on different data sources and metrics. The ACCC understands that Apple's iMessage has an estimated range of 6 million to 12 million daily active users in Australia.[84] Public estimates of Apple's iOS operating system indicate that it occupies approximately half of the supply of mobile operating systems in Australia[85], and noting that iMessage is enabled by default on Apple's Messages, and Apple's Messages and FaceTime are pre-installed, this suggests that a substantial number of Australians may be regular users of iMessage and FaceTime. Further, the 2020 ACMA Consumer Survey reported that 16 per cent and 33 per cent of online Australian adults surveyed have used Apple iMessage and FaceTime respectively in the six months leading up to June 2020.[86]

On the other hand, the take up of Google's 'Chat' feature on Google's Messages has been relatively small.[87]

---

81 Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Active Reach and Average Time Spent.
82 Information provided to the ACCC.
83 ACMA, Trends in online behaviour and technology usage – ACMA consumer survey 2020, September 2020, p. 9.
84 Information provided to the ACCC.
85 Statcounter, Mobile Operating System Market Share in Australia, accessed 22 September 2020.
86 ACMA, Trends in online behaviour and technology usage – ACMA consumer survey 2020, September 2020, p. 9.
87 Information provided to the ACCC.

**Figure 2.1: Australian monthly active users and time spent in June 2020 for selected standalone online private messaging services (excluding iMessage, FaceTime and Google's Chat feature)**



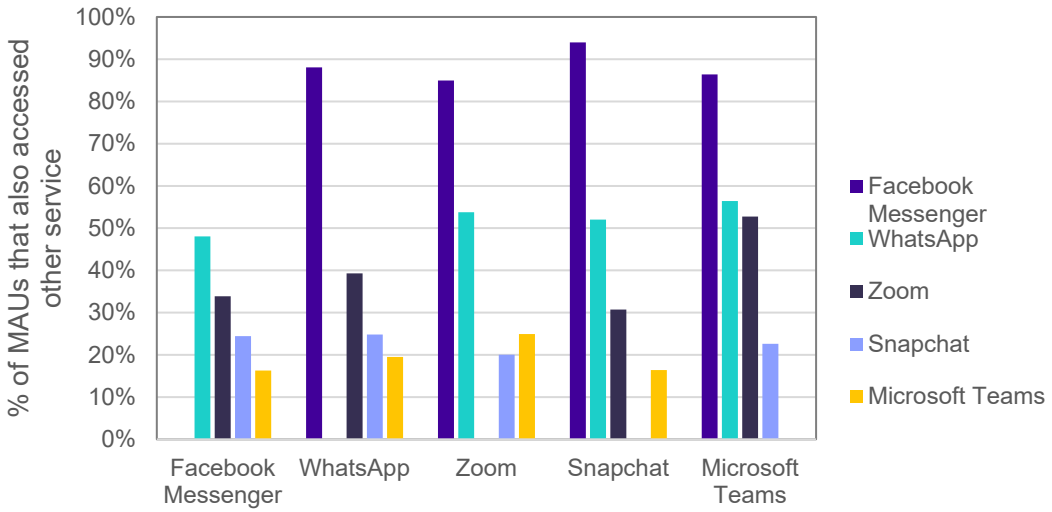

Source: Nielsen Digital Content Ratings, June 2020, Monthly Total, Persons 13+, PC, Smartphone and Tablet, Unique Audience and Total Time Spent.

Note: Nielsen Digital Content Ratings data does not capture use of iMessage, FaceTime or Google's Chat feature. Skype includes Skype and Skype for Business.

Many users of standalone services sign up to and/or use more than one service—that is, they multi-home. The degree of multi-homing differs across services. For example, among the top five most used standalone services in Australia (excluding iMessage, FaceTime and Google's chat feature), at least 80 per cent of WhatsApp, Zoom, Snapchat and Microsoft Teams users are also monthly active users of Facebook Messenger.[88] However, this multi-homing is asymmetric—of Facebook's monthly active users, only approximately 50 per cent also use WhatsApp, approximately 35 per cent use Zoom, less than 25 per cent use Snapchat and approximately 15 per cent use Microsoft Teams, as set out in figure 2.2.[89]

[88] Nielsen Digital Panel, June 2020, P13+, PC, Smartphone, Tablet.
[89] Nielsen Digital Panel, June 2020, P13+, PC, Smartphone, Tablet.

**Figure 2.2: Proportion of monthly active users that accessed another standalone service for the top 5 most used standalone services, excluding iMessage, FaceTime and Google's Chat feature (June 2020)[90]**




Source: Nielsen Digital Panel, June 2020, P13+, PC, Smartphone, Tablet; Note: Nielsen Digital Panel data does not capture use of iMessage, FaceTime or Google's Chat feature.

Figure 2.3 illustrates shifts in monthly active users of the five most used standalone services in Australia from May 2018 to June 2020 (noting that the data does not include usage of iMessage, FaceTime or Google's Chat feature and there was no record of usage of Microsoft Teams before April 2020).[91] The figure shows a gradual rise in the number of monthly active users of WhatsApp and Facebook Messenger, the rapid growth in Zoom users (likely linked to the COVID-19 pandemic) and the steady use of Snapchat (before a fall in usage from about January 2020 onwards).[92]

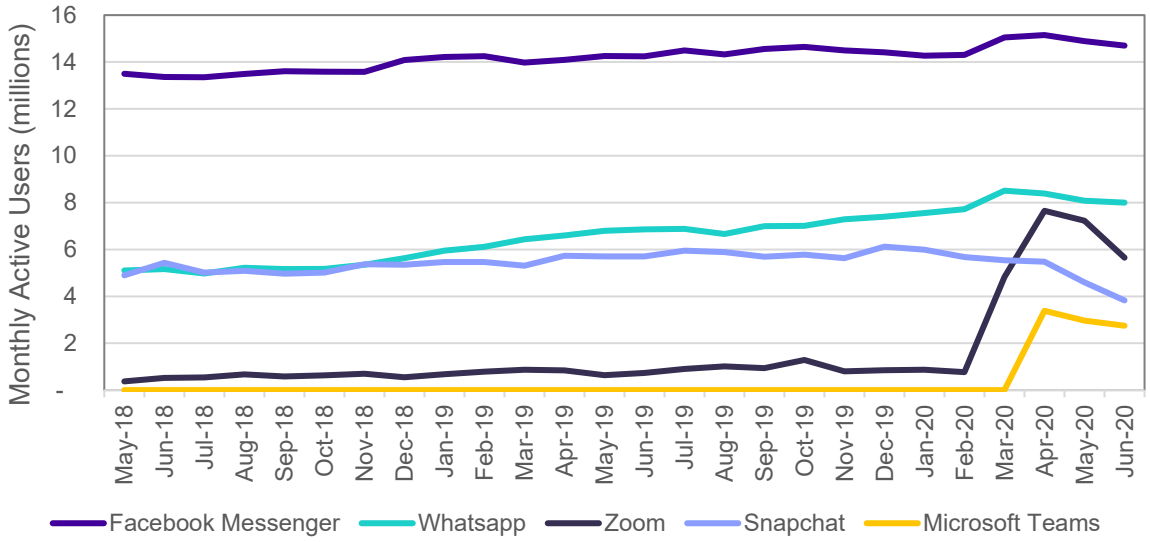
---

90 Refers to overlap in the monthly active users between two online private messaging services. As users can multi-home across more than two online private messaging services, proportions do not necessarily add to 100 per cent.

91 A 'monthly active user' is a unique user who visits a website or uses an app within the past month. As discussed earlier, some users multi-home across a number of online private messaging services.

92 The ACCC notes that there are some platforms that can be considered both a social media service and a standalone service. For example, the ACCC, in the DPI Final Report, considered Snapchat to be Facebook's closest competitor in the supply of social media services. The ACCC has included Snapchat in its analysis of standalone services because the ACCC considers that Snapchat's main function is the ability to send messages (by way of text, photos and videos) to other Snapchat users. In contrast, while Instagram, which shares certain similar features to Snapchat, provides users with the ability to send messages to other Instagram users as a secondary function, its main focus is to provide a platform to post photos and videos to a wide array of Instagram users, which is more akin to a social media function than messaging function, and so has not been included in the ACCC's analysis of competition between standalone services. The ACCC notes that the Bundeskartellamt considered Snapchat to be a 'messaging service'. See Bundeskartellamt, 6th Decision Division B6-22/16, 6 February 2019, p. 74.

**Figure 2.3: Australian monthly active users for the top 5 standalone services from May 2018 to June 2020 (excluding iMessage, FaceTime or Google's Chat feature)**




Source: Nielsen Digital Content Ratings, May 2018–June 2020, Persons 13+, PC, Smartphone and Tablet, Unique audience.

Note: These are the top 5 standalone services based on number of monthly active users as at June 2020. Nielsen Digital Content Ratings data does not capture use of iMessage, FaceTime or Google's Chat feature. Nielsen Digital Content Ratings did not record usage of Microsoft Teams before April 2020.

Given the significant use of Facebook Messenger and WhatsApp by Australian users, for this first report, the ACCC has assessed the competitive constraints faced by Facebook in the supply of its Facebook Messenger and WhatsApp services. Although there is variability in estimates of the use of iMessage (as described above in box 2.1), information provided to the ACCC indicates that iMessage has a significant user base in Australia. Further, iMessage holds the default position on iPhones, and around half of mobile devices used in Australia are Apple devices.[93] Therefore, the ACCC has also assessed the competitive constraints faced by Apple in the supply of its iMessage service. The ACCC has also specifically considered the competitive constraints posed by Zoom due to the high usage of this service.

## 2.2. Competitive constraints on each of Facebook Messenger and WhatsApp

Standalone services compete for users in a number of different ways, including by developing innovative ways for consumers to communicate, differentiating their services to better suit particular consumer groups, offering enhanced privacy controls, and on pricing and reliability.

Standalone services also give rise to identity-based network effects.[94] Since standalone services are not interoperable (that is, one cannot send a message from one service to a user on a different service[95]), the more a user's friends, family, colleagues and

---

93 Statcounter, Mobile Operating System Market Share in Australia, accessed 21 August 2020. These estimates indicate that Apple's iOS operating system occupies approximately half of the supply of mobile operating systems in Australia.

94 Identity-based effects exist where members of a group directly benefit from higher representation of members of their group on the platform (these may also be referred to as 'positive' direct network effects). With respect to online private messaging services, these network effects can also be described as 'identity-based' since the users' identity, rather than just the number of users, is relevant to determining the utility of the service to users.

95 The ACCC notes that for some online private messaging services, such as Zoom, an account is required to set up a video conference or call. However, users who subsequently join the video conference or call do not necessarily need an account to use the service.

acquaintances use a particular service, the more attractive that service is likely to be to that user. Services with a large and relevant user base have an advantage in enabling users to communicate with other people they want to communicate with. As such, standalone services also compete over the size and identity of their user base.

The ACCC has considered the extent to which other standalone services competitively constrain Facebook Messenger or WhatsApp. As discussed further in box 2.2 below, the ACCC considers that there are limited constraints imposed on these services by online private messaging services that are not standalone but are offered as part of a broader offering, and SMS and traditional voice services.

### 2.2.1. Closeness of competition between standalone services

As noted above, standalone services differentiate their offerings in a variety of ways. Services with similar user interfaces, technical features and user bases are more likely to be closer substitutes to each other. Table 2.1 below sets out the functionalities of some of the most used standalone services offered in Australia as at September 2020 (based on figure 2.1 and box 2.1 above) and the features upon which they compete. A more detailed table comparing the features and functionalities of a broader range of services is at appendix C.

**Table 2.1: Functionalities and features of selected standalone services in Australia**

| | | Facebook Messenger | WhatsApp | Snapchat | Zoom | Microsoft Teams | iMessage* | FaceTime* |
|---|---|---|---|---|---|---|---|---|
| **Messaging/ call features** | **Text** | • | • | • | • | • | • | ⊗ |
| | **Voice** | • | • | • | • | • | •[96] | • |
| | **Video** | • | • | • | • | • | •[97] | • |
| | **Video call participant limit** | 8[98] | 8[99] | 15[100] | 100[101] | 50[102] | ⊗ | 32[103] |
| **Device access point** | **Smartphone** | • | • | • | • | • | • | • |
| | **Tablet** | • | • | • | • | • | • | • |
| | **Computer** | • | • | ⊗ | • | • | • | •[104] |
| **Network** | **Ownership** | Facebook | Facebook | ⊗ | ⊗ | Microsoft | Apple[105] | Apple[106] |
| | **Target audience/ demographic** | Facebook users | Everyone | Young | Everyone, business | Everyone, Enterprise | Everyone, business | Everyone |

96 iMessage supports voice messaging where an audio message is recorded and sent to another user, but not voice calling. See Apple Support, Send photo, video or audio messages on your iPhone, iPad or iPod touch, accessed 23 September 2020.

97 iMessage supports video messaging where a video message is recorded and sent to another user, but not video calling. See Apple Support, Send photo, video or audio messages on your iPhone, iPad or iPod touch, accessed 23 September 2020. FaceTime, another app preinstalled on Apple devices, supports video calling. See Apple Support, Use FaceTime with your iPhone, iPad or iPod touch, accessed 23 September 2020.

98 Facebook has introduced Messenger Rooms, which allows group video calls of up to 50 people. See Facebook, Facebook Messenger Rooms, accessed 23 September 2020.

99 WhatsApp, Group Video and Voice Calls Now Support 8 Participants, *WhatsApp Blog,* 28 April 2020, accessed 23 September 2020

100 Snapchat, Snapchat support: voice and video chat, accessed 23 September 2020.

101 The limit varies by package: the Business package allows up to 300 participants, the Enterprise package allows up to 500 participants, and the Enterprise Plus package allows up to 1000 participants. See Zoom, Choose a plan, accessed 23 September 2020.

102 The limit varies by package. Microsoft recently increased the maximum number of participants in its paid packages from 250 to 300. Teams for Government is still subject to the 250 participant limit. Microsoft also announced plans to expand the number of participants visible on screen at any one-time to 49 in a 7x7 grid. See Microsoft, Limits and specifications for Microsoft Teams, 14 August 2020, accessed 23 September 2020; Microsoft Education Blog, What educators have learned from remote learning prepares them for the new school year, 15 June 2020, accessed 23 September 2020.

103 Apple Support, Use Group FaceTime on your iPhone, iPad and iPod touch, accessed 23 September 2020.

104 In addition to smartphones, tablets and computers, FaceTime audio call functionality can also be accessed on Apple's smartwatch device (Apple Watch) using the Walkie-Talkie app. See Apple Support, Use Talkie-Talkie on you Apple Watch, accessed 23 September 2020.

105 iMessage is only available on Apple operating systems.

106 FaceTime is only available on Apple operating systems.

| | | Facebook Messenger | WhatsApp | Snapchat | Zoom | Microsoft Teams | iMessage* | FaceTime* |
|---|---|---|---|---|---|---|---|---|
| | **Use by users outside network** | ⊗ | ⊗ | ⊗ | • (can join via web browser) | • (can join via web browser) | ⊗ | ⊗ |
| **Privacy** | **E2EE/privacy** | ⊗[107] | • | • | ⊗ (paid feature)[108] | • | • | • |
| **Chat/call features** | **Group chat** | • | • | • | • | • | • | • |
| | **Stickers/GIFs** | Stickers, Gifs | Stickers | Cameos | Stickers, Gifs | Stickers | Stickers, Gifs | ⊗ |
| | **Screen share** | ⊗ | ⊗ | ⊗ | • | • | ⊗ | ⊗ |
| | **Location tracking** | • | • | • (Snap Map) | ⊗ | ⊗ | • | ⊗ |
| | **Payment service** | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ |
| | **Other notable features** | Polls, Games | | Games | Polls, Waiting Rooms, screen sharing, co-annotation on shared screen, scheduled meetings | Teams, screen sharing, scheduled meetings | | Memoji and Animoji, Live Photos captured during a video call[109] |
| **Pricing** | **Upfront charges/ subscription fees** | ⊗ | ⊗ | ⊗ | Basic package is $0; plans with additional features at various costs | Free; plans with additional features at various costs[110] | Preinstalled on Apple devices[111] | Preinstalled on Apple devices[112] |
| | **Notable paid features** | | | Premium SnapChat | E2E Encryption, meeting recordings, live phone support[113], dial-in functionality.[114] | Meeting recordings, live phone support, dial-in functionality.[115] | | |

Source: ACCC analysis.

* iMessage and FaceTime are only available on Apple operating systems.

All of the standalone services set out in the above table offer some form of text, voice and video messaging, across different device types. A notable difference is, unlike the other services in the table, Zoom and Microsoft Teams (noting that it is replacing Skype for Business[116]) allow users outside of the network to use the service, offer various pricing plans with many targeted at business customers and have a much higher video call participant limit. These differences, both in the features offered and target audiences, reflect the

---

107 Facebook Messenger provides a 'secret conversations' feature which allows for end-to-end encryption. However, that feature is not provided by default and not available for group conversations. See Facebook, Secret conversations, *Facebook Help Center*, accessed 23 September 2020.

108 Zoom does not currently provide end-to-end encryption by default to free calls. However, on 17 June 2020 it announced that it will roll out end-to-end encryption to all users (including free users). See E Yuan, End-to-end encryption update, *Zoom Blog*, 17 June 2020, accessed 23 September 2020.

109 Apple Support, Use FaceTime with your iPhone, iPad or iPod touch, accessed 23 September 2020.

110 Paid versions of Microsoft Teams are only offered as part of the Microsoft 365 bundles which comprise a variety of office applications. See Microsoft, Microsoft 365 Business, accessed 23 September 2020; Microsoft, Microsoft Teams, accessed 23 September 2020.

111 Apple Support, About iMessage and SMS/MMS, accessed 23 September 2020.

112 Apple Support, Delete built-in Apple apps on your iOS 12, iOS 13 or iPadOS device or Apple Watch, accessed 23 September 2020.

113 For Business and Enterprise packages.

114 Available as an add-on. See Zoom, Zoom Pricing, accessed 23 September 2020.

115 Available as an add-on. See Microsoft, Compare Microsoft Teams Options, accessed 23 September 2020.

116 Skype, Skype for Business, accessed 22 September 2020.

differentiation in standalone services. For example (and with reference to other suppliers of standalone services detailed in appendix C):

- Zoom and Microsoft Teams have a primary focus on business customers and are aimed at facilitating communication and workplace productivity among staff and employees as well as providing enhanced features, such as data security and cloud storage. For example, Microsoft Teams markets itself as enabling 'instant messaging, audio and video calling, rich online meetings, mobile experiences, and extensive web conferencing capabilities. In addition, Teams provides file and data collaboration and extensibility features, and integrates with Microsoft 365 and other Microsoft and partner apps.'[117] Zoom notes that 'a growing number of businesses, small and large, use Zoom for a variety of use cases—agile scrum meetings, remote teams, product training, group mediation, customer support, sales interaction and many more'.[118] Both Zoom and Microsoft Teams offer pricing plans for business customers.

- Certain services focus on a particular type of online communication. For example, FaceTime only provides video and voice calling between Apple users. Zoom's emphasis on providing video conferencing facilities is highlighted in its mission, which is to 'make video communications frictionless'[119], although it does provide text messaging functionalities. Similarly, WhatsApp has noted that it 'started as an alternative to SMS. Our product now supports sending and receiving a variety of media: text, photos, videos, documents, and location, as well as voice calls'.[120]

- Some standalone services market themselves on their privacy controls. For instance, Signal offers end-to-end encryption for every message and call on its platform.[121]

This differentiation suggests that services such as Skype, Microsoft Teams, Slack or Zoom are likely to compete more closely with each other than with Facebook Messenger and WhatsApp, and therefore may pose a relatively weak constraint on Facebook Messenger and WhatsApp. However, the ACCC notes that this competition may be dynamic in nature as recent reports suggest that Zoom has been increasingly popular with non-business customers[122], and that Facebook Messenger's new video call feature, Messenger Rooms, has been developed in response to Zoom's success.[123] As discussed further below, the extent to which dynamic competition may constrain Facebook may also be tempered by the extent to which the services are used as complements as opposed to substitutes, and identity-based network effects.

The figures below further highlight some similarities and differences in the functionality of selected standalone online private messaging services. Outside of the top six most used standalone services discussed above, there are a number of other standalone services used in Australia, including Signal, Line, Threema and Discord. Further information about these services is set out in appendix C.

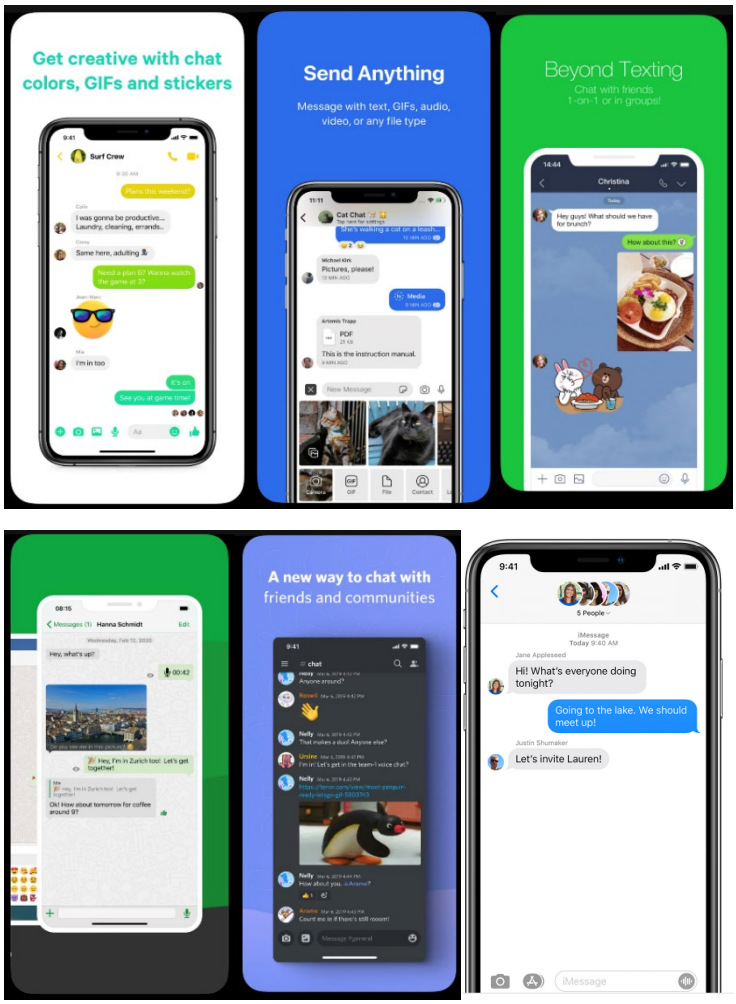
Figures 2.4 and 2.5 show there are strong similarities between the chat function of services like Facebook Messenger, WhatsApp, Signal, Line, Threema, Discord and iMessage. On the other hand, services like Snapchat, Zoom and Microsoft Teams have additional features (such as games and filters, screen sharing, and calendar integration) that distinguish them from other standalone services. The similarities between the chat function of some of these services suggests that some of these services may be likely to compete more closely with

---

117 Microsoft, Microsoft Teams service description, 31 July 2020, accessed 22 September 2020.
118 Zoom, Enterprise – Zoom, accessed 22 September 2020.
119 Zoom, About Us, accessed 22 September 2020.
120 WhatsApp, About WhatsApp, accessed 22 September 2020.
121 Signal, Signal, accessed 22 September 2020.
122 The Motley Fool, Zoom Video Communications Inc (ZM) Q1 2021 Earnings Call Transcript, 3 June 2020, accessed 22 September 2020.
123 Facebook, Introducing Messenger Rooms and more ways to connect when you're apart, *Facebook Newsroom*, 24 April 2020, accessed 22 September 2020. S Knight, Facebook's answer to Zoom and Houseparty is Messenger Rooms, *Techspot,* 25 April 2020, accessed 22 September 2020.

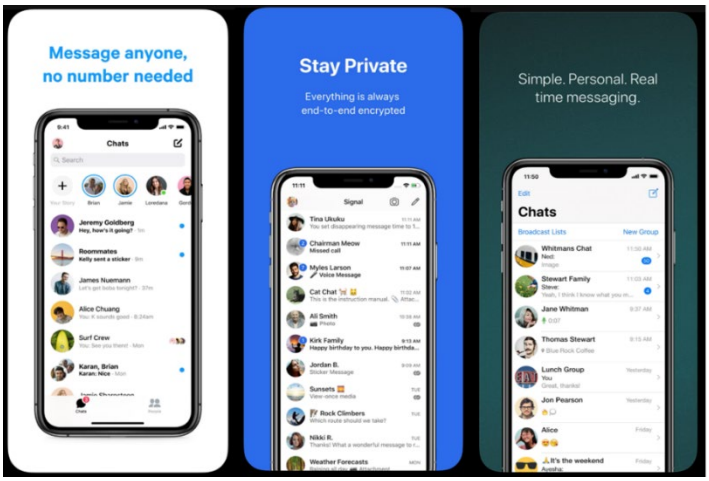
Facebook Messenger and WhatsApp than others. However, as noted above, the degree of this constraint may be tempered by identity-based network effects.

**Figure 2.4: Chat interfaces of selected standalone services**




Source: Apple App Store listings for Facebook Messenger, Signal, LINE, Threema, and Discord (provided in order of the source listing), accessed 30 June 2020; Apple, Send a group text message on your iPhone, iPad, or iPod touch, 14 April 2020, accessed 24 August 2020.

**Figure 2.5: Interfaces of Facebook Messenger, Signal, and WhatsApp**




Source: Apple App Store listings for Facebook Messenger, Signal, and WhatsApp, accessed 30 June 2020.

The ACCC notes the quick and significant uptake of Zoom during COVID-19. However, the degree to which Zoom may currently constrain Facebook Messenger and WhatsApp is unclear.

As discussed above, the key focus of Zoom is on its video calling functionalities and business customers, whereas Facebook Messenger and WhatsApp have only recently expanded their video calling features. Moreover, Facebook Messenger and WhatsApp do not currently enable as many participants on video calls as Zoom. The extension of Facebook Messenger's and WhatsApp's video calling features may provide a degree of competition with Zoom but the competition is unlikely to necessarily work the other way. That is, it is likely that Zoom users will continue to use Facebook's services for text and voice based messaging in parallel with Zoom's video calling services. Accordingly, the ACCC considers it is likely that Zoom is used as a complement to such services rather than as a substitute.

The ACCC also considered the extent to which standalone services that are limited to a particular operating system or device, such as iMessage and FaceTime, constrain standalone services such as Facebook Messenger and WhatsApp. Particularly, as iMessage is enabled by default on a significant proportion of smartphones, iMessage has a potential competitive advantage as users of Apple devices are not required to download or sign up to the application in order to use it. FaceTime is also preloaded on a significant proportion of smartphones and similarly, has a potential competitive advantage.

As iMessage is used by a significant number of Australians and may therefore enable users to communicate with many of their contacts, iMessage could be a relatively close substitute to Facebook Messenger and WhatsApp for Apple users. However, there are likely to be many Apple users who are unable to access all of their desired contacts through iMessage (in particular as around half of mobile devices used in Australia are not Apple devices[124], as noted in box 2.1). Converting all desired contacts to iMessage would require some contacts to change operating systems, and therefore devices, and it is likely to be costly for users to switch to iMessage if it involves purchasing an Apple device. Converting all desired contacts to FaceTime would similarly involve high costs.

As such, the ACCC's view is that while iMessage may be a relatively close substitute to Facebook Messenger and WhatsApp for Apple users whose close contacts have an Apple

[124] Statcounter, Mobile Operating System Market Share in Australia, accessed 22 September 2020.

device, for others, the competitive constraint imposed by iMessage and other proprietary services on Facebook Messenger and WhatsApp are limited by user switching costs.

For similar reasons, the ACCC's view is that while FaceTime may provide a similar service to Facebook Messenger's and WhatsApp's video and voice calling functionalities, the competitive constraint imposed by FaceTime is limited by user switching costs. Moreover, FaceTime users may continue to use Facebook's services for text messaging in parallel with FaceTime's video and voice calling service.

**Box 2.2: Constraint imposed by online private messaging services offered as a broader offering, and SMS and traditional voice services**

**Constraint imposed by online private messaging services offered as part of a broader offering**

As discussed above, there is a distinction between standalone services and services where communication is offered as part of a broader offering.

There is likely to be some potential for consumers to substitute between these two types of services to privately message other users, particularly for certain groups of users and for certain purposes. For example, users of WhatsApp or Facebook Messenger may be able to switch to the private messaging functions offered by social media platforms, such as Instagram, LinkedIn and Twitter. However, as the primary purpose for the use of these broader services is not communication (for example, the primary purpose of LinkedIn is for professional networking), the constraint imposed by such services appears to be weaker than the constraint imposed by other standalone services.

**Constraint imposed by SMS and traditional voice services**

There are similarities in the functionality of SMS and traditional voice services with online private messaging services (such as private communication). This indicates that they could provide some competitive constraint on online private messaging services, for some users and for specific purposes (for example, text-based one-to-one messaging). However, there are many features of online private messaging services that are not available through SMS or traditional voice services (such as group messaging, stickers, gifs and video calls), suggesting imperfect substitutability between these services from a consumer's perspective. In addition, the ACCC has found that consumers are increasingly using online private messaging services to communicate, in place of SMS but not the other way around.

In particular, the ACCC found that consumers were increasingly using over the top (OTT) messaging services (such as WhatsApp and Facebook Messenger), while the use of SMS had stagnated despite the fall in the cost of sending an SMS. As such, the ACCC reached the view that these services were an effective substitute for SMS services.[125] Mobile voice minutes showed a significant decline, indicating an increasing preference for using OTT communications services, either voice or message based, over traditional voice services.[126] It further found that the increase in the number of mobile phone plans with unlimited calls or texts is likely to reflect both a decline in the costs of providing these services as well as increased competition from OTT services that provide similar functionalities.[127]

[125] ACCC, Domestic Mobile Terminating Access Service Declaration Inquiry final report, June 2019, p. 24.
[126] ACCC, Communications Market Report 2018–19, December 2019, p. 7.
[127] ACCC, Communications Market Report 2018–19, December 2019, p. 36. A similar conclusion was reached in the ACCC, Communications sector market study final report, April 2018, p. 31.

### 2.2.2. Barriers to entry and expansion in the supply of standalone services

As noted above, services such as Facebook Messenger and WhatsApp give rise to identity-based network effects.[128] These network effects appear to be the key barrier to entry and expansion in the supply of standalone services. In order to attract individual users away from Facebook, rival standalone services need to attract some or many of the user's friends, family, colleagues and acquaintances to their service.

While the significant growth in the use of Zoom has shown that a new entrant is able to establish its own network, as noted above, it appears likely that Zoom is more often used as a complement, rather than a substitute to Facebook Messenger and WhatsApp. Accordingly, its entry is unlikely to be indicative of a strong competitive constraint on these services.

Other barriers to entry and expansion such as branding and customer inertia may also play a role. For instance, as noted in the DPI Final Report, while brand strength may reflect the quality of a service, if a consumer does not know the quality of a product and does not have the time to assess the quality of the product, the consumer may treat the prominence of a brand as an indicator of the quality of the product.[129] To overcome this effect and persuade customers to try their products, new firms may have to make substantial sunk investments in promotional activities to compensate customers for the risk they perceive in trying the new product.

Customer inertia may also create challenges for new entrants. For instance, consumers may have a tendency to stick with their current supplier so long as it continues to offer acceptable quality at an acceptable price, without reviewing whether a better deal could be achieved in the market (also known as status quo bias).[130]

With the exception of identity-based network effects, international competition regulators have previously found that some barriers to entering and expanding into the supply of online private messaging services may be relatively low. As part of the European Commission's (EC) investigation into Facebook's acquisition of WhatsApp, the EC found that developing and launching a consumer communications app did not require significant time and investment, nor are there any known patents that could constraint entry.[131]

In addition, in its 2014 decision regarding Facebook's acquisition of WhatsApp, the EC noted that costs to consumers to sign-up to, and use, alternatives to Facebook and WhatsApp appear to be relatively low:[132]

> *'consumer communications apps are offered for free or at a very low price…*
>
> *all consumer communications apps are easily downloadable on smartphones and can coexist on the same handset without taking much capacity…*
>
> *once consumer communications apps are installed on a device, users can pass from one to another in no-time…*

---

128 This is consistent with the findings of the European Commission in its decision regarding Facebook's acquisition of WhatsApp in 2014. The European Commission noted that 'Respondents to the market investigation indicated that the size of the user base and the number of a user's friends/relatives on the same consumer communications app is of important or critical value to customers of consumer communications apps. These parameters increase the utility of the service for a user since they increase the number of people he or she can reach. Therefore, the Commission considers that in the present case network effects exist in the market for consumer communications apps'. See European Commission, Comp/M.7217 - FACEBOOK/ WHATSAPP, 3 October 2014, pp. 23–24.

129 ACCC, DPI Final Report, 26 July 2019, pp. 72–73.

130 Economic and Social Research Council Centre for Competition Policy, Behavioural Economics in Competition and Consumer Policy, 2013, p. 111.

131 European Commission, Comp/M.7217 - FACEBOOK/ WHATSAPP, 3 October 2014, p. 22.

132 European Commission, Comp/M.7217 - FACEBOOK/ WHATSAPP, 3 October 2014, pp. 19–20.

*consumer communications apps are normally characterised by simple user interfaces so that learning costs of switching to a new app are minimal for consumers …*

*information about new apps is easily accessible given the ever increasing number of reviews of consumer communications apps on app stores.'*

This is supported by figure 2.2 **Error! Reference source not found.**above, which shows that many users of WhatsApp and Facebook Messenger in Australia currently multi-home.

Data portability does not appear to be a significant barrier to switching, given the temporal nature of online private messaging services.[133] In particular, the EC did not find that data portability issues would create a significant barrier to switching since communication via online private messaging services tended to not necessarily carry long-term value, and the messaging history would remain accessible on a user's phone even if they used a different app.[134]

## 2.3. Conclusions: competitive constraints on Facebook

While there are other providers of standalone services, some with similar features and functionality to Facebook's services, Facebook supplies some of the most used standalone services (Facebook Messenger and WhatsApp) in Australia.

Facebook Messenger's and WhatsApp's large user bases and the presence of identity-based network effects provides Facebook with a significant competitive advantage relative to alternative standalone services, including:

- a greater likelihood that new users will find other users that they want to communicate with on Facebook Messenger or WhatsApp, compared to alternative online private messaging services, and
- that existing users may have greater difficulties switching to alternative services where they may be less likely to find friends, family or contacts.

While Apple's online private messaging services are used by a significant number of Australians, their use is limited to users of Apple devices. For users wanting to communicate with users of other devices, Apple's services are not an effective alternative to Facebook Messenger and WhatsApp. This limits the competitive constraint that Apple's services impose on Facebook Messenger and WhatsApp.

Further, the ACCC does not consider online private messaging services supplied as part of a broader offering with other services, or SMS or traditional voice services, to be strong constraints on standalone services such as Facebook Messenger or WhatsApp.

While the ACCC notes the quick and significant uptake of Zoom during COVID-19, the ACCC does not have any information to suggest that Zoom currently offers a strong competitive constraint to Facebook Messenger and WhatsApp.

Accordingly, the ACCC considers that Facebook has a degree of freedom from competitive constraints in the supply of standalone online private messaging services.

## 2.4. Competitive constraints on iMessage

In addition to considering the competitive constraints on the Facebook standalone services, the ACCC has also considered the competitive constraints on iMessage, given its widespread use in Australia and the default position it holds on iPhones.

---

133 See, for example, Bundeskartellamt, 6th Decision Division B6-22/16, 6 February 2019, p. 81.
134 European Commission, Comp/M.7217 - FACEBOOK/ WHATSAPP, 3 October 2014, pp. 20–21.

Given the similarity of the features and functionality of iMessage and Facebook's standalone services, the nature of many of the competitive constraints on iMessage are similar to those discussed in section 2.2 in relation to Facebook.

As with Facebook's standalone services, some alternative standalone services have similar features and functionality to iMessage. However, standalone services that focus on a particular functionality (for example, Zoom's focus on providing video conferencing facilities) or target audience (for example, Microsoft Teams' focus on business customers) are differentiated and are unlikely to be a close competitive constraint on iMessage. As there are many features available through iMessage that are not available through SMS, SMS is unlikely to be as close a competitive constraint on iMessage as other popular standalone services (as discussed above in box 2.2). Further, as with Facebook, identity-based network effects make it difficult for new entrants to challenge iMessage.

However, as discussed above in section 2.2, iMessage is a feature of Apple's default messaging app and can only be used to communicate with other Apple users with the iMessage feature enabled. This results in two important differences between iMessage and Facebook's standalone services.

First, as iMessage is enabled by default on Apple devices, this default position provides it with a potential competitive advantage as users of Apple devices are not required to download or sign up to the service in order to use it. Further, as it is the default, many Apple users may not be actively choosing to use to iMessage.

Second, as iMessage is only available on Apple devices, it is costly for non-Apple users to switch to iMessage as switching involves acquiring an Apple device. Given that around half of mobile devices used in Australia are not Apple devices,[135] a significant number of Australians are likely to face this switching cost. Conversely, it is relatively inexpensive for Apple users to switch away from iMessage to another standalone service such as Facebook Messenger or WhatsApp as this may simply involve downloading and signing up to the service. As a result, the competitive constraints that Facebook Messenger and WhatsApp impose on iMessage are most likely to be stronger than the constraint iMessage imposes on Facebook Messenger and WhatsApp.

## 2.5. Conclusions: competitive constraints on iMessage

The ACCC understands that Apple's iMessage has an estimated range of 6 million to 12 million daily active users in Australia.[136] iMessage's large user base and the presence of identity-based network effects is likely to provide it with a significant competitive advantage over smaller standalone services. This advantage is likely to be enhanced by the default position that iMessage holds on Apple devices.

However, these advantages are limited by two factors. First, iMessage is only available to users of Apple devices. Second, there are low costs to Apple users for switching to other standalone services, in particular to Facebook Messenger and WhatsApp. Subsequently, the competitive constraints that Facebook Messenger and WhatsApp impose on iMessage are most likely to be stronger than the constraint iMessage imposes on Facebook Messenger and WhatsApp.

Therefore, while the ACCC considers that Apple, through iMessage, has a degree of freedom from competitive constraints in the supply of standalone services to users of Apple devices, this freedom is limited by the presence of Facebook Messenger and WhatsApp.

---

135 Statcounter, Mobile Operating System Market Share in Australia, accessed 22 September 2020.
136 Information provided to the ACCC.

# 3. Online private messaging services—key consumer concerns

- **Many Australian consumers are concerned with the tracking of their online activities and the sharing of their data with third parties. However, many online private messaging services have terms and policies that enable the collection of a broad range of information from their users, including through the use of cookies and other tracking technologies. Further, the disclosures regarding the collection, sharing and use of user's data are often vague and for many services, it is unclear as to who the potential third party recipients of user data are.**
- **As noted in chapter 2, a number of online private messaging services used by consumers are funded by advertising. While the content of messages between users is private, the policies of most services confirm that other user information (such as user's account, device and location information) may be used for targeted advertising.**

This chapter examines the relationship between consumers and platforms providing online private messaging services and discusses key consumer concerns.

Many Australian consumers are concerned with the sharing of their data with third parties and the tracking of their online activities. Recent research has noted that at least two thirds of those surveyed indicated that they are uncomfortable with information (including their browsing history and messages) being shared with third parties.[137] The Australian Community Attitudes to Privacy Survey 2020 by the OAIC (OAIC survey) found that 81 per cent of those surveyed considered the monitoring of their online activities and recording of information on the websites visited without their knowledge to be a misuse of their personal information.[138] In addition, the OAIC survey found that 82 per cent of those surveyed considered it a misuse for organisations to reveal their information to other organisations.[139]

Given these consumer concerns, the ACCC reviewed the terms and privacy policies that apply to consumers using key online private messaging services to understand the extent to which policies reflect consumer preferences and concerns (see box 3.1). The ACCC's review found that most platforms collect a broad range of consumer data (including personal information and location information) and that this information can be collected through cookies and other tracking technologies. The ACCC's review also found that many policies contain ambiguous and vague language and for many, it was unclear who or what information of users may be shared with third parties.

Information regarding the ACCC's review of online private messaging terms and privacy policies are outlined in box 3.1. Key findings of the ACCC's review are provided below.

---

137 Consumer Policy Research Centre, Consumer data and the digital economy: emerging issues in data collection, use and sharing, May 2018, p. 32.
138 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, pp. 36–37.
139 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, pp. 36–37.

**Box 3.1: ACCC review of online private messaging terms and privacy policies**

The ACCC reviewed the terms and privacy policies of the following online private messaging services between May and July 2020: Apple iMessage, Facebook Messenger[140], Google Hangouts, Signal, Viber, WeChat, WhatsApp and Zoom. [141] The ACCC's review considered the terms and policies in effect during that period.

Further information on the ACCC's review of online private messaging services' terms and policies, including its research in relation to the sign-up process of selected online private messaging services, is provided at appendix D.

## 3.1. Online private messaging services collect a broad range of user information through cookies and tracking technologies; the use of the information for advertising purposes is not made clear

The ACCC's review found that most online private messaging services are able to collect a broad range of user information through cookies and other tracking technologies.[142] Cookies are small files that are placed on user's computers and mobile devices that store data on a user's activity and browsing.[143] Cookies and tracking technologies enable platforms to collect extensive information about users, including for targeted advertising.

Many consumers are concerned with the tracking of their online activities. The ACCC's commissioned 2018 survey found over 77 per cent of digital platform users consider it a misuse of their personal information to have their online activities monitored, including on websites not directly connected to social media or search platforms, in order to be shown relevant ads.[144] The OAIC's 2020 survey indicates that more than four in five of those surveyed consider it a misuse of their information for an organisation to ask them for personal information that does not seem relevant to the purpose of the transaction.[145]

However, the ACCC's review found that some online private messaging services did not clearly outline the extent to which a consumer is tracked for the purpose of online advertising. For example:

- Some platforms, such as Facebook Messenger[146], Viber[147] and WhatsApp[148], describe the benefit of cookies and tracking technologies to users, and emphasise the importance of cookies to improve products or for user convenience.
- Platforms such as Apple[149] and Viber[150] describe the use of cookies as standard practice and some platforms, such as WeChat[151] and Zoom[152], include statements that discourage a consumer from deleting or disabling cookies.

---

140 The ACCC notes that in September 2020, Facebook announced that it would update its Terms of Service, effective 1 October 2020. See Facebook, Terms of Service, accessed 22 September 2020.
141 The ACCC reviewed the terms and policies of these online private messaging services between May to July 2020. For some platforms such as Facebook, Google and Apple, the terms of use and privacy policies that applied to search or social media services also applied to online private messaging services.
142 Other types of tracking technologies include web tags, ad-tags and pixels. For further information, see ACCC, DPI Final Report, 26 July 2019, p. 130.
143 ACCC, DPI Final Report, 26 July 2019, p. 130.
144 Roy Morgan, Consumer views and behaviours on digital platforms, November 2018, p. 21.
145 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, p. 36.
146 Facebook, Cookies & other storage technologies, accessed 21 May 2020.
147 Viber, Ads, Cookies & Tracking Technologies Policy, accessed 8 July 2020.
148 WhatsApp, Cookies Policy, accessed 8 July 2020.
149 Apple, Privacy Policy, accessed 8 July 2020.
150 Viber, Ads, Cookies & Tracking Technologies Policy, accessed 8 July 2020.
151 WeChat, Cookies Policy, accessed 8 July 2020.
152 Zoom, Cookie Policy, accessed 8 July 2020.

- In some cases, online private messaging service policies outline that a service's persistent cookies[153] can be stored for up to five years on a user's device.[154]

Box 3.2 below provides an example of the types of data that were observed to be collected by WhatsApp. This is provided by way of illustrative example and it is noted that the information collected by WhatsApp in this example (such as the user's contacts) may be collected to enable WhatsApp to provide their service to the user.

**Box 3.2: Example: What types of data does WhatsApp indicate it collects from its users?**

An ACCC staff member requested their WhatsApp account information in July 2020. They found that WhatsApp had stored account information such as their mobile phone number and profile photo, as well as device and connection information, such as the model of their mobile device, and the manufacturer of their device, and their network provider. The data also showed that WhatsApp collected information including their current IP address, and their previous IP address.

They had previously used WhatsApp on their desktop device, and found that WhatsApp could also store information about whether WhatsApp was active on their desktop.

They found that WhatsApp had the mobile phone numbers of all of their contacts (almost 350), and the names of every chat group they were a part of (which included group chats with family and friends).

They found that WhatsApp also stored information about their settings, including the phone numbers of the contacts they had blocked.

In addition, the ACCC found that some online private messaging services used vague language to indicate that a user's information could be used for advertising, or referred to advertising only after long lists of other uses for collected data. The ACCC also found that some online private messaging services framed advertising as a benefit to users, for reasons including that advertising allows platforms to 'provide free services'[155] and to 'personalise'[156] a user's experience.

The ACCC's review also found a number of services provided vague disclosures regarding the use of user information for advertising despite, as discussed in chapter 2, it being a key source of revenue for a number of platforms supplying online private messaging services. Some services also amended their descriptions over time. For example, some platforms, such as WeChat, had clearer descriptions of the use of data for advertising in previous versions[157] of their terms and privacy policies compared to more recent versions.[158]

Signal was the exception to these observations. Signal's web page states that 'There are no ads, no affiliate marketers and *no creepy tracking in Signal*'[159] (emphasis added). Further information on Signal is provided at box 3.3 below.

---

153 Types of cookies include 'session cookies' which last for the duration of a user's visit on a website, and 'persistent cookies' which last for a specified duration or until they are deleted by users.

154 This persistent cookie is 'used to record advertising opt-outs'. Facebook, Cookies & other storage technologies, accessed 3 September 2020. To view the types of browser cookies, see the hyperlinked description of 'cookies'.

155 Facebook, Data Policy, accessed 8 July 2020.

156 WeChat, Privacy Policy, accessed 2 February 2017; Viber, Privacy Policy, accessed 8 July 2020.

157 WeChat, Privacy Policy, as at 2 February 2017.

158 WeChat, Privacy Policy, accessed 8 July 2020

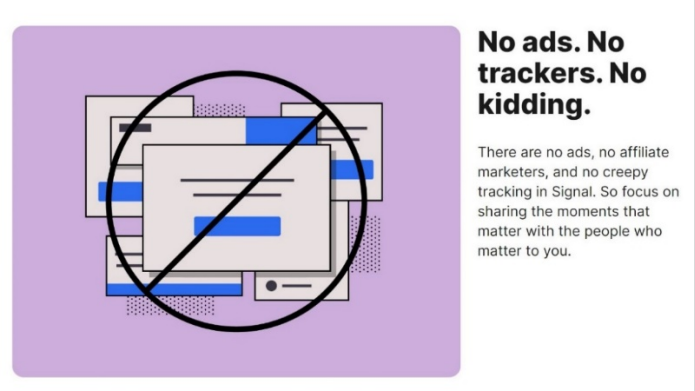
159 Signal, Homepage, accessed 8 July 2020

**Box 3.3: Signal**

Signal is a zero monetary price online private messaging service available for iOS and Android devices and desktop that allows users to send messages and make voice and video calls. Signal was developed by the Signal Technology Foundation, a non-profit organisation based in the US.[160] Signal does not use advertisements, and is supported by grants and donations.[161] It has gained particular prominence for its stated privacy and security features, some of which include:

- automatic end-to-end encryption of all messages and calls, which cannot be turned off[162]
- no ability to back messages up to a cloud service[163]
- a 'Screen Lock' functionality that requires a password or other biometric verification to view the app, even when the phone is unlocked,[164] and a 'Screen Security' functionality that prevents previews of the app and messages appearing when switching between apps[165], and
- the option to send 'disappearing' messages that are deleted after a set period of time[166] and 'view once' media messages that disappear after being viewed.[167]

Signal is also known for its policy of collecting minimal user data. This is reflected in its Privacy Policy which states that Signal 'does not sell, rent or monetize your personal data or content in any way—ever.' This is restated in images on its web page.




The encryption 'protocol' developed by Signal (that is, the technical system Signal developed to implement its form of end-to-end encryption) is the end-to-end encryption protocol now implemented by various other online private messaging services including WhatsApp[168], Facebook Messenger (in 'secret conversations'),[169] and Skype (in 'private conversations').[170]

## 3.2. Online private messaging services' disclosures regarding third party data sharing are unclear

Most consumers are concerned about the sharing of their information with third parties. The ACCC's 2018 commissioned consumer survey found over 90 per cent of digital platform

160 Signal, Donor FAQs, accessed 21 August 2020.
161 Signal, How can I contribute to Signal?, accessed 21 August 2020.
162 Signal, Signal Support - Is it private? Can I trust it?, accessed 20 August 2020.
163 Signal stores messages, pictures and files locally on a user's device. However, users may be able to manually back up their files by moving their backup file to a cloud service. Signal, Signal Blog – Technology Preview for secure value recovery, 19 December 2019, accessed 20 August 2020; Signal, Signal Support – Backup and Restore Messages, accessed August 2020.
164 Signal, Signal Support—Screen Lock, accessed 20 August 2020.
165 Signal, Signal Security—Screen Security, accessed 20 August 2020.
166 Signal, Signal Support—Set and manage disappearing messages, accessed 20 August 2020.
167 Signal, Signal Support—View-once Media, accessed 20 August 2020
168 WhatsApp, WhatsApp Encryption Overview—Technical white paper, 19 December 2017, accessed 21 August 2020, p. 3.
169 Signal, Signal Blog—Facebook Messenger deploys Signal Protocol for end-to-end encryption, 8 July 2016, accessed 22 September 2020.
170 Microsoft, Skype Support—What are Skype Private Conversations?, accessed 21 August 2020.

users consider that platforms should inform users who they are providing their personal information to.[171] In addition, 86 per cent of digital platform users considered the sharing of information with unknown third parties to be a misuse of their personal information.[172] The OAIC's 2020 survey similarly found that many Australians are uncomfortable with platforms and businesses sharing personal information and user data with other organisations, with 70 per cent of those surveyed 'very uncomfortable' or 'somewhat uncomfortable' with this practice.[173]

The ACCC's review found that the terms of use for online private messaging services indicate the providers may collect a broad range of information and this information can potentially be shared with a range of third party recipients. The ACCC found that disclosure around sharing data with third parties is vague for many online private messaging services.[174] Generally, it is not clear from online private messaging services' terms and policies who or what entities are considered to be third parties and what information is shared with those third parties (including third parties that receive user data and third parties that provide user data).

In some cases, services describe that third parties who may receive user data include related group companies, advertising partners, service providers (such as communication providers or payment processors), and measurement partners. For example, Google Hangouts' third parties include 'our partners—like publishers, advertisers, developers, or rights holders'.[175] In the case of Facebook Messenger, the range of potential third parties also include 'partners offering goods and services in our products', 'vendors and service providers' and 'researchers and academics'.[176]

## 3.3. Disclosures regarding security and privacy of messages

The ACCC's 2018 commissioned consumer survey found that over 40 per cent of digital platform users indicated that they didn't think or didn't know if digital platforms they used collected the content of their messages.[177] The OAIC's survey also found that approximately 28 per cent of those surveyed were not aware or do not know whether businesses target ads based on the content of their emails or other written, electronic communications.[178]

Some online private messaging services make statements about the privacy and security of their platform, including that the content of users' messages is not accessed by the platform, or are used for targeted advertising. Box 3.4 below outlines the extent to which online private messaging terms clarify if users' unencrypted private messages are used for targeted advertising.

**Box 3.4: Do online private messaging services use non encrypted private messages for targeted advertising?**

Many online private messaging services which do not offer end-to-end encryption by default state that they have a policy of not accessing or using the content of messages for advertising purposes. For example, while end-to-end encryption only applies to 'secret chats' in Telegram, its Privacy Policy states that it has a general principle of not using users' data to show them ads.[179] Similarly,

171 Roy Morgan, Consumer views and behaviours on digital platforms, November 2018, p. 17.
172 Roy Morgan, Consumer views and behaviours on digital platforms, November 2018, p. 21.
173 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, pp. 27–28.
174 Further information is provided at appendix D.
175 Google, Privacy Policy, accessed 8 July 2020.
176 Facebook, Data Policy, accessed 8 July 2020.
177 The survey asked respondents, 'Do you believe that the following types of information are being collected by digital platforms: (if I use a platform for these purposes) the content of my text messages, social media direct messages and emails)'. Roy Morgan, Consumer views and behaviours on digital platforms, November 2018, p. 19.
178 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, p. 24. In response to the question 'How many Australian businesses do you think do each of the following…target ads to people based on the content of their emails or other written, electronic communications', 24 per cent of those surveyed stated that they don't know and 4 per cent of those surveyed stated that no businesses do this.
179 Telegram, Telegram Privacy Policy, accessed 11 August 2020.

although only 'secret conversations' on Facebook Messenger are currently subject to end-to-end encryption, a 'Privacy & Safety' page states that Facebook does not use the content of messages between users for ad targeting.[180]

In some cases, it may not be clear from terms and policies whether an online private messaging service can access message content to personalise advertising. For example, Google Hangouts is subject to Google's Privacy Policy, which states that Google uses automated systems to analyse 'your content' for a number of reasons, which includes providing 'personalised ads'.[181] However, it is not clear whether the content of Google Hangouts calls or messages would be captured within the meaning of 'your content'.[182]

The ACCC notes that in circumstances where an online private messaging service states that it cannot or will not use the content of users' messages for advertising purposes, some policies confirm that other user information may be used for this purpose. For example, though messages on Viber are end-to-end encrypted, Viber's Privacy Policy states that 'Registration and Account information' (such as a user's name, email, age and phone number) may be used for targeted advertising.[183]

The ACCC notes that online private messaging services such as Facebook Messenger indicate they may analyse the content of users' messages for reasons including to detect prohibited behaviour, suspicious activity or spam content.[184]

A number of the online private messaging services examined by the ACCC stated that they provide end-to-end encryption of messages as an additional privacy feature for users. Box 3.5 provides an overview of 'end-to-end encryption' and explains some of the limitations of end-to-end encryption in securing users' messages.[185]

**Box 3.5: What is end-to-end encryption?**

End-to-end encryption is a method of protecting data so that it can only be read by the sender and recipient.[186] A message sent with end-to-end encryption is sent from the sender's device in a scrambled (or 'encrypted') form that is undecipherable (other than by 'the sender and intended recipient'[187] ) and then decoded (or 'decrypted') on the recipient's device.[188] This process can be likened to 'a locked mailbox. Anyone with a public key can put something in [the recipient's] box and lock it, but only [the recipient has] the private key to unlock it.'[189]

This process all occurs automatically, without the user necessarily being aware that their message has been sent or received through this process.

---

180 Messenger, Privacy & safety, accessed 22 September 2020.
181 Google, Privacy Policy, accessed 10 August 2020.
182 Google, Privacy Policy, accessed 2 September 2020. The policy states that Google collects 'the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.' Separately, the policy states that if you use Google services to make and receive calls or send and receive messages (which includes Google Hangouts), Google 'may collect telephony log information like your phone number, calling-party number, receiving-party number, time and data of calls and messages, duration of calls, routing information and types of calls'. This does not refer to call or message content.
183 Viber, Privacy Policy, accessed 11 August 2020.
184 Facebook Messenger, Privacy & safety, accessed 10 August 2020.
185 For an overview of selected online private messaging services and whether they offer end-to-end encryption, see appendix D.
186 N Perlroth, 'What Is End-to-End Encryption? Another Bull's-Eye on Big Tech', *The New York Times,* 19 November 2019, accessed 22 September 2020; N Unuth, What is End-to-End Encryption?, *Lifewire,* 12 August 2019, accessed 22 September 2020.
187 N Perlroth, 'What Is End-to-End Encryption? Another Bull's-Eye on Big Tech', *The New York Times,* 19 November 2019, accessed 22 September 2020.
188 N Perlroth, 'What Is End-to-End Encryption? Another Bull's-Eye on Big Tech', *The New York Times,* 19 November 2019, accessed 22 September 2020; N Unuth, What is End-to-End Encryption?, *Lifewire,* 12 August 2019, accessed 22 September 2020.
189 N Perlroth, 'What Is End-to-End Encryption? Another Bull's-Eye on Big Tech', *The New York Times,* 19 November 2019, accessed 22 September 2020. This scrambling and decoding is done by encryption algorithms that use 'keys', with each device generating a public key (which can be shared with anybody who wants to send a message to the user) and a private key (which never leaves the user's device). The sender's device uses the recipient's public key to encrypt the message, which sends it to the recipient in a scrambled form that can only be decrypted using the recipient's private key.

**Circumstances in which end-to-end encryption might not apply**

Where an online private messaging service does implement end-to-end encryption, it may only be available in certain circumstances.[190]

Furthermore, a message sent with end-to-end encryption may subsequently be stored in a way that is not subject to end-to-end encryption. For example, if a user backs-up messages to a cloud storage provider, it will make it easy for the user to restore their messages if they lose or change devices, but the security of the backed-up messages will be governed by the cloud storage provider's encryption which may not be end-to-end encrypted. Some online private messaging services including WhatsApp and Viber allow users to back-up messages to iCloud or Google Drive.[191] These back-ups are subject to Google or Apple's own server-side encryption which means that they, or anybody with access to a user's Google Account or iCloud account, have the capability to decrypt the backup.[192]

Similarly, where a chat history is stored locally on a users' device, archived messages are subject to the device operating system's encryption and security technology.[193]

## 3.4. Data accessed by online private messaging services and where it is going

It is difficult for a consumer to determine how their data is actually used and where it is going. Box 3.6 below provides a case study of a consumer's experience signing up to WhatsApp and an overview of the information that WhatsApp can collect from users according to its privacy policy.

Chapter 4 provides greater discussion of commissioned research by AppCensus, including its findings regarding its observations of the data collected and transmitted by Android apps, including online private messaging apps, during the testing period.

190 For example, LINE's end-to-end encryption cannot apply to group chats with more than 50 people, or any images or videos. LINE, LINE Encryption Report, 13 November 2019, accessed 22 September 2020.

191 WhatsApp, About Google Drive backups, accessed 22 September 2020; WhatsApp, How to back up to iCloud, accessed 22 September 2020; Viber, Back Up and Restore Viber Messages, accessed 22 September 2020.

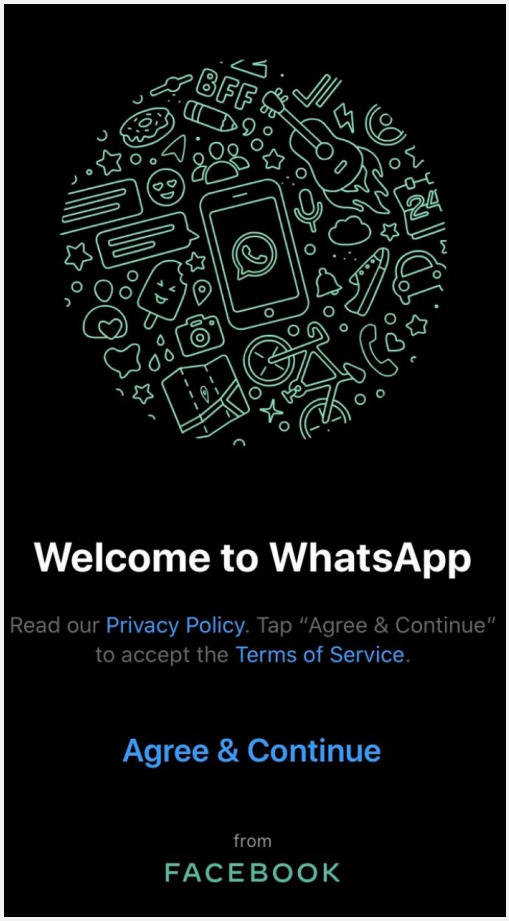
192 Y Ng and G Ivens, 'How to Back Up WhatsApp', *Witness*, 25 January 2019, accessed 22 September 2020.

193 G Zanon, 'No, end-to-end encryption does not prevent Facebook from accessing WhatsApp chats', *Medium,* 13 April 2018, accessed 22 September 2020; L Bershidsky, 'End-to-end encryption isn't as safe as you think', *Bloomberg Opinion,* 14 May 2019, accessed 22 September 2020; N Lomas, 'WhatsApp to share user data with Facebook for ad targeting—here's how to opt out', *TechCrunch*, August 26 2016, accessed 22 September 2020; N Douglas, 'Facebook isn't recording your conversations, but it may as well be', *Lifehacker*, 11 August 2017, accessed 22 September 2020.

**Box 3.6: Case study—WhatsApp's sign up process and the types of information it is able to collect from users under its privacy policy**

Charlie decides to sign up to WhatsApp to communicate with her family interstate and overseas during COVID-19. After downloading the app, Charlie opens WhatsApp and receives the following message. Charlie doesn't read the Privacy Policy or the Terms of Service and taps 'Agree & Continue'.

**Figure 3.1: WhatsApp screenshot taken by ACCC—as at 11 June 2020**



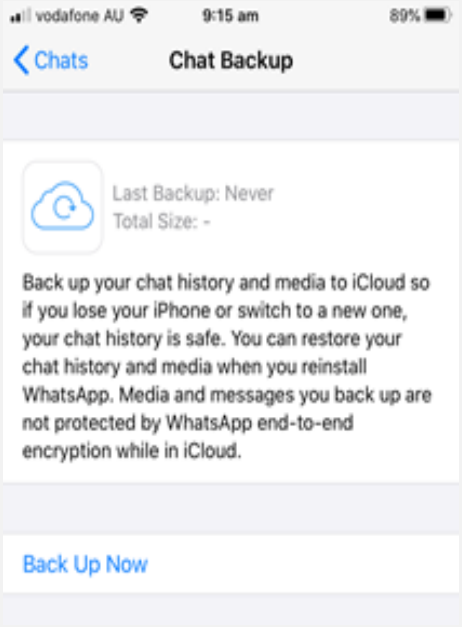

Charlie is asked to provide her phone number. Once her phone number is verified, WhatsApp asks Charlie to 'enter your name and add an optional profile picture'. Charlie uploads an old holiday photo and enters her full name.

Charlie then receives the following notification: 'WhatsApp would like to access your contacts. Upload your contacts to WhatsApp's servers to help you quickly get in touch with your friends and help us provide a better experience'. Charlie taps 'OK'.

Charlie starts regularly using WhatsApp to communicate with family and friends. When Charlie gets a new dog, Mason, Charlie regularly shares photos and videos of Mason in her family group chat. Charlie also uses WhatsApp to arrange a catch up with her friend and her friend's dog at the local park. Charlie's friend is having trouble finding her, so Charlie shares her location.

Charlie receives a notification to back up her chat history on WhatsApp, 'Back up your chat history and media to iCloud so if you lose your iPhone or switch to a new one, your chat history is safe….Media and messages you back up are not protected by WhatsApp end-to-end encryption while in iCloud'.

**Figure 3.2: WhatsApp—screenshot taken by ACCC as at 31 July 2020**




Charlie visits WhatsApp's FAQ page, where it also states, 'Media and messages you back up aren't protected by WhatsApp end-to-end encryption while in iCloud'.[194]

Charlie decides to read WhatsApp's Privacy Policy. Charlie finds that WhatsApp can collect the following information about her under its Privacy Policy:[195]

- Charlie's account information, including her mobile number; the mobile numbers of all of her contacts (including those who also use WhatsApp, and her other contacts who do not); her profile photo; profile name; and status message.
- Charlie's messages (including chats, photos, videos, voice messages, files and location information). WhatsApp states that, 'If a message cannot be delivered immediately (for example, if you are offline), we may keep it on our servers for up to 30 days as we try to deliver it. If a message is still undelivered after 30 days, we delete it'.[196]
- Charlie's usage and log information (including how Charlie uses and interacts with others on WhatsApp), log files and performance logs and reports.
- Charlie's device and connection information, including the hardware model of her mobile phone, operating system information, browser information, IP address and device identifiers of the devices Charlie uses to access WhatsApp.
- Charlie's location information, which is collected when Charlie shares her location with contacts, views locations nearby or those locations that others have shared with Charlie.
- Charlie's cookies information[197], which WhatsApp uses to 'understand, secure, operate, and provide our Services.'[198]
- Charlie's status information, such as when Charlie was last online or when she last updated her status message.
- Information about Charlie provided by third parties, such as Charlie's friends who also use WhatsApp. This may include Charlie's phone number, information about Charlie when they send her a message, or a message to a group chat they are both part of.
- Information about Charlie from third party providers and services. For example, WhatsApp may receive information about Charlie when she uses the WhatsApp share button on a news app to share the article with her work group chat.

Charlie reads that WhatsApp uses this information 'to help … operate, provide, improve, understand, customise, support and market its Services'. Charlie also has Facebook and Instagram accounts, and finds that WhatsApp receives information from, and shares information with other Facebook companies, including to 'provide…marketing for our Services and those of the Facebook family of companies'[199] Charlie reads that, 'However, your WhatsApp messages will not be shared onto Facebook for others to see. In fact, Facebook will not use your WhatsApp messages for any purpose other than to assist us in operating and providing our Services'.[200]

## 3.5. Conclusions

The ACCC's review found that, as with search and social media platforms[201], the terms and privacy policies of online private messaging services contain broad disclosures that enable these platforms to collect extensive information about users. While some of this information may be required to provide the service, online private messaging platforms often provide little clarity about the extent to which user data will be collected, used, or shared with others.

Given consumer preferences and concerns with data collection practices, the ACCC considers that online private messaging services' terms and privacy policies typically deepen information asymmetries and bargaining power imbalances between these platforms and consumers and further support the DPI Final Report's recommendations outlined in box 3.7.

**Box 3.7: Recommendations in the DPI Final Report to improve consumer choice and control of data**

The ACCC remains of the view that improved consumer choice and control of data are needed to address consumer concerns with platforms' data practices, including strengthened protections in the Privacy Act (recommendation 16) and an enforceable code which would require platforms to be more transparent about their data sharing, consent requirements and provide consumers with opt-out controls (recommendation 18).

194 WhatsApp, How to back up to iCloud, accessed 31 July 2020.
195 WhatsApp, Privacy Policy, accessed 30 July 2020.
196 WhatsApp, Privacy Policy, accessed 30 July 2020.
197 Cookies are small files that are placed on users' computers or mobile devices and store data on their activity and browsing. ACCC, DPI Final Report, 26 July 2019, p. 130.
198 WhatsApp, Cookies Policy, accessed 30 July 2020.
199 WhatsApp, Privacy Policy, accessed 30 July 2020.
200 WhatsApp, Privacy Policy, accessed 30 July 2020.
201 ACCC, DPI Final Report, 26 July 2019, pp. 401–407, 413–421.

# 4. Platforms and consumer harms

This chapter discusses the actual and potential consumer harms the ACCC has observed across platforms providing online private messaging, social media and search services and online advertising. This chapter is structured as follows:

- **Section 4.1** discusses the extensive online tracking of consumers by platforms and other third parties and associated harms on consumers.
- **Section 4.2** discusses the malicious targeting of consumers by third parties, through scams, on platforms.
- **Section 4.3** discusses the increased prominence of non-organic search results (including sponsored results) on Google Search and its effect on consumers and small businesses.

## 4.1. Extensive tracking of consumers' online activity

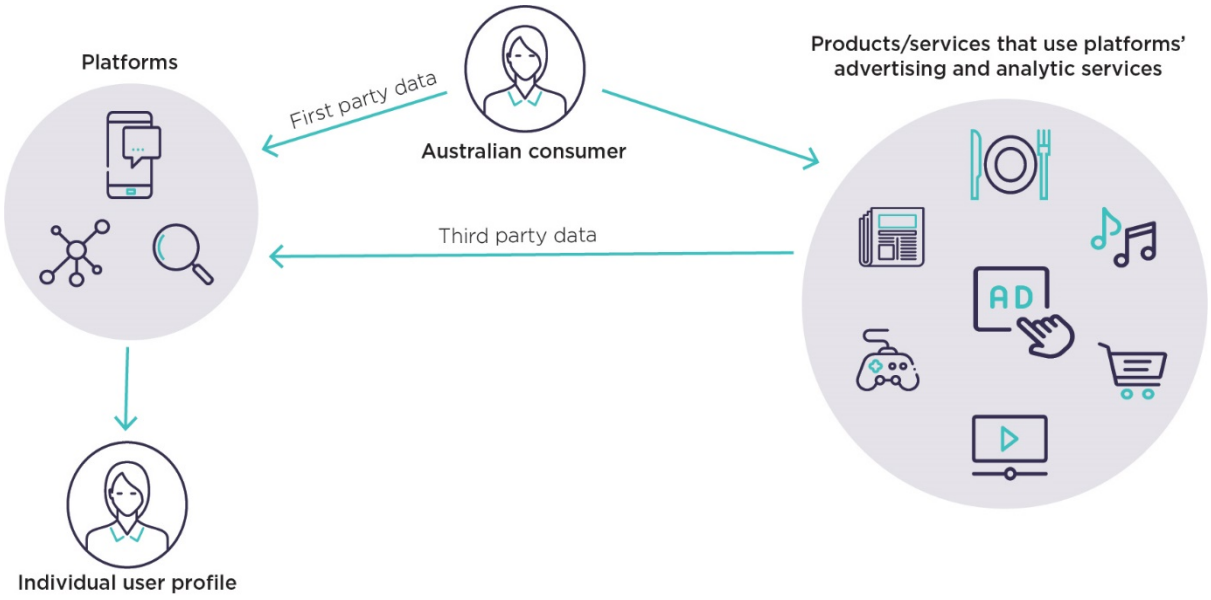
- **Despite increasing consumer concern about use of their information, new research conducted by the ACCC and AppCensus has found that consumers are tracked extensively online. Many popular online private messaging, social media and search services, including those provided by Facebook and Google, receive vast amounts of information on consumers' activity on websites and apps not connected to their platforms.**
- **AppCensus observed that many communications apps analysed, including online private messaging services, requested access to sensitive information from users and some were observed transmitting user's information to third parties during the testing period.**

### 4.1.1. Data, consumers and platforms

Platforms typically collect data from their consumer-facing products and services (known as first party data).[202] Large platforms such as Facebook and Google are also able to collect information about consumers through third parties that use their services for advertising purposes (known as third party data), as shown in figure 4.1 below. As noted in the DPI Final Report, consumer data is an important input to the supply of online advertising services.[203]

[202] ACCC, DPI Final Report, 26 July 2019, pp. 377–381; CMA, Online platforms and digital advertising market study final report, 1 July 2020, p. 49.
[203] ACCC, DPI Final Report, 26 July 2019, pp. 377–381.

**Figure 4.1: How platforms can collect user data**




Source: ACCC analysis. This figure is provided as an illustrative example of how platforms commonly collect user data and platforms may vary in how they collect and receive data.

Increased tracking and profiling of consumers has a range of potential and actual harms from decreased welfare, decreased privacy, risks from increased profiling and risks from discrimination and exclusion.[204]

Given these potential harms, the ACCC has sought to further examine the extent of tracking and profiling across 1000 popular websites and top 1000 popular Android mobile applications (apps) in Australia:

- Websites: The ACCC conducted an analysis of online tracking across 1000 popular websites in Australia in May 2020 using OpenWPM.[205]
- Android apps: The ACCC commissioned research from privacy analysis firm AppCensus to conduct an analysis of the top 1000 popular Android apps in Australia, including the top 100 'Health apps' and the top 100 'Kids apps'[206] on Android devices based in Australia during June and July 2020.[207] The purpose of the research was to examine the extent to which consumer data collected by apps may flow to platforms which provide online private messaging, social media and search services, as well as other businesses and third parties; and secondly, to examine the types of user information typically gathered by apps, and potentially provided to third parties.[208]

---

204 ACCC, DPI Final Report, 26 July 2019, pp. 442–448.

205 This analysis was performed using OpenWPM, a web privacy measurement framework. Using a sample of 1000 websites, on the 27 May 2020 the ACCC accessed each site from a clean browser session on a non-networked virtual computer and recorded the third party scripts each site accessed. These scripts were identified by domains and so were manually examined and grouped by their owners. Scripts have been classified as either tracking or non-tracking, based on the publicly available EasyList and EasyPrivacy lists (which provide rules for detecting trackers), and whether these indicate this particular instance of a script should be blocked. OpenWPM, accessed 13 August 2020; EasyList, accessed 13 August 2020.

206 Based on ranking and active users, the top 1000 most popular Android apps consist of top apps on the Google Play Store across all categories and at least 100 top apps in both the Fitness and Health categories ('Health apps') and in the Education, Games and Animation and Comics categories that are targeted to children aged 13 and under ('Kids apps').

207 Further information on AppCensus' methodology is at AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 4. Android apps were the focus of this analysis due to AppCensus' ability to analyse the Android operating system, which is based on open source code.

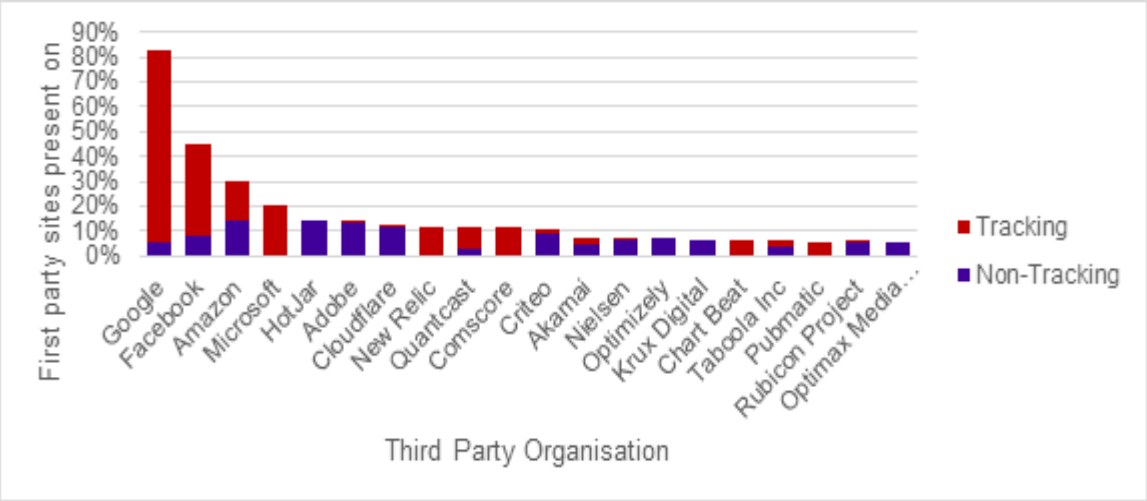
208 The dynamic nature of the analysis undertaken by AppCensus means that additional data could be detected under different, or even the same circumstances. Further information on the limitations of the research is provided at section 5 of the report. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. 13, 65–68.

Key themes coming out of this analysis are observed below.

### 4.1.2. Platforms continue to track consumers extensively online and large platforms such as Facebook and Google are the largest actual and/or potential recipients of user data

The ACCC's analysis found that almost all of the 1000 websites analysed contained a tracking method (such as cookies)[209], with large platforms such as Google and Facebook having the largest presence in online tracking.[210] For example, Google's third party scripts (see below)[211] were found on over 80 per cent of sampled websites, followed by Facebook (over 40 per cent of websites). Other large platforms, including Amazon, had the next largest number of third party scripts. As shown in figure 4.2 below, Amazon's trackers were observed on nearly 30 per cent and Microsoft on almost 20 per cent of sampled websites.[212]

**Figure 4.2: Third party scripts found on popular Australian websites**




Source: ACCC analysis.

Box 4.1 below provides further information on third party scripts.

**Box 4.1 What are third party scripts?**

Third party scripts are offered by developers and organisations, and can be embedded into websites to provide certain functionality.[213] For example, third party scripts may be used for analytics or advertising purposes, or to allow users to engage with a platform's services outside of its website.[214] Facebook's scripts can engage users outside of the social media platform by allowing them to 'like' or share content (known as 'social plugins').[215] As shown in figure 4.2 above, while third party scripts can be used to track users, not all third party scripts are tracking scripts.

---

209 While tools for blocking trackers do exist, these are not 100 per cent effective, particularly against some of the less common tracking methods such as canvas fingerprinting.

210 The ACCC's analysis was based on a sample of 1000 websites frequently visited by consumers in Australia, based on top ranked websites and the number of monthly active users. The websites analysed also included 100 health-related websites, 100 children-related websites and 800 other websites (such as social networking websites).

211 The ACCC's analysis was based on a sample of 1000 websites frequently visited by consumers in Australia, based on top ranked websites and the number of monthly active users. The websites analysed also included 100 health-related websites, 100 children-related websites and 800 other websites (such as social networking websites).

212 ACCC analysis.

213 B Vinegar and A Kovalyov, *Third Party JavaScript*, Manning Publications Co., New York, 2013, accessed 22 September 2020.

214 B Vinegar and A Kovalyov, *Third Party JavaScript*, Manning Publications Co., New York, 2013, accessed 22 September 2020.

215 Facebook for Developers, Social Plugins FAQs, accessed 22 September 2020.

Commissioned research by AppCensus of the 1000 most popular Android apps[216] in Australia found that Facebook received data from approximately 40 per cent of all apps analysed.[217] AppCensus also observed that user data was sent to advertising services providers and platforms such as Google, Amazon and Twitter (as discussed below).[218]

AppCensus further observed that third parties, including platforms, have the potential to collect a range of information from app users through apps' use of third party Software Development Kits (SDKs). AppCensus noted that, for example, apps containing Facebook's SDKs can communicate information to Facebook's servers by default (that is, without any configuration by the app developer), including the specific app that users install; the user's usage of the app (such as how long and often they use the app); and when users make in-app purchases in those apps.[219]

Facebook and Google were observed by AppCensus to have the greatest potential ability to collect user information through their observed prevalence of their respective SDKs in popular apps.[220] For example, Google's SDKs for advertising and analytics purposes were found embedded in 91 per cent[221] of apps analysed, while Facebook's advertising and analytics SDKs were observed on 62 per cent of apps.[222] AppCensus also observed that Google's ownership of the Android operating system and oversight of the Google Play Store provides it with further avenues to potentially collect user data.[223] Other platforms, such as Oracle, were observed having their analytics and advertising SDKs embedded in about 23 per cent of apps.[224]

AppCensus noted that third party SDKs that are embedded in an app are able to access the same user information as the host app[225] and the presence of third party SDKs is an important indication of potential data collection from apps.[226] Box 4.2 provides further information on SDKs.

---

216 AppCensus examined Android apps as Android is an 'open source' operating system, which means that the source code is available for others to use and modify. To conduct its analysis and observation of apps, AppCensus requires access to the source code. AppCensus does not have access to Apple's iOS source code. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 4.

217 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. vi–vii.

218 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. vi–vii.

219 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 27.

220 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii.

221 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 24.

222 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 24.

223 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. 25–26.

224 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 24.

225 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 21.

226 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii.

**Box 4.2: What are Software Development Kits (SDKs)?**

SDKs are a third party software component used to develop applications. Third parties, such as platforms, may provide SDKs to app developers so that they can be bundled with an app to provide a particular functionality. Some SDKs are therefore necessary to support the primary function of the app, while other SDKs are for secondary purposes, such as advertising.[227] However, in addition to providing functionality in service of the app, SDKs may also collect user information for secondary purposes.[228]

Third party SDKs which are embedded in an app can access the same user information accessible to their host apps.[229] This means that the presence of third party SDKs can indicate that user information can be potentially collected and transmitted to third parties.[230] Reports have noted that while 'SDKs themselves are not trackers, but they are the means through which most tracking through mobile apps occurs'.[231]

AppCensus also estimated that almost two thirds of apps have the ability to transmit user information to Facebook, regardless of whether those users have Facebook accounts.[232]

Similar research has been conducted internationally. Research from Privacy International found that at least 61 per cent of apps tested automatically sent data to Facebook, regardless of whether a consumer has a Facebook account and whether they are logged-in to Facebook.[233] More recently, reports indicate that Zoom's iOS app, which contained a Facebook SDK, had been found to send analytics information about user's devices to Facebook, regardless of whether those users were logged in, or had a Facebook account.[234]

Google's Android mobile operating system, hardware and development of the Google Play Store provides it with extensive access to user information. In addition to Google's SDKs being observed by AppCensus to be embedded Android apps[235], every Android device from an original equipment manufacturer certified vendor is pre-installed with several Google components.[236] AppCensus notes that this means that each time an Android user installs an app from the Google Play Store, Google can be notified of the app being installed and receive user information extracted from the device, including identifiers such as the Android Advertising ID.[237]

Many apps in the Google Play Store contain Google SDKs, often by default. For example, Google Play Services is required for developers to integrate some aspects of Google's Firebase[238] or Analytics functionality within their apps.[239]

As noted in box 4.3 below, the practice of tracking consumers for the purposes of targeted advertising is currently the subject of investigations by overseas regulators.

---

227 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 21.
228 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 21.
229 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 21.
230 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 21.
231 S Morrison, 'The hidden trackers in your phone, explained', *Vox*, 8 July 2020, accessed 22 September 2020. Others have similarly described that third party analytics packages and advertising technology code may be used to associate user data with information collected from other sources. See G Fleishman, 'Here's how to track the smartphone apps that are tracking you', *Fast Company*, 30 May 2017, accessed 22 September 2020.
232 AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 27.
233 ACCC, DPI Final Report, 26 July 2019, p. 391; Privacy International, How Apps on Android Share Data with Facebook – Report, 29 December 2018, p. 3.
234 Analysis undertaken by Motherboard. J Cox, 'Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account,' *VICE*, 27 March 2020, accessed 22 September 2020.
235 AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. iii-iv, 24.
236 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 26.
237 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 26.
238 Firebase, Dependencies of Firebase Android SDKs on Google Play services, accessed 22 September 2020.
239 Google Analytics, Add Analytics to Your Android app, accessed 22 September 2020; AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 26.

**Box 4.3: International cases relating to the collection of data for the purposes of targeted advertising**

In August 2020, Twitter noted in its corporate filing that it is being investigated by the US Federal Trade Commission (FTC) for potentially misusing users' personal information for the purposes of targeted advertising.[240] The FTC's draft complaint alleges that Twitter used the phone numbers and email addresses provided by users to verify and secure their account and provided this information to its advertising partners.[241] Under the terms of its settlement agreement with the FTC in 2011 in respect of an earlier investigation, Twitter was prohibited for 20 years from misleading consumers about the extent to which it protects the security, privacy and confidentiality of users' information.[242] In September 2020, a separate complaint was filed in the US District Court for the Western District of Washington, alleging that Twitter violated a state law against unauthorised procurement or sale of phone records by inadvertently using user's phone numbers for advertising purposes.[243]

There have been several complaints relating to platforms' collection of data for the purposes of targeted advertising under the General Data Protection Regulation (GDPR). In March 2020, web browser 'Brave' filed a complaint with the Irish Data Protection Commission alleging that Google's collection and sharing of data, including for advertising purposes, is in violation of the GDPR's requirement that data be collected for purposes which are clear and specific.[244]

As noted in box 4.5, Google's Android Advertising ID is currently the subject of a GDPR complaint filed with the Austrian Data Protection Authority, which alleges that the ID is generated without valid user consent.[245]

### 4.1.3. Key recipients of user information include other large platforms and businesses involved in the supply of advertising services

Table 4.1 below sets out AppCensus' findings in relation to the companies observed to receive the most user information from apps during the testing period.[246] A number of these companies are other large platforms, such as Google, Amazon and Twitter, or businesses involved in the supply of advertising services.

---

240 K Conger, 'F.T.C. Investigating Twitter for Potential Privacy Violations', *The New York Times*, 3 August 2020, accessed 22 September 2020.

241 K Conger, 'F.T.C. Investigating Twitter for Potential Privacy Violations', *The New York Times*, 3 August 2020, accessed 22 September 2020.

242 FTC, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information, 11 March 2011, accessed 22 September 2020.

243 Darlin Gray v Twitter, Inc., Class Action Complaint and Jury Demand, 21 September 2020, accessed 22 September 2020; A Ng, Twitter faces class-action privacy lawsuit for sharing security info with advertisers, CNET, accessed 22 September 2020.

244 J Ryan, 'Formal GDPR complaint against Google's internal data free-for-all', *Brave*, 16 March 2020, accessed 22 September 2020; Grounds of Complaint to the Data Protection Commission, Dr Johnny Ryan v 1. Google Ireland Limited, 2. Google LLC, 16 March 2020, accessed 22 September 2020.

245 Noyb, Google: if you don't want us to track your phone – just get another tracking ID, 13 May 2020, accessed 22 September 2020; Noyb, Complaint under Article 77(1), 80(1) GDPR, 12 May 2020, accessed 22 September 2020.

246 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 33.

**Table 4.1: AppCensus observations of the top ten recipients of user information from top 1000 apps during the testing period**

| | Company* | Number of top 1000 apps observed sending data to company |
|---|---|---|
| **1** | Facebook | 405 |
| **2** | AppsFlyer | 151 |
| **3** | Unity Technologies | 123 |
| **4** | Adjust | 113 |
| **5** | Google | 108 |
| **6** | Twitter | 81 |
| **7** | Verizon | 78 |
| **8** | Branch Metrics | 70 |
| **9** | Amazon | 44 |
| **10** | Liftoff | 44 |

Source: AppCensus analysis. AppCensus undertook an analysis of approximately 1000 Android apps with devices located in Australia during the testing period (June to July 2020)[247]

* AppsFlyer, Adjust, Branch Metrics, Liftoff and Unity Technologies are companies involved in the supply of online advertising services. For example, AppsFlyer is a mobile and marketing and analytics company; Unity Technologies is a video game software development company; Adjust is a mobile analytics and advertising measurement firm; Branch Metrics is a mobile measurement company; and Liftoff is a mobile app marketing platform [248]

The ACCC considers that many consumers would be unaware that these platforms and other businesses involved in the supply of advertising services are receiving user information in this way.

### 4.1.4. While consumers are increasingly concerned about the collection, use and sharing of their information, user information including location information continues to be requested by websites and transmitted by apps

Many consumers are increasingly concerned about their privacy and how their information—including their location information—is collected, used and shared.[249]

The ACCC's analysis found that location information is one of the categories of user data requested by popular websites in Australia. For example, the ACCC found that websites were observed to request a user's location 11 per cent of the time and their IP address 6 per cent of the time.[250]

The AppCensus research also found that a user's location information was a type of user information collected by apps and transmitted to third parties.[251] For example, AppCensus

---

247 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 33. AppCensus analysed the top 1000 Android apps in Australia from June–July 2020. Based on ranking and active users, the top 1000 most popular Android apps consist of top apps on the Google Play Store across all categories and at least 100 top apps in both the Fitness and Health categories ('Health apps') and in the Education, Games and Animation and Comics categories that are targeted to children aged 13 and under ('Kids apps'). For further information on AppCensus' methodology, see AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 4.

248 See AppsFlyer, accessed 4 September 2020; Adjust, accessed 4 September 2020; Branch, accessed 4 September 2020; Liftoff, accessed 4 September 2020; Unity, accessed 4 September 2020.

249 ACCC, DPI Final Report, 26 July 2019, pp. 382–386.

250 ACCC analysis.

251 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii, 16.

observed that a user's GPS coordinates was accessed by apps and was transmitted by almost 12 per cent of 'Health apps' and 7 per cent of 'Other apps'.[252] Additionally, as nearly all apps transmit the user's IP address to enable it to operate, almost every app can infer a user's location to city-level accuracy.[253] However, while AppCensus confirmed that data was transmitted by apps, how that information was ultimately used by the recipient was not observed by the research.[254]

Recent research and reports have also found that consumers continue to be uncomfortable with platforms' data practices as outlined in box 4.4 below.

**Box 4.4: Consumer attitudes to data collection**

Recent studies and reports have observed that many consumers are generally not aware of how their data is collected, used and shared online and many consumers are increasingly concerned about these data practices.

Deloitte's 2020 Australian Privacy Index found that only 7 per cent of those surveyed said that they had a 'very good' understanding of how their personal information is used after they consent to its use. [255] Further, Deloitte's 2020 survey found 83 per cent of consumers said that they are concerned about the use of cookies which track their online activity and use this information for targeted advertising or sell information on to third parties. [256]

The OAIC's 2020 survey on Australian attitudes to privacy found that 79 per cent of those surveyed consider an organisation inferring information about them (such as their mental health and political views) based on their online activities to be a misuse. [257]

In addition, the 2018 consumer survey commissioned by the Digital Platforms Inquiry found that 83 per cent of digital platform users considered sharing information with third parties to enable targeted advertising a misuse of personal information and 84 per cent considered using personal data for unrelated purposes to be a misuse. [258]

AppCensus observed that the most common type of user information that was accessed and transmitted by apps was the Android Advertising ID.[259] The Android Advertising ID was accessed and transmitted by over 60 per cent of apps in the categories of 'Health' and 'Other', and over 45 per cent of 'Kids apps'.[260] While the Android Advertising ID is a type of identifier that can be reset by users, AppCensus observed 32 per cent of apps transmitting the Android Advertising ID alongside other identifiers (as discussed below).[261] As noted by the Norwegian Consumer Council, the practice of collecting, combining and using identifiers allows the extensive tracking of consumers across apps and devices over time and the creation of highly detailed profiles of consumers.[262] Further information on the Android Advertising ID is provided in box 4.5.

252 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii, 16.
253 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii, 16.
254 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. 67-68.
255 Deloitte, Australian Privacy Index 2020, accessed 22 September 2020, p. 7.
256 Deloitte, Australian Privacy Index 2020, accessed 22 September 2020, p. 7
257 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, p. 36.
258 Roy Morgan, Consumer views and behaviours on digital platforms, November 2018, p. 21.
259 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. ii–iii.
260 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. ii–iii.
261 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. v.
262 Norwegian Consumer Council (Forbrukerradet), Out of Control – How consumers are exploited by the online advertising, 14 January 2020, p. 5.

**Box 4.5: What is the Android Advertising ID?**

The Android Advertising ID is a type of identifier that uniquely identifies a mobile device and can be used to track users over time and across services.[263] The Android Advertising ID is stored by a mobile device and shared with trackers in different apps[264] (similar to cookies on web browsers).[265] The Android Advertising ID is available to all apps by default and does not require special permissions or consents from users.

Unlike other types of identifiers, the Android Advertising ID's primary purpose is for advertising. For example, Google's Advertising ID page states that 'the advertising ID is a unique, user-resettable ID for advertising, provided by Google Play services. It gives users better controls and provides developers with a simple, standard system to continue to monetize their apps.'[266]

Although the Android Advertising ID can be manually reset by users, the Norwegian Consumer Council has noted that 'this does not necessarily work to limit the tracking capabilities of the identifier. If the Advertising ID is transmitted together with other identifiers, third parties can simply append the new Advertising ID to the other identifier, and resume tracking the user.'[267]

Google's developer guidelines prohibits developers from transmitting other identifiers alongside the Android Advertising ID (such as a device's serial number that cannot be reset), however apps have been observed to disregard this policy.[268] AppCensus observed that 32 per cent of apps were observed to transmit other identifiers alongside the Android Advertising ID.[269]

The Android Advertising ID is currently the subject of a complaint filed with the Austrian Data Protection Authority by not-for-profit privacy advocacy group Noyb, which alleges that the Android Advertising ID is generated without user consent.[270]

---

263 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 9.

264 These trackers may include third party trackers that are embedded within apps by being embedded into the source code. Most trackers in apps obtain an identification code from a user's mobile device or web browser, which can then be shared with third parties (such as the app developer). Reports have noted that while 'SDKs themselves are not trackers, but they are the means through which most tracking through mobile apps occurs'. See R Binns et al, Third Party Tracking in the Mobile Ecosystem,18 October 2018, p. 1; Y Grauer, 'Staggering variety of clandestine trackers found in popular Android apps', *The Intercept*, 24 November 2017, accessed 22 September 2020; S Morrison, 'The hidden trackers in your phone, explained', *Vox*, 8 July 2020, accessed 22 September 2020; G Fleishman, 'Here's how to track the smartphone apps that are tracking you', *Fast Company*, 30 May 2017, accessed 22 September 2020.

265 B Cyphers, Behind the One-Way Mirror: A Deep Dive Into The Technology of Corporate Surveillance, Electronic Frontier Foundation, 2 December 2019, p. 1.

266 Google, Advertising ID, accessed 22 September 2020.

267 Norwegian Consumer Council (Forbrukerradet), Out of Control—How consumers are exploited by the online advertising, 14 January 2020, p. 29.

268 S Egelman, 'Ad IDs Behaving Badly', The AppCensus Blog, 14 February 2019, accessed 22 September 2020.

269 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. v.

270 Noyb, Google: if you don't want us to track your phone – just get another tracking ID, 13 May 2020, accessed 22 September 2020. The complaint alleges that Android Advertising ID violates Europe's General Data Protection Regulation because it is generated without the consent of consumers. Additionally, the complaint alleges that consumers do not have real control over it as it can never be deleted and only reset.

### 4.1.5. Online private messaging services were observed requesting access to sensitive information from users and some were observed transmitting data to third parties

As part of its analysis of 1000 apps, AppCensus analysed 75 communications apps, which included online private messaging apps, during the testing period.[271] Of these, 45 apps were observed to have transmitted data to at least one third party recipient.[272]

AppCensus's review of each app also observed that 71 communications apps[273] requested access to at least one type of 'dangerous' permission during the testing period.[274] These types of permissions are labelled as 'dangerous' by Android as they have the potential to request sensitive user information, or could potentially affect a user's stored data or the operation of other apps.[275] For example, the types of 'dangerous' permissions requested included:

- access to a user's camera (requested by 52 communications apps)[276]
- access to a user's location (requested by 43 communications apps)[277]
- access to read a user's contacts (requested by 46 communications apps)[278]
- access to read from and write to a device's external storage[279] (requested by 61 and 68 communications apps respectively) [280], and
- permission to record audio (requested by 46 communications apps).[281]

AppCensus observed that 25 communications apps[282] used at least one of the 'dangerous' permissions that it requested.[283]

While these actions may have been permitted by the terms of an online private messaging service (as noted in chapter 3), it can be difficult for a user to understand what data is being accessed and/or transmitted due to the vague nature of these terms. The repeated use of

---

271 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-1. This refers to apps analysed in the 'Communications' category on the Google Play Store.

272 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, pp. D-87–D-92. See table 85. Further information on the permissions that each app was observed to have requested and used during the testing period, as well as the data observed to have been transmitted to third parties, are detailed for each app analysed by AppCensus in Appendix F. See AppCensus, 1000 Mobile Apps in Australia: Appendix F: App Analysis Data, 24 September 2020.

273 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-106–D110. See table 93.

274 Android describes 'dangerous' permissions as covering 'areas where the apps wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of others apps. For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant permission to the app'. See Android, Permissions overview, accessed 22 September 2020.

275 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 38. Android, Permissions overview, accessed 15 July 2020. AppCensus notes that while Android labels these permissions as 'dangerous', the 'declaration and use of 'dangerous' permissions (neither the specific types, nor the quantity) does not necessarily indicate privacy-invasive behaviour' (p. 38). A description of these 'dangerous' permissions is at section 4.3 of the AppCensus Report. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. 38–39.

276 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-97.

277 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-97. For example, 43 apps requested for access to a user's 'fine' location and 43 apps requested access to a user's 'coarse' location.

278 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-97.

279 This refers to an app's ability to access and write to any file outside the app's specific directory. See Android, Data and file storage overview, accessed 22 September 2020.

280 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-97.

281 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, p. D-97.

282 AppCensus, 1000 Mobile Apps in Australia: Appendix D: Other Apps, 24 September 2020, pp. D-106–D-110. See table 93.

283 The ACCC notes that AppCensus's report indicates there may be instances where the permissions requested and used by apps were not detected as not all features of apps were tested, in particular, apps which required 'lengthy' sign up account processes. The permissions that AppCensus observed apps to request and use may understate the extent to which apps use these permissions in practice. See AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 67.

'may' in online private messaging services' terms and policies also means it is not clear what is actually occurring.[284]

### 4.1.6. Data collection practices have the potential to cause harm for consumers, and in particular for vulnerable consumers

The ACCC considers that it is difficult for a typical consumer to be aware of the extent to which their data is collected, used and shared by apps and third parties, and that, this lack of transparency enables user data to be misused.

The ACCC has previously identified the potential consumer harms which can result from significant information asymmetries, bargaining power imbalance and behavioural biases between platforms and consumers to obtain broad discretions in the collection, use and disclosure of user data.[285] As discussed in appendix D, the ACCC has found continued examples of these harms ranging from risks to consumers from increased profiling, the potential for discrimination and exclusion and risks to vulnerable consumers.

In particular, the ACCC has observed that social media platforms have been subject to recent regulatory settlements and investigations regarding their alleged collection and processing of children's data, as discussed in box 4.6 below.

**Box 4.6: Cases involving the collection and processing of children's data**

**Google and YouTube**

In September 2019, Google and YouTube agreed to pay a penalty of USD170 million as part of its settlement with the US FTC and the New York Attorney General for allegedly collecting personal information from viewers of YouTube channels targeted at children.[286] This information was alleged to have been collected for the purposes of targeted advertising, and obtained without parental consent, in breach of the *Children's Online Privacy Protection Act*.[287] The FTC stated in its complaint that YouTube had actively marketed itself as a popular destination for children, with its marketing materials stating that YouTube is 'the favourite website for kids 2–12'.[288]

**TikTok**

Social media platform TikTok has faced scrutiny over its handling of children's data. In February 2019, Musical.ly (which was acquired by TikTok's parent company in November 2017)[289] agreed to pay a penalty of USD5.7 million to the FTC for allegedly breaching the Children's Online Privacy Protection Act by collecting information from children without parental consent.[290] In its complaint, the FTC noted that 'a significant percentage'[291] of users are children under 13. As part of its settlement, TikTok was directed to comply with the *Children's Online Privacy Protection Act*, including by deleting personal information it had collected from users aged under 13.[292] However, in May 2020, several US children and consumer groups lodged a complaint with the FTC, alleging that TikTok's treatment of children's data continues to violate the *Children's Online Privacy*

---

284 Further information is provided at appendix D.
285 ACCC, DPI Final Report, 26 July 2019, pp. 442–448.
286 FTC, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, 4 September 2019, accessed 22 September 2020.
287 FTC, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, 4 September 2019, accessed 22 September 2020.
288 FTC and People of the State of New York v Google LLC and YouTube LLC, Complaint for civil penalties, permanent injunction and other equitable relief, 4 September 2019.
289 D Lee, 'The popular Musical.ly app has been rebranded as TikTok', *The Verge,* 2 August 2018, accessed 22 September 2020.
290 FTC, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law, 27 February 2019, accessed 22 September 2020; United States of America v Musical.ly, Complaint for civil penalties, permanent injunction, and other equitable relief, 27 February 2019.
291 United States of America v Musical.ly, Complaint for civil penalties, permanent injunction, and other equitable relief, 27 February 2019, at [19].
292 United States of America v Musical.ly, Complaint for civil penalties, permanent injunction, and other equitable relief, 27 February 2019, at [24].

*Protection Act* and the 2019 FTC order.[293] TikTok is currently subject to several investigations by overseas regulators that relate to its alleged treatment of children's data, including the Dutch Data Protection Authority[294] and the European Data Protection Board's forthcoming taskforce.[295]

## 4.2. Harms through scams and malicious targeting on platforms

- **Consumers are continuing to experience harms in the use of platforms. Scam reports involving online private messaging, social media and search services are increasing and resulted in losses of $38.5 million in 2019, compared to $23.5 million in 2018. The ACCC notes that these scam reports and reported losses considerably understate the extent to which harms are occurring, with only 13 per cent of people losing money or personal information in a scam reporting the event to Scamwatch.[296]**
- **The ACCC considers that all platforms should do more to remove scam activity on their platforms and provide redress to consumers, where appropriate.**

The ACCC has found scam reports involving online private messaging, social media and search services are steadily increasing and are resulting in significant losses to consumers. Based on complaints received by the ACCC through Scamwatch, scams involving these platforms resulted in reported losses of over $23.5 million in 2018 and this increased to $38.5 million in 2019.[297] As at 30 June 2020, reported losses from scams on these platforms totalled $25.5 million—compared to almost $15 million in the same period in 2019.[298]

The number of scams reported by consumers involving online private messaging, social media and search services have increased by almost 32 per cent from 2018 to 2019.[299] In 2018, the ACCC received 14 060 reports of scams from consumers involving these platforms and this increased by 4434 reports to 18 494 in 2019.[300] The ACCC notes that on average, the number of scams that involve at least one online private messaging service have experienced the biggest increase. For example, online private messaging scams reported by consumers increased by almost 95 per cent in the first half of 2020 compared to the first half of 2018, which may be due to the increased uptake of these services during COVID-19.[301]

---

293 Electronic Privacy Information Center, Groups Tell FTC to Investigate TikTok's Failure to Protect Children's Privacy, 14 May 2020, accessed 22 September 2020; Campaign for a Commercial-Free Childhood et al, Complaint and Request for Investigation of TikTok for Violations of the Children's Online Privacy Protection Act and Implementing Rule, 14 May 2020.

294 Dutch Data Protection Authority (Autoriteit Persoonsgegevns), Dutch Data Protection Authority to investigate TikTok, 8 May 2020.

295 European Data Protection Board, Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB, 10 June 2020.

296 ACCC, Targeting Scams Report 2019, 22 June 2020, p. i.

297 These figures are based on self-reported data provided to the ACCC through the Scamwatch website, during 2018 and 2019.The figures include all scams reported during this period by consumers, businesses and unspecified reports that involve at least one platform providing social media, search, online private messaging or dating app services.

298 These figures are based on self-reported data provided to the ACCC through the Scamwatch website during the first half of 2019 and the first half of 2020.The figures include all scams reported during this period by consumers, businesses and unspecified reports that involve at least one platform providing social media, search, online private messaging or dating app services.

299 These figures (nominal) are based on self-reported data provided to the ACCC through the Scamwatch website, during 2018 and 2019. The figures include all scams reported during this period by consumers, businesses and unspecified reports that involve at least one platform providing social media, search, online private messaging or dating app services.

300 These figures (nominal) are based on self-reported data provided to the ACCC through the Scamwatch website, during 2018 and 2019. The figures include all scams reported during this period by consumers, businesses and unspecified reports that involve at least one platform providing social media, search, online private messaging or dating app services.

301 The percentage change is calculated using self-reported data provided to the ACCC through the Scamwatch website, between the first half of 2018 against the first half of 2020. The calculation compares the number of all scams reported during the period by consumers that involve at least one platform providing online private messaging services. Scams sometimes take place across multiple platforms, and therefore this data may include scams that also involved digital platforms providing services other than online private messaging.

Consumer losses involving scams on online private messaging, social media and search services have also increased by 64 per cent from 2018 to 2019. Consumers reported losses of $23 558 800 in 2018 and this increased to $38 571 210 in 2019.[302] The ACCC notes that over this period, consumers' average loss has increased by 24 per cent.

The ACCC notes that these figures considerably understate the extent to which scams are occurring on platforms and the losses that are incurred by consumers. Scams are underreported, with only 13 per cent of individuals who have lost money or personal information in a scam reporting the event to Scamwatch.[303]

Since the release of the DPI Final Report, the ACCC observes that celebrity endorsement scams, which are hosted on social media platforms, continue to be common. As noted in the *Targeting Scams Report 2019*, many celebrity endorsement scams occur on social media platforms including Facebook and in 2019, Scamwatch received over 400 reports about celebrity endorsement scams with over $1 million in losses.[304] Celebrity endorsement scams include false advertisements featuring Australian mining business owner Andrew Forrest, chef Maggie Beer and the television show 'Shark Tank'.[305]

The ACCC has also observed a significant increase in the number of investment scams reported between 2018 and 2019, and associated losses. This increase is particularly prominent on online private messaging services, where the number of reported investment scams almost tripled across the period, and average consumer losses increased by more than 200 per cent to over $22 000 per scam.

The ACCC has observed a trend of dating and romance scams increasingly leading to investment scams. This type of scam has been observed across many online private messaging services and social media platforms including WhatsApp and Facebook, and in some cases can lead to significant losses. For example, one victim reported a loss exceeding $675 000 as a result of this type of scam.

Outlined below is an overview of some of the key scams observed by the ACCC through reports received through Scamwatch.

### 4.2.1. Scams on platforms providing online private messaging services

In 2019, the ACCC received over 4000 reports of scams occurring on online private messaging services.[306] The most prevalent types of scams occurring on online private messaging services are dating and romance scams; attempts to gain personal information; and buying or selling scams. While some scams are initiated on online private messaging services, other scams are initiated elsewhere (such as social media platforms or via email) but can then be moved to online private messaging platforms to avoid detection.

The ACCC received almost 1000 reports of dating and romance scams on online private messaging services, and over 800 involving attempts to gain personal information. The ACCC also understands that an increasing number of younger people are reporting scams occurring on Discord, and that these scams typically involve gaming and technology such as cryptocurrency.[307]

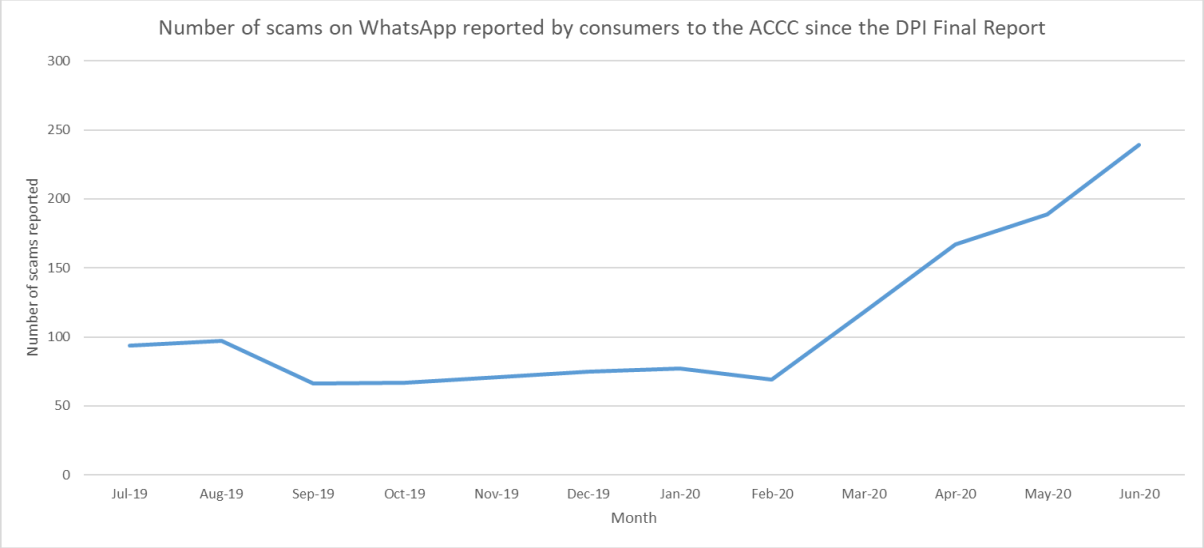
Across online private messaging services, the ACCC received the most reports about scams involving WhatsApp and Facebook Messenger in 2019. Reports involving scams on

---

302 These figures (nominal) are based on self-reported data provided to the ACCC through the Scamwatch website, during 2018 and 2019. The figures include all scams reported during this period by consumers, businesses and unspecified reports that involve at least one platform providing social media, search, online private messaging or dating app services.
303 ACCC, Targeting Scams Report 2019, 22 June 2020, p. i.
304 ACCC, Targeting Scams Report 2019, 22 June 2020, p. 5.
305 ACCC, Targeting Scams Report 2019, 22 June 2020, p. 5.
306 ACCC analysis. We note that scams may be reported as occurring on multiple platforms, and this figure reflects scams which involved at least one online private messaging service.
307 ACCC, Targeting Scams Report 2019, 22 June 2020, p. 18.

WhatsApp have increased since 2018, and in particular, there has been a significant increase in reports since COVID-19, as seen in figure 4.3 below.[308]

**Figure 4.3: Number of reports reported by consumers regarding scams involving WhatsApp from July 2019 to June 2020**




Source: ACCC analysis. Based on self-reported data provided to the ACCC through the Scamwatch website, between 1 July 2019 and 30 June 2020 involving all scams reported by consumers during this period that involved WhatsApp.

Box 4.7 below is an example of a typical dating and romance scam which was hosted on an online private messaging platform.

**Box 4.7: Case study—Dating and romance scams on Facebook and WhatsApp resulting in a loss exceeding $5000**

The following is an anonymised complaint to Scamwatch:

> *He added me on FB [Facebook] in Feb and persuaded me to add him on WhatsApp to talk. He said he came to Australia not long ago to work as a pilot. He said hi often and sent photos at work or taken in Sydney of him (fake pilot) after gaining my trust… I saw him as a real friend. He started scamming me for money in the middle of April. He made up a certificate document and email, text messages, Facebook market selling information to show me that he was really working hard to solve the financial difficulty and that's why he needed my help so much and even begged miserably. I helped him but in the end was told by the police it was a big scam and the Facebook account was stolen. I searched images and found out all photos sent by him belonged to "Captain Joe".*
>
> *I lost 6k… because of the scammer. I reported to the local police and the bank in April but no updates so far just let me wait. Apparently the amount I lost was not big enough to gain their attention. I reported on Facebook platform, nothing happened either. He is still using that fake pilot account. I reported on the WhatsApp platform. I guess his WhatsApp number got banned but mine did too, probably because he used multiple accounts to complain and got mine banned too. Anyway, he got a new WhatsApp account…still harming other … girls. I know that thanks to one of his new FB friends I contacted.*

As noted in the *Targeting Scams Report 2019*, reported losses from scams involving cryptocurrency have been increasing significantly, and commonly involve victims being targeted on online private messaging services such as Discord and Telegram.[309] Box 4.8

---

[308] Note that some scams take place across multiple platforms, and therefore the scams represented in figure 4.3 may have involved other digital platforms in addition to WhatsApp.

[309] ACCC, Targeting Scams Report 2019, 22 June 2020, p.18.

below provides an example of cryptocurrency scams which occurred on an online private messaging service.

**Box 4.8: Case study—Cryptocurrency scams occurring on an online private messaging platform**

The following are anonymised complaints to Scamwatch involving cryptocurrency scams on an online private messaging platform:

- *'Website appeared to be an investment website operating a bitcoin mining farm in the Ukraine but registered in Australia…promising that investments would be made back in approximately one month. This worked for two or three months, people would receive earnings from the bitcoin mining operation every day. And they were able to transfer these earning to a bitcoin wallet on other external websites. But on July 15th, it became clear that this was an exit scam. On that day it was not possible anymore to withdraw earnings anymore. Shortly after [redacted] (official communication channel linked to on the website) was deleted.' This scam resulted in a reported loss exceeding $140,000.*
- *'[Redacted] claimed to be a cryptocurrency mining and trading company that sells mining contracts. I purchased contracts from them and paid using cryptocurrency in an amount of AUD 98 600 starting May 15 2019. On the date of July 15 2019 the website and support groups in different online social media [redacted] disappeared and was showing "hacked" while no contact from the company could be established and it seems very obviously that they scammed their customers including me.' This scam resulted in a reported loss exceeding $95,000.*

### 4.2.2. Scams on platforms providing search services

In relation to platforms providing search services, the ACCC received almost 4000 reports of scams in 2019. Scams involving buying or selling scams on platforms providing search services comprised approximately 1100 reports and almost 1000 scams were reported relating to attempts to gain personal information.

### 4.2.3. Scams on social media platforms

In relation to social media platforms, the ACCC received over 12 000 reports in 2019. The most common types of scams occurring on social media platforms included buying or selling scams, dating and romance scams and attempts to receive personal information.

The ACCC notes that there are some ongoing scams which continue to be hosted on platforms such as Facebook, despite reports by consumers and the media, as discussed in box 4.9 below.

**Box 4.9: Example of ongoing scams hosted on social media platforms—Facebook lottery and Instagram forex scams**

**Facebook lottery scams**

There are some scams on social media platforms which continue to be reported by consumers over an extended period of time. For example, 'Facebook lotto' frauds have been reported by consumers and in the media since at least 2011 and continue to be one of the main ways that scammers monetise compromised Facebook accounts.[310]

The 'Facebook lotto' fraud has been reported in Australia, as well as overseas. In 2018, the ABC reported that the 'Facebook lotto' fraud which promised $7.5 million in prize money scammed

[310] ACCC, Targeting Scams: Report of the ACCC on scam activity 2011, 19 March 2012, p. 10.

nearly 30 Queensland residents, with one scam victim reporting a loss of over $100 000.[311] US and Canadian media outlets have also reported on the prevalence of Facebook lotto scams.[312]

**Instagram investment scams**

Since October 2018, fraudulent investment schemes have been advertised on Instagram in Australia and overseas. This scam involves scammers advertising 'get rich quick' investment schemes on Instagram.[313] The ACCC's Scamwatch and UK regulator Action Fraud have received reports of these investment scams, with Action Fraud reporting that it received over 350 reports between October 2018 and February 2019. [314] To date, the ACCC is unaware of any action taken by Facebook (which owns Instagram) to take measures to remove this scam activity. While broad advice on scams can be found on Instagram's help page, it is unlikely that victims would read this prior to suffering losses.[315]

### 4.2.4. More action should be taken by all platforms to remove scams

Recent research has found that 64 per cent of adult Australians consider exposure to scams or fraud to be the top risk of harm online.[316] In addition, the eSafety Commissioner found that while 75 per cent of those surveyed considered that technology companies have a responsibility for people's online safety, only 23 per cent consider that companies are doing enough to include safety features into their services and products.[317]

The ACCC recognises that platforms have taken some action to address scam activity on their platforms. However, the ACCC considers that all platforms should continue to do more to remove scams, and to provide redress, where appropriate, for consumers. This is particularly acute where the type of scams, such as those noted above, have been ongoing methods of malicious activity across many years, with ongoing media attention and reporting by consumers and regulators. As noted in box 4.10 below, the ongoing nature of scams on platforms supports the DPI Final Report's recommendations 22 and 23.

311 P Williams, 'Facebook lottery' promising $7.5 million prize scams Australians out of hundreds of thousands', *ABC*, 3 May 2018, accessed 22 September 2020.
312 J Nicas, 'How Fake Mark Zuckerbergs Scam Facebook Users Out of Their Cash', *The New York Times,* 25 April 2018, accessed 22 September 2020; K DeClerq, 'Toronto woman targeted by fake Facebook lottery scam', *CTV News*, 21 November 2018, accessed 22 September 2020.
313 Action Fraud, Instasham: Fraudulent investments being advertised on social media, 25 February 2019, accessed 22 September 2020.
314 Action Fraud, Instasham: Fraudulent investments being advertised on social media, 25 February 2019, accessed 22 September 2020.
315 Instagram, How do I avoid scams on Instagram?, accessed 22 September 2020.
316 eSafety Commissioner, Building Australian adult's confidence and resilience online, September 2020, p. 5.
317 eSafety Commissioner, Building Australian adult's confidence and resilience online, September 2020, p. 7.

**Box 4.10: Recommendations in the DPI Final Report for platforms to comply with internal dispute resolution and the establishment of an ombudsman scheme**

The ACCC remains of the view that effective dispute resolution mechanisms are needed to address complaints and disputes to platforms (recommendation 22) and that the establishment of an ombudsman scheme to resolve complaints and disputes, including in relation to scam content (recommendation 23), is required to address scam activity on platforms.

## 4.3. Increased prominence of non-organic search results, including sponsored results, at the expense of organic search results

- **ACCC research suggests that on Google Search, consumers are more likely to be shown a sponsored result (that is, an advertisement) as the first item, in response to a product search on a mobile device than on a desktop device. Research by the UK's CMA also suggests that organic results on a mobile device are much less prominent on a desktop. This is significant as almost half the visits to Google.com and Google.com.au by Australian consumers are now from mobile devices and consumers often focus their attention on the highest ranking search results.**
- **Overseas research also suggests that more generally, non-organic search results (including sponsored results) appear to be making up an increasing proportion of overall search results at the expense of organic search results.**
- **These reported shifts in the balance of sponsored and organic posts are important as this can affect both the quality of services provided to consumers and the opportunities for small businesses to reach customers online.**

The way in which information and advertising is displayed in response to search queries on search engine results pages can have wide-ranging impacts on both consumers and businesses. This has resulted in increased scrutiny on how search results and search advertising are presented and calls for greater transparency by search engines.[318]

As discussed in appendix B, Google occupies a substantial share of the market for general search services, with a market share of 95 per cent in Australia, and faces limited competitive constraints by other search service providers. Consequently, this analysis focuses on Google and its role as gatekeeper between consumers seeking information on goods and services, and businesses offering or advertising those goods and services online. Google performs this role in at least three broad ways:

- The provision of a set of hyperlinks on Google's search engine results page, considered by Google's algorithm as responsive to a user search query. These results are known as organic results.
- Advertising shown on Google's search engine results page, in the form of 'sponsored results' (that is, advertisements).
- Outside of 'standard' organic results and sponsored results, Google also provides users with a number of different answers considered responsive to a user's search query, which varies depending on the search query and the information sought. These include:
    - **OneBoxes**[319], which is a separate display box within Google search results that allows Google to include results from its other search products (e.g. carousel from Google Shopping or nearby locations from Google Maps) within its standard Google search. Users may see the weather, news result or flight details. Sometimes OneBoxes will also provide direct answers to search queries (e.g. if searching for

[318] See, for example, Competition and Markets Authority, Online platforms and digital advertising market study final report, July 2020, pp. 16–17; K Grind et al, 'How Google interferes with its search algorithms and changes your results', *Wall Street Journal,* 15 November 2019, accessed 22 September 2020; A Jeffries and L Yin, 'Google's top search result? Surprise! It's Google', *The Markup*, 28 July 2020, accessed 22 September 2020.

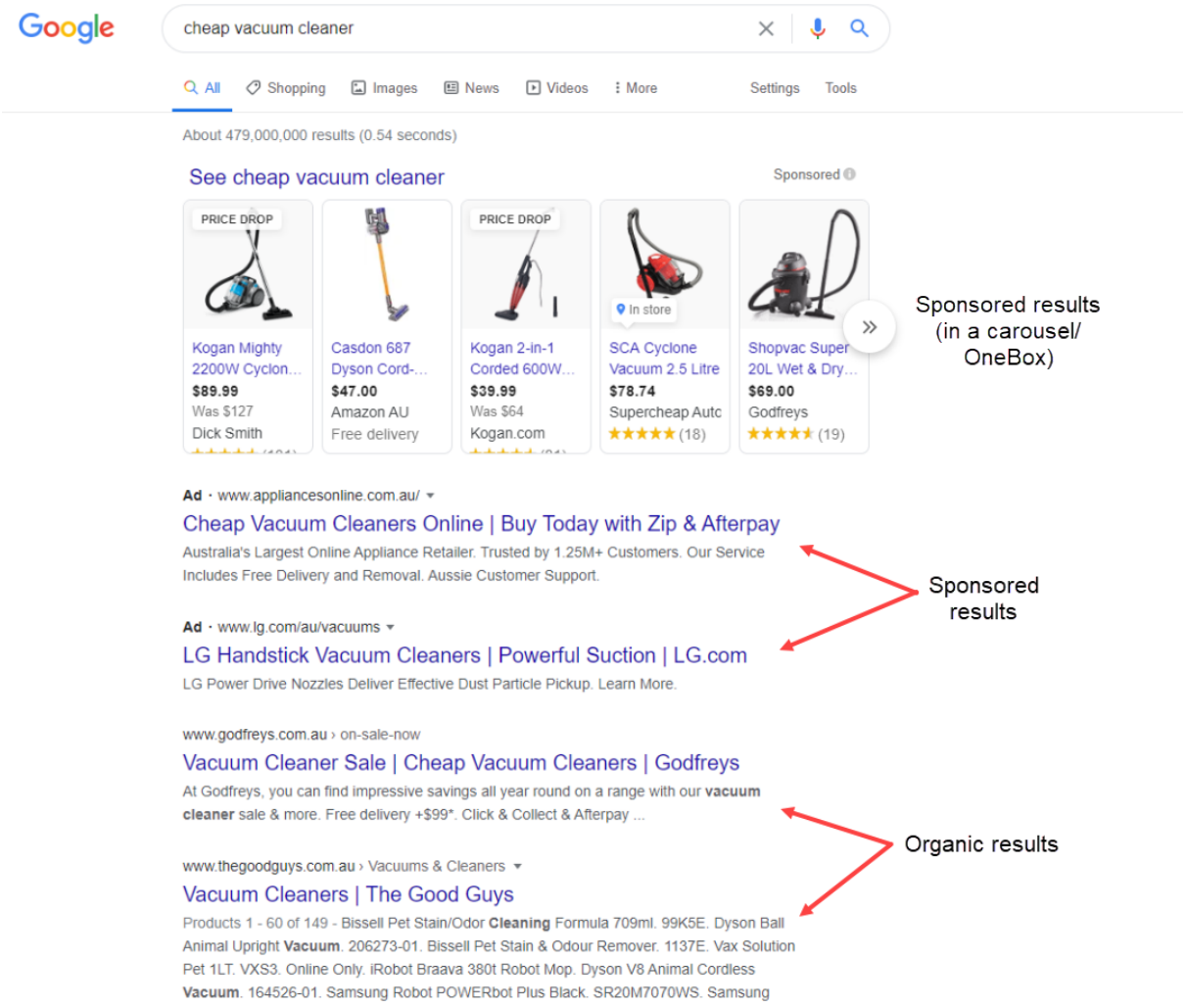
[319] A OneBox is a separate display box within Google search results that allows Google to include results from its other search products (e.g. carousel from Google Shopping or nearby locations from Google Maps) within its standard Google search. Users may see the weather, news result or flight details. Sometimes OneBoxes will also provide direct answers to search queries (e.g. if searching for 'When is Christmas Day?' users may get December 25 in a box at the top of their search results). OneBoxes may sometimes feature sponsored results.

'When is Christmas Day?' users may get December 25 in a box at the top of their search results). OneBoxes may also sometimes feature sponsored results.

- **Featured snippets**, which provide 'quick answers to questions by drawing attention to programmatically generated snippets from websites that… [Google's] algorithms deem relevant to the specific question being asked', [320] and
- **Answers from the Knowledge Graph**, which contain answers from a 'database of more than one billion real-world people, places and things'.[321]

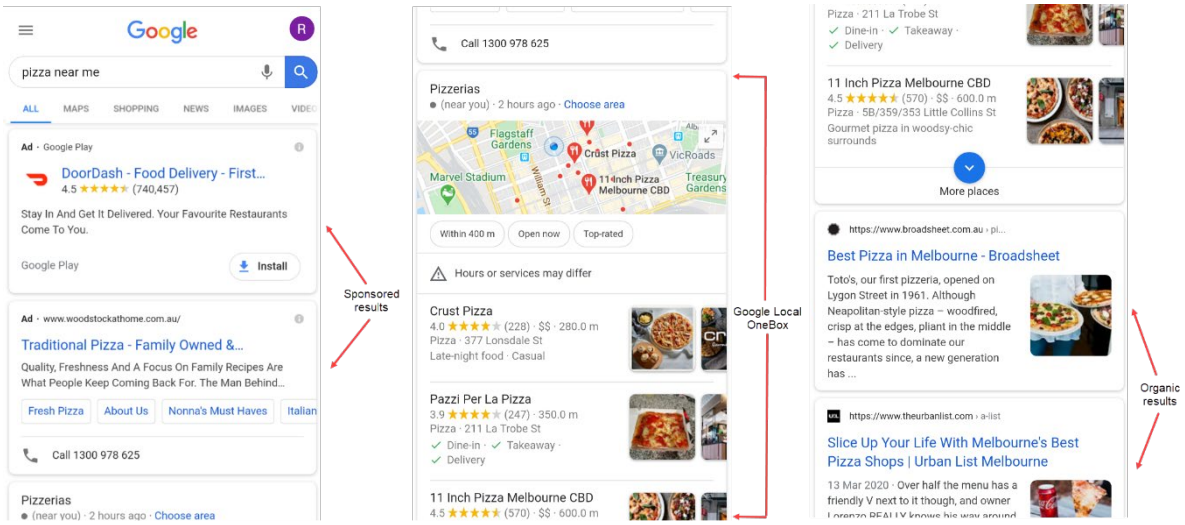
These results can be structured in a number of ways and how and where on a search engine results page the results are presented may be influenced by variables beyond the search query, such as the user's location, device type (phone, tablet or desktop) and browser used. Figure 4.4 and figure 4.5 below demonstrate the different types of information presented to user search queries on a desktop and a mobile device.

**Figure 4.4: Desktop search for 'cheap vacuum cleaner'[322]**




320 Google, How search works: useful responses, accessed 22 September 2020.
321 Google, How search works: useful responses, accessed 22 September 2020.
322 Search conducted on 6 June 2020, on a Chrome browser on a Windows laptop by a user located in Melbourne.

**Figure 4.5: Mobile search for 'pizza near me'[323]**




Websites have an incentive to be positioned as highly as possible in a search engine results page as the higher a website appears on a page, the more traffic it is likely to receive. For example, research of search browsing habits noted that 47 per cent of viewing time on search engine results page was spent on the top 20 per cent of the page, and more than 75 per cent of viewing time was spent on the top 40 per cent of the page.[324]

Research has also shown that for search engine results page featuring only organic listings, 76 per cent of page clicks were to the top four organic listings, and when the search engine results page featured additional non-organic results such as sponsored or universal search results, clicks to the top four organic listings fell from 76 per cent to 60 per cent.[325]

The ACCC has sought to examine how search results are currently presented to users and in particular, whether there are any differences in how search results are displayed on mobile devices, compared to desktops, given that almost half of all visits to Google.com and Google.com.au are now on mobile devices.[326] The ACCC undertook an analysis over one month to examine the results of multiple Google searches across devices and location within Australia. The results of the ACCC's analysis is set out in box 4.11 below.

**Box 4.11: Case study—user queries on Google Search**

Every day between 6 June 2020 and 6 July 2020, the ACCC ran 4 search queries on Google Search, using a Windows PC, a MacBook, an Android Emulator and an iOS Simulator. This ran 8 search queries across 4 different devices, 3-4 different browsers (depending on the device) for three different profiles (a signed in user, a signed out user and a guest user) across two locations (Melbourne and Ballarat) by means of location spoofing.[327] The search queries were 'cheap vacuum cleaner', 'pizza near me', 'accommodation in Melbourne/Ballarat'.

Based on the results of the case study, the ACCC has made the following observations:

---

323 Search conducted on 6 June 2020, on a Chrome browser on a device emulating an Apple iPhone by a user located in Melbourne.

324 T Fessenden, Scrolling and Attention, Nielsen Norman Group, 15 April 2018, accessed 22 September 2020.

325 Mediative, The evolution of Google search results pages and their effect on user behaviour, September 2014, pp. 40-41.

326 Estimates indicate that from February 2020 to July 2020, around 47 per cent of visits of Australian users to Google.com were on mobile, and around 45 per cent of visits of Australian users to Google.com.au were on mobile. SimilarWeb Website Analysis, Traffic and Engagement Metrics, for http://www.google.com and http://www.google.com.au, for the period from February 2020 to July 2020 in Australia. Please note that SimilarWeb's data provides estimated traffic and usage data for websites and mobile apps. More information about SimilarWeb's methodology can be found at: https://www.similarweb.com/corp/ourdata/.

327 'Location spoofing' occurs is the overriding of the geolocation supplied by the device/browser to the search engine.

- Most of the search results pages for the queries tested had a OneBox presented above organic results (90 per cent of searches for 'pizza near me', 87 per cent for 'cheap vacuum cleaner' and 50 per cent for 'accommodation in Melbourne/Ballarat').
- Many searches for 'cheap vacuum cleaner' resulted in a sponsored result above OneBoxes and organic results across all locations and devices (82 per cent). This falls to 52 per cent for 'accommodation in Ballarat/Melbourne' and 18 per cent for 'pizza near me'.
- Mobile devices typically had a higher proportion of sponsored results as the first result on a search engine results page than desktop devices (i.e. they were more likely to have a sponsored result as a search result). For example, for the 'cheap vacuum cleaner' query, 91 per cent of results pages had a sponsored result as a first result on mobile, compared to 63 per cent on desktop; similarly, for the 'accommodation in Melbourne/Ballarat' search, 59 per cent of results pages had a sponsored result as a first result on mobile, compared to 37 per cent on desktop.
- For searches run on mobile devices, 54 per cent of 'cheap vacuum cleaner' query results led to a search engine results page consisting entirely of sponsored results in the first screen, requiring users to scroll through to access organic results. For the other queries, generally less than half the first screen was taken up by these results.

The results relating to online shopping may be particularly pertinent, given the high proportion of online shopping that occurs on mobile devices relative to desktops devices. For example, PayPal reported that 41 per cent of consumers preferred online shopping on mobile devices, compared to desktop devices (including laptops) with the figure rising to 54 per cent for consumers aged between 18 and 34 years.[328]

The CMA considered this issue in its 2017 report into online search and consumer behaviour and conducted a similar analysis of search results for the term 'pizza' on a mobile device and a desktop device. The CMA noted found that based on its analysis, organic results on a mobile device were much less prominent than on a desktop, and appeared only after a consumer scrolls through at least two screens.[329] The CMA noted that this may have important consequences for consumer behaviour and firms' online strategies. The CMA also found that:

> *[C]onsumers mostly focus their attention on the highest-ranking search results, especially on the top 3 or 4 results. Therefore a new entrant may find it necessary to be ranked in the very top positions to get the level of website traffic needed to expand its operations successfully.*[330]

This is even more pronounced on mobile devices, and given increasing usage of mobile devices for online shopping, this may be a more significant issue for new entrants into online shopping in the future.[331]

In this way, the proportion of results which are sponsored, relative to organic results, can impact small businesses seeking to reach those consumers online. Businesses typically have two options—either to engage in search engine optimisation to rank higher in organic results, or to bid for sponsored search results (potentially spending more of their budget on advertising than they otherwise would).[332] Research suggests that businesses are increasingly using sponsored results as a means of attracting web traffic; as Kraemer and Zierke explain:

> *the role of sponsored rankings has become increasingly important in recent years, as organic search results were moved further and further down the results lists.*

---

328 PayPal, PayPal mCommerce Index 2019, October 2019, p. 6.
329 Competition and Markets Authority, Online Search: Consumer and Firm Behaviour, 7 April 2017, p. 24.
330 Competition and Markets Authority, Online Search: Consumer and Firm Behaviour, 7 April 2017, p. 86.
331 Competition and Markets Authority, Online Search: Consumer and Firm Behaviour, 7 April 2017, p. 86.
332 Competition and Markets Authority, Online Search: Consumer and Firm Behaviour, 7 April 2017, p. 16–17.

> *Especially on mobile devices with limited screen size, often the first page of the search results list is completely occupied by sponsored search results.*[333]

Relatedly, in its submission to the CMA's market study into online platforms and digital advertising, Google recognised that the position and characteristics of ads on Google Search, both on mobile and desktop, have changed significantly over the past 10 years from 2011 to 2020.[334] The CMA noted that some of these changes 'illustrate that Google is able to generate significant additional revenue through apparently minor changes to presentation that have a significant effect on click-through rates'.[335] The CMA also noted submissions made by specialised search providers that changes to the presentation of ads and Google's search results pages have affected their business.[336]

There has been public commentary on the changes to the way in which Google presents ads on Google Search, with some noting the difficulty in differentiating between a sponsored result and an organic result.[337] For example, the CMA noted that:

> *Several advertisers, including both specialised search providers and other advertisers, submitted to us that recent changes to Google's policies on ad load and the presentation of search advertising had the effect of increasing the propensity for users to click on ads. This resulted in the crowding out organic traffic and an increase in the overall cost of accessing user traffic. Most advertisers submitted that the effects were particularly pronounced in mobile.*[338]

The image below demonstrates the changes to the way Google shows ads on Google Search, from 2013 to 2019.

---

333 J Kraemer and O Zierke, Paying for Prominence: The Effect of Sponsored Rankings on the Incentives to Invest in the Quality of Free Content on Dominant Online Platforms, 24 April 2020, p. 2.

334 Competition and Markets Authority, Appendix Q to Online platforms and digital advertising market study final report, July 2020, p. Q20.

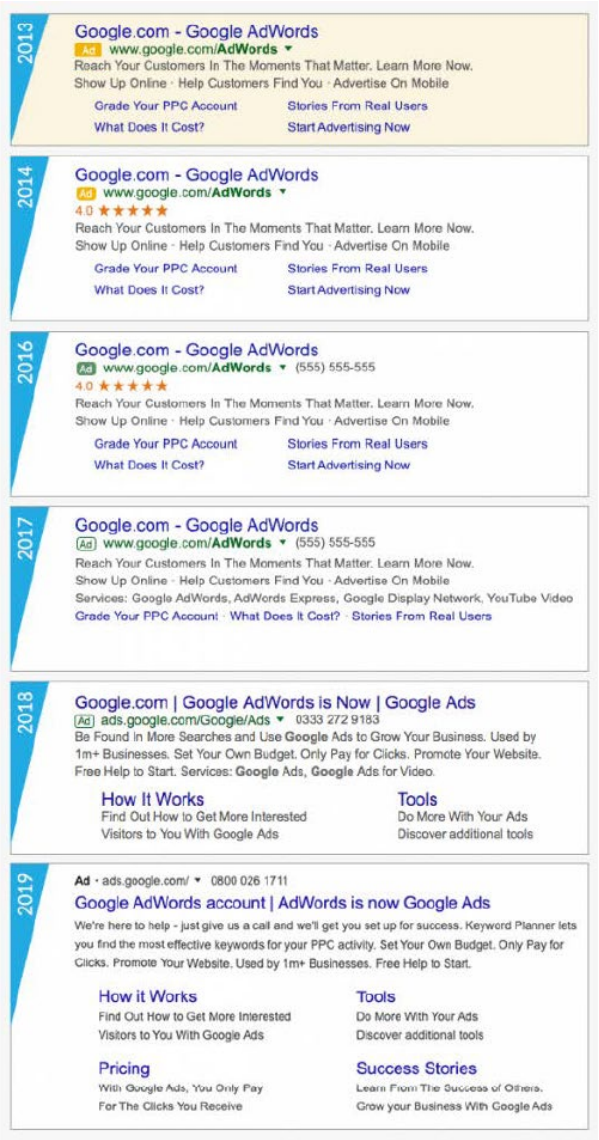
335 Competition and Markets Authority, Appendix Q to Online platforms and digital advertising market study final report, July 2020, p. Q21.

336 Competition and Markets Authority, Appendix Q to Online platforms and digital advertising market study final report, July 2020, pp. Q22-Q23.

337 See, for example, J Porter, Google's ads just look like search results now, *The Verge*, 23 January 2020, accessed 24 August 2020; N Lomas, Google's latest user-hostile design change makes ads and search results look identical, *TechCrunch*, 23 January 2020, accessed 24 August 2020; D Ting, Google's latest search results change further blurs what's an ad, *DigiDay*, 23 January 2020, accessed 24 August 2020.

338 Competition and Markets Authority, Appendix Q to Online platforms and digital advertising market study final report, July 2020, p. Q21.

**Figure 4.6: Illustration of changes to the presentation of ads on Google Search over time**




Source: Competition and Markets Authority, Appendix Q to Online platforms and digital advertising market study final report, July 2020, p. Q21.

As a result, for businesses reliant on reaching customers on Google Search, the changes in the proportion of organic to sponsored search results may have the effect of businesses spending a larger proportion of their advertising budget on sponsored results and/or search engine optimisation services. The impact of this increase in expenditure could harm small businesses that would otherwise use that budget for other purposes, potentially reducing their competitiveness.

This increased expenditure by businesses on advertising could also result in consumer harm. The CMA report noted a number of specialised search providers have indicated that traffic has shifted from organic to paid results, particularly on mobile where space available is much more limited than desktop. The CMA concluded that this could harm consumers by way of increased costs to specialised search providers as they spend more on search advertising rather than relying on organic results, which would ultimately be passed onto consumers in the form of higher prices.[339] The same concerns exist in relation to other

[339] Competition and Markets Authority, Appendix P to Online platforms and digital advertising market study final report, p. 44.

businesses using search advertising as well as the specialised search providers considered by the CMA.

The exposure of consumers to fewer organic results on mobile search may also arguably reduce the level of choice directly made available to consumers. As noted by Burquet, Caminal and Ellman (2014), 'as with any two-sided platform that only charges one side, it is motivated to favour that side's interest. So it is no surprise that an ad-funded engine might encourage consumers to visit the merchants most willing to pay for sponsored ads, even when not ideal for consumers.'[340]

[340] R Burguet et al, In Google we trust?, November 2014, p. 1.

# 5. Platforms and small business

This chapter examines the relationship between large platforms supplying online private messaging, social media and search services and small businesses that utilise the advertising and other business services of these platforms. This chapter is structured as follows:

- **Section 5.1** discusses the benefits that platforms have brought to small businesses, particularly in the supply of online advertising opportunities.
- **Section 5.2** provides a summary of the ACCC's analysis of the platform to business terms of service arrangements of selected search, social media and online private messaging platforms from 2017 to 2020.
- **Section 5.3** discusses the effect of potentially unfair platform to business terms on small businesses.

## 5.1. Benefits of platforms supplying online private messaging, social media and search services to small businesses

- **Small businesses are increasingly reliant on platforms as a means of advertising to, and communicating with consumers and potential customers.**

Advertising is a key way through which small businesses utilise platforms' services. The ACCC recognises that digital platforms, and their supply of online advertising services, provide businesses with numerous and significant benefits.[341] These include the ability to target consumers, increasing the efficiency and effectiveness of advertising and advertisers' return on investment, access to a broader audience and the ease and low cost of access to advertising services.

As a consequence, small businesses are becoming increasingly reliant on large platforms to reach customers. The Australian Small Business and Family Enterprise Ombudsman submitted to the Ad Tech Inquiry that:

> *…the size and reach of technology companies such as Facebook and Google allows businesses to reach larger and more targeted audiences. That size and reach however, creates near-monopoly status for Facebook and Google, leaving advertising businesses no similarly sized alternative options should the advertiser-publisher relationship deteriorate).*[342]

Facebook has previously acknowledged the reliance of business, and in particular, small businesses, on Facebook in Australia, stating that:

> *…more than 350,000 businesses placing advertisements on Facebook spent less than USD $100 in 2017. In the same year, fewer than 150 Australian businesses spent more than USD $1 million to place advertisements on Facebook. More than half of all Australian [small to medium businesses (SMBs)] have a Facebook Page. An estimated 8.2 million Australians have purchased from, or visited an SMB after seeing content relevant to the business on Facebook.*

---

341 ACCC, DPI Final Report, 26 July 2019, p. 131.

342 Australian Small Business and Family Enterprise Ombudsman, Submission to the ACCC Digital Advertising Services Inquiry, 16 April 2020, p. 1.

*Approximately 210 million people from around the world are connected on Facebook to an Australian business.*[343]

As discussed in section 4.3 of chapter 4, a growing proportion of search results on Google Search consist of sponsored results (i.e. advertisements). As a result, businesses traditionally reliant on organic search result may need to spend more of their advertising expenditure on search advertising to reach the same audience.

Google and Facebook are increasingly performing 'gatekeeper' roles; as shown in figure 1.5 of chapter 1, Google and Facebook each have a reach of over 80 per cent of Australians aged over 13 years, who visit Google and Facebook owned services multiple times a day.

## 5.2. Platform and small business relationships

- **While platforms have brought wide-ranging benefits to businesses, the imbalance of bargaining power, reflected in the terms and conditions applicable to business users with large platforms, can have negative impacts. The ACCC has identified some contract terms that are potentially unfair.**

To better understand the relationship between large platforms and small businesses, the ACCC reviewed the platform to business terms of service agreements of selected search, social media and online private messaging platforms from 2017 to 2020, including their terms of service/use, privacy policies and policies and contracts related to use of advertising services.[344]

The terms of service considered by the ACCC are standard terms governing the supply of advertising services by large platforms (particularly terms related to self-service advertising), which, as default terms, are more likely to be utilised by small businesses rather than larger businesses that may negotiate their own arrangements with platforms. However, this does not preclude the ACCC's analysis from applying to larger businesses, particularly given the significant reach of large platforms and the limited substitutes available that offer similar reach and targeting capabilities.

The ACCC's review found potentially unfair terms across the platforms examined, which (when viewed in light of the market positions of some of these platforms) may harm businesses, particularly small businesses, seeking to advertise on these platforms using their standard terms. In particular, the ACCC's analysis identified the prevalence of a number of potentially unfair clauses, including:

- *A broad unilateral discretion for the platform to remove or block advertising or other content for any reason*—in many terms, the platforms have an unqualified discretion in respect of decisions to remove content, suspend services or terminate accounts. This could have a significant impact on businesses reliant on producing content for or on platforms. Such a discretion may be reasonably necessary to protect the legitimate interests of the platforms, where such content may be illegal and/or inappropriate. However, there may be cases where the removal of such content is not justified.
- *A broad unilateral discretion for the platform to suspend or terminate the user's account or ad campaign for any reason*—this may have a significant impact on users where the

---

343 Facebook, Response to the ACCC's Preliminary Report by Facebook Australia Pty Limited, 3 March 2019, p. 20.

344 Between April and June 2020, the ACCC reviewed platforms: Amazon, Bing, DuckDuckGo, Expedia, Facebook, Google, Instagram, Snapchat, Twitter, WhatsApp and YouTube. The focus of the review was standard platform-to-business contracts (such as self-serve advertising) which are generally available on set up of a self-service advertising account (usually available through a click-wrap agreement) for small business advertisers. Larger businesses with more complex needs and/or higher advertising spend may have detailed and/or bespoke contracts and have specific contact points within major digital platforms.

platform decides to terminate the user's account and prohibits them from using the service.

- *The ability for the platform to vary terms without notice or with only a short notice period*—this includes instances where the agreement either specifies that no notice is required, notification methods are broad or unspecified, or changes come into effect soon or immediately after notification. This may be particularly harmful to businesses reliant on the platform for advertising, as they would have no option but to cease advertising altogether, or to continue using the services until they are able to find alternative advertising.
- *Prohibitive dispute resolution processes*—this includes dispute resolution clauses that require claims to be made in the US or via international arbitration, or would be otherwise prohibitive to small businesses, such as limitations on class actions. The dispute resolution processes provide users with little scope for recourse. Any available internal dispute resolution processes are often not clearly specified in the terms, and litigation or arbitration is highly unlikely to be a viable alternative for small businesses, with many terms stipulating that any claims are to be made in courts overseas and extensively limiting the liability of platforms.
- *Confidentiality or publicity limitations*—this includes prohibitions on users making public statements about the platforms or their relationship with the platform, including, in some cases, even the existence of the agreement between the platform and the user.
- *Disclaimers on the reach or performance of ads*—this includes instances where the agreement explicitly disclaims any guarantee about the rank, performance or position of an ad or, in some cases, whether it will be displayed at all. This does not include general disclaimers on quality of services, which were also often included in the agreements reviewed.

A summary of these clauses and some of the arrangements in which these concerns are identified are set out in table 5.1. The ACCC notes that the table below does not provide an exhaustive summary of all terms reviewed as part of the review (for example, it excludes agreements relating to developer products and services). Nor does it capture all potentially unfair terms identified, only those that were most common across all terms reviewed. For example, the table does not include terms that hold the user responsible for actions in respect of an account, even where these actions are not authorised by the user (for example, where the user has not contributed to a security breach and the platform could have monitored and identified suspected activity). However, the ACCC has identified the presence of such terms in some arrangements.[345]

[345] For example, see clause 2A of Amazon's Advertising Agreement, accessed 9 June 2020, which states: 'Customer is solely responsible for its Advertising Console account, including all activity that occurs under its Advertising Console account (including incurred Fees) regardless of whether the activities are authorized or undertaken by Customer.'

## Table 5.1: Types of potentially unfair clauses in advertising or business terms

| | Broad discretion to remove content | Broad discretion to suspend/ terminate | Ability to vary terms without notice | Prohibitive dispute resolution process | Confidentiality or publicity limitations | Disclaimer on reach or performance of ads |
|---|---|---|---|---|---|---|
| ***Advertising terms*** | | | | | | |
| **Amazon**[346] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Expedia**[347] | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| **Facebook**[348] | ✓ | × | ✓[349] | ✓ | ✓ | ✓ |
| **Google**[350] | ✓ | ✓ | ×[351] | ✓ | ✓ | × |
| **Instagram**[352] | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| **Microsoft**[353] | ✓ | ✓ | ×[354] | ✓ | × | × |
| **Snapchat**[355] | ✓ | ✓ | ✓[356] | ✓ | × | ✓ |
| **Twitter**[357] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ***Business terms*** | | | | | | |
| **WhatsApp Business**[358] | ✓ | ✓ | ✓ | ✓ | ✓ | N/A |
| **YouTube**[359] | ✓ | ×[360] | ×[361] | ✓ | × | N/A |

346 Amazon, Advertising Agreement, accessed 9 June 2020.
347 Expedia, Terms and Conditions for the TravelAds Service, accessed 5 June 2020.
348 Facebook, Self-Serve Ad Terms, accessed 28 April 2020; in conjunction with Facebook, Terms of Service, accessed 24 April 2020; Facebook, Commercial Terms, accessed 28 April 2020; Facebook, Advertising Policies, accessed 29 April 2020.
349 As noted above, the ACCC's review of platform terms was undertaken at a point in time between April and June 2020. During that review, the Self-Serve Ad Terms (applicable to all users that use Facebook's self-serve advertising services), Commercial Terms and Advertising Policies did not specify a notice period for changes to those respective terms, or else indicated that no notice is required. However, the ACCC notes that Facebook amended its Terms of Service (which also apply to users of Facebook's self-serve advertising services) during 2020, both before and after the ACCC's review. Facebook's Terms of Service have, at various times, included a clause requiring Facebook to provide 30 days' notice before making changes to the terms.
350 Google, Ads Terms & Conditions, accessed 4 June 2020.
351 Google may make non-material changes at any time without notice, but will provide 7 days' notice of any material changes, except changes made for 'legal reasons', which may be effective immediately upon notice; see Google, Ads Terms & Conditions, accessed 4 June 2020.
352 The applicable terms are the same as those for Facebook.
353 Microsoft, Advertising Agreement, accessed 4 June 2020; in conjunction with Microsoft, Services Agreement, accessed 4 June 2020.
354 Microsoft will provide 15 days' notice of any material changes, but may make non-material changes at any time without advance notice; see Microsoft, Advertising Agreement, accessed 4 June 2020.
355 Snap, Self-Serve Advertising Terms, accessed 17 June 2020; Snap, Business Services Terms, accessed 10 June 2020; Snap, Terms of Service, accessed 5 June 2020.
356 Snap's Self-Serve Advertising Terms are silent regarding revisions, but Snap may terminate its Business Services Terms without notice, which the Self-Serve Advertising Terms are incorporated into.
357 Twitter, Master Services Agreement, accessed 6 May 2020; see also Twitter, Terms of Service, accessed 30 April 2020.
358 WhatsApp, Business Terms of Service, accessed 31 May 2020; WhatsApp, Business Policy, accessed 30 May 2020.
359 YouTube, Terms of Service, accessed 7 June 2020; see also YouTube, Channel Monetisation Policies, accessed 7 June 2020, which incorporate the Terms of Service.
360 YouTube may suspend or terminate users' access or account in the case of a material or repeated breach of the Terms of Service, where required by law, or where YouTube believes there has been potentially harmful conduct; see YouTube, Terms of Service, accessed 7 June 2020.
361 YouTube will provide reasonable advance notice of any material modifications, but modifications addressing newly available features or modifications made for legal reasons may be effective immediately without notice; see YouTube, Terms of Service, accessed 7 June 2020.

## 5.3. Effect of potentially unfair terms

As noted above, the ability to advertise, and create and maintain relationships with customers, on platforms has brought wide-ranging benefits to businesses and the affordability, efficiency and ease of use of platforms has been particularly valuable for small businesses. However, the power imbalance between platforms and small businesses, and the terms that small businesses are required to adhere to in order to use platforms' services, may be unfair to small businesses and result in harmful consequences.

For example, Bloomberg reported arbitrary suspensions of seller accounts by Amazon on its e-commerce platform, resulting in significant losses for those sellers.[362] There are also reports of Facebook applying advertising policies inconsistently and preventing businesses from advertising on its platform.[363]

**Box 5.1: Recommendations in the DPI Final Report for internal dispute resolution standards and the establishment of an ombudsman scheme**

The observations related to the dispute resolution processes of platforms and their policies further support the Digital Platform Inquiry's recommendations that digital platforms comply with set standards for internal dispute resolution of raised issues (recommendation 22) and potentially the establishment of an ombudsman scheme to resolve complaints and disputes (recommendation 23). Both recommendations were informed by business feedback relating to difficulties in resolving issues with key platforms, particularly in relation to advertising as well as concerns with scam advertising.

In addition, the arrangements offered by large platforms can affect users of services that embed the terms of service of larger platforms into the supply of their own goods and services. For example:

- Shopify offers online retailers 'tools to start, grow, market, and manage a retail business of any size'.[364] When merchants enrol in Shopify Payments, Shopify creates a Google Payment account on the user's behalf that states that, by using Google Payment, the merchant/user agrees to be bound by the Google Payment API Terms of Service.[365]
- Mailchimp, a marketing automation platform and email marketing service, uses Google Maps and YouTube to provide certain features of its service. In its terms and conditions, users must agree that by signing up for an account and using Mailchimp's service, they are bound by the Google Maps/Earth Additional Terms of Service and the YouTube Terms of Service (including Google's Privacy Policy).[366]

Accordingly, the effect of platforms' terms and conditions may extend beyond immediate users of platforms' services. Further, while the application of certain standard terms to businesses may vary, the ACCC had concerns that when the standard terms are applied to small businesses, the impact may be particularly acute.

---

362 S Soper, Amazon Angers Mom-and-Pop Sellers With 'Arbitrary' Suspensions, *Bloomberg*, 27 August 2016, accessed 22 September 2020.

363 See, for example, M Elmas, "Bane of my life": How Facebook's hemp ban is holding back an industry, *Smart Company*, 22 September 2019, accessed 22 September 2020; Australian Small Business and Family Enterprise Ombudsman, Submission to the ACCC Digital Advertising Services Inquiry, 16 April 2020, p. 1.

364 Shopify, Company Information, accessed 22 September 2020.

365 Shopify, Terms of Service, accessed 22 September 2020.

366 Mailchimp, Terms of Service, accessed 22 September 2020.

**Box 5.2: Recommendations in the DPI Final Report prohibitions on unfair contract terms and unfair trading practices**

Due to the impact of potentially unfair clauses in the terms and conditions of large digital platforms on businesses, and particularly small businesses, the ACCC reiterates the recommendations in the DPI Final Report that unfair contract terms be prohibited (including penalties applying to their use) and there be a prohibition on certain unfair trading practices (recommendations 20 and 21).

Governments across the world are recognising the need for greater transparency on the part of large platforms and enacting legislation to ensure fairness in dealings between platforms and businesses, including small businesses. This is discussed further in chapter 7.

# 6. Emerging trends, technologies and practices

The terms of the Direction for this Inquiry cover consideration of trends, including innovation and technology change, that may affect the degree of market power held by digital platform providers and the impact on the characteristics and quality of their services. This includes considering developments in digital platform services markets outside of Australia.

This chapter focuses on key emerging trends, technologies and practices observed in relation to the supply of online private messaging, social media and search services and their impact on competition and consumers. The chapter is structured as follows:

- **Section 6.1** discusses the growth of platforms' ecosystems through acquisitions and expansion into new markets.
- **Section 6.2** discusses consumer use of voice activated services such as through connected devices and voice assistants, supplied by platforms like Google, Amazon and Facebook.
- **Section 6.3** discusses new consumer products and services, including augmented and virtual reality services offered by platforms also supplying online private messaging, social media and search services.
- **Section 6.4** discusses the potential for personalised pricing in online markets and the role of search and social media platforms.

## 6.1. The expansion of large platforms' activities and ecosystems could impact competition and consumer choice

- **The expansion of large platforms, including Google, Facebook, Microsoft, Amazon and Apple into new markets and sectors has the potential to impact competition and consumer outcomes if platforms are able to leverage their market power into these new markets. By extending their ecosystems into new markets, large platforms are increasingly facilitating potential lock-in of consumers.**

Large platforms such as Google, Facebook, Microsoft, Amazon and Apple continue to grow globally and within Australia, driven by both organic expansion and acquisitions.

Between 1987 and 2019, Amazon, Apple, Facebook, Google/Alphabet and Microsoft between them acquired over 720 companies[367], with more than half of these acquisitions made in the last decade. In the last decade to 2019, Bloomberg estimates these companies made 431 acquisitions worth a combined USD $155.7 billion.[368] Gautier and Lamesch estimate 175 acquisitions were made between 2015 and 2017 alone, most of which were 'small and young technology companies, with some outliers of more experienced firms'.[369]

Google, in particular, reportedly made 168 acquisitions between 2008 and 2018[370], and some parts of Google's business such as its home-automation business have been established almost entirely by acquisition.[371]

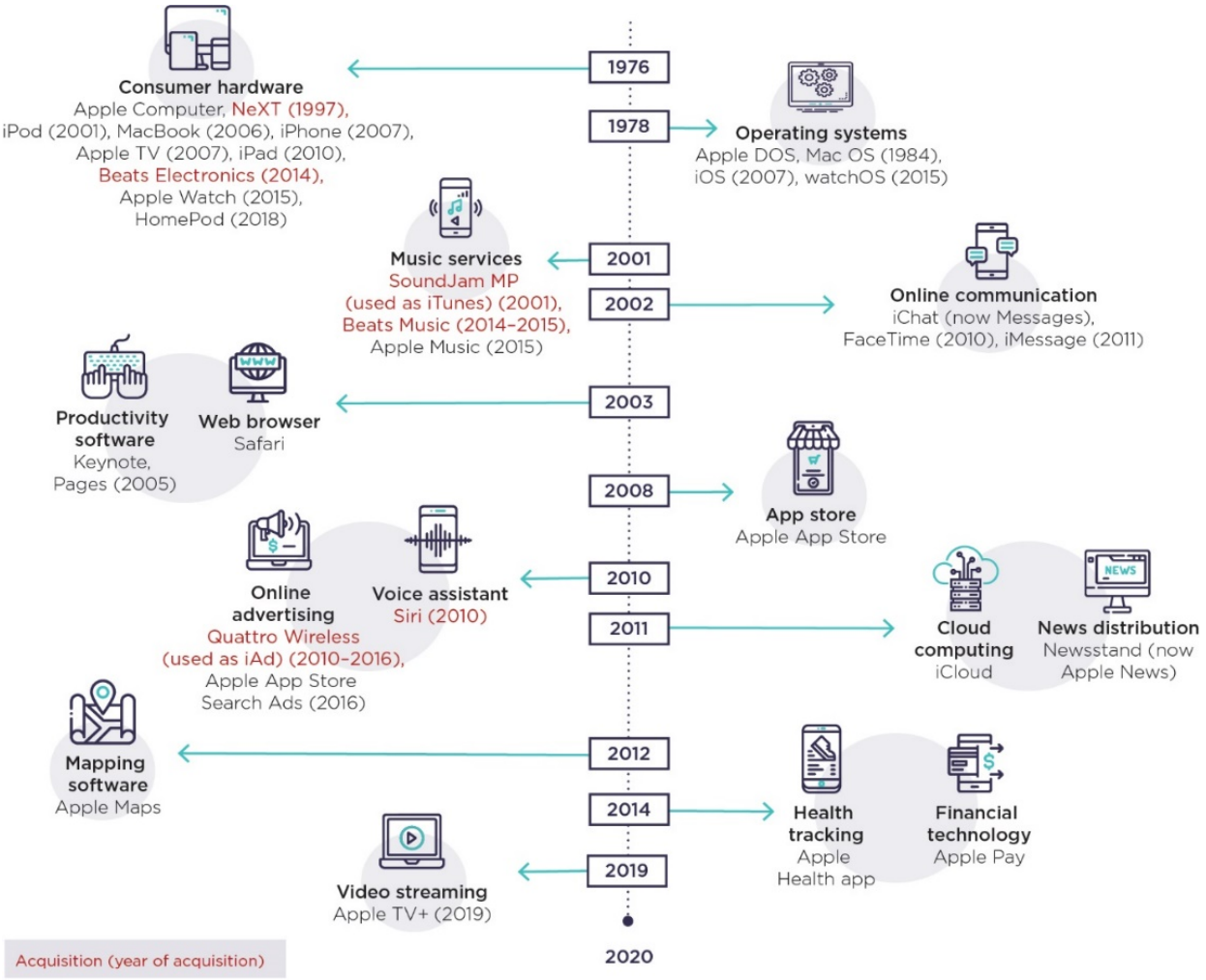
---

367 D L Moss, The Record of Weak US Merger Enforcement in Big Tech, *American Antitrust Institute*, 8 July 2019, pp. 4–5.
368 D McLaughlin, Did Big Tech Get Too Big? More of the World is Asking, *Bloomberg Businessweek*, 22 March 2019, updated 27 July 2020, accessed 22 September 2020.
369 A Gautier and J Lamesch, Mergers in the Digital Economy, CESifo Working Paper No. 8056 (2020), p. 14.
370 E Argentesi et al, Ex-post assessment of merger control decisions in digital markets: final report, document prepared by Lear for the Competition and Markets Authority, 9 May 2019, p. 149.
371 L M Khan, The Separation of Platforms and Commerce, Columbia Law Review, Vol. 119, No. 4, May 2019.

Figure 6.1, figure 6.2, figure 6.3 and figure 6.4 below show the expansion in the activities of key platforms, the result of both acquisitions and organic expansion.

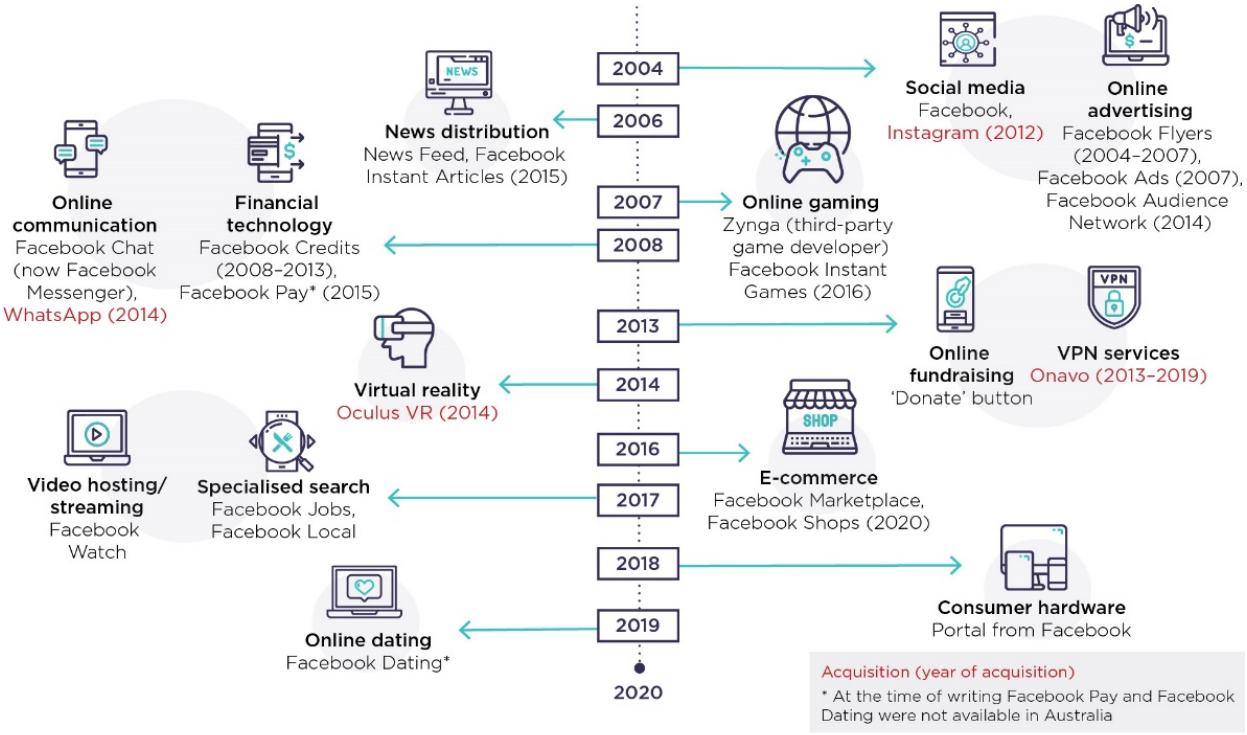
More detailed illustrations of Google and Facebook's expansion can also be found at appendices E and F.

**Figure 6.1: Examples of Apple's expansion**



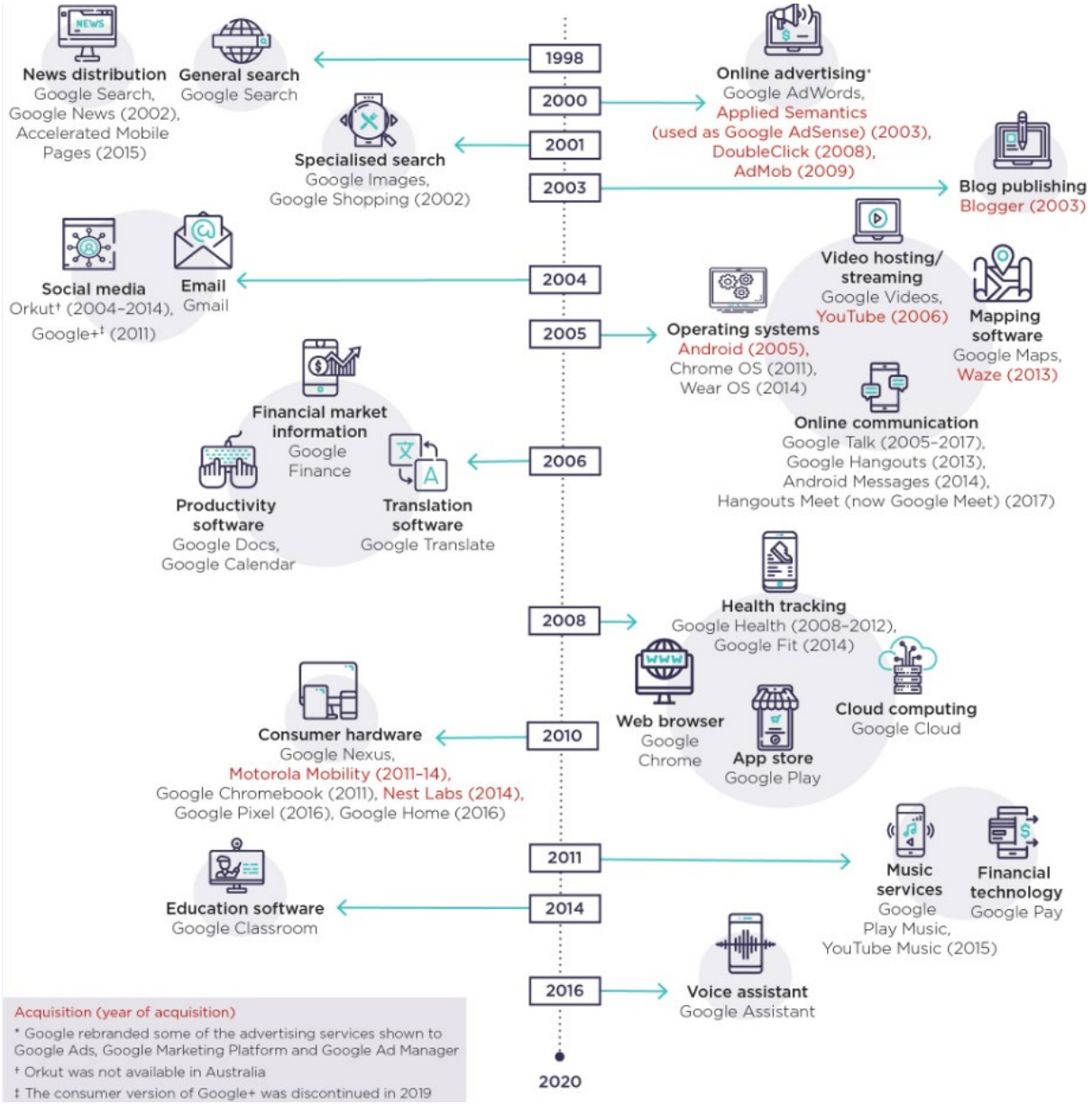

Source: ACCC analysis.

## Figure 6.2: Examples of Facebook's expansion



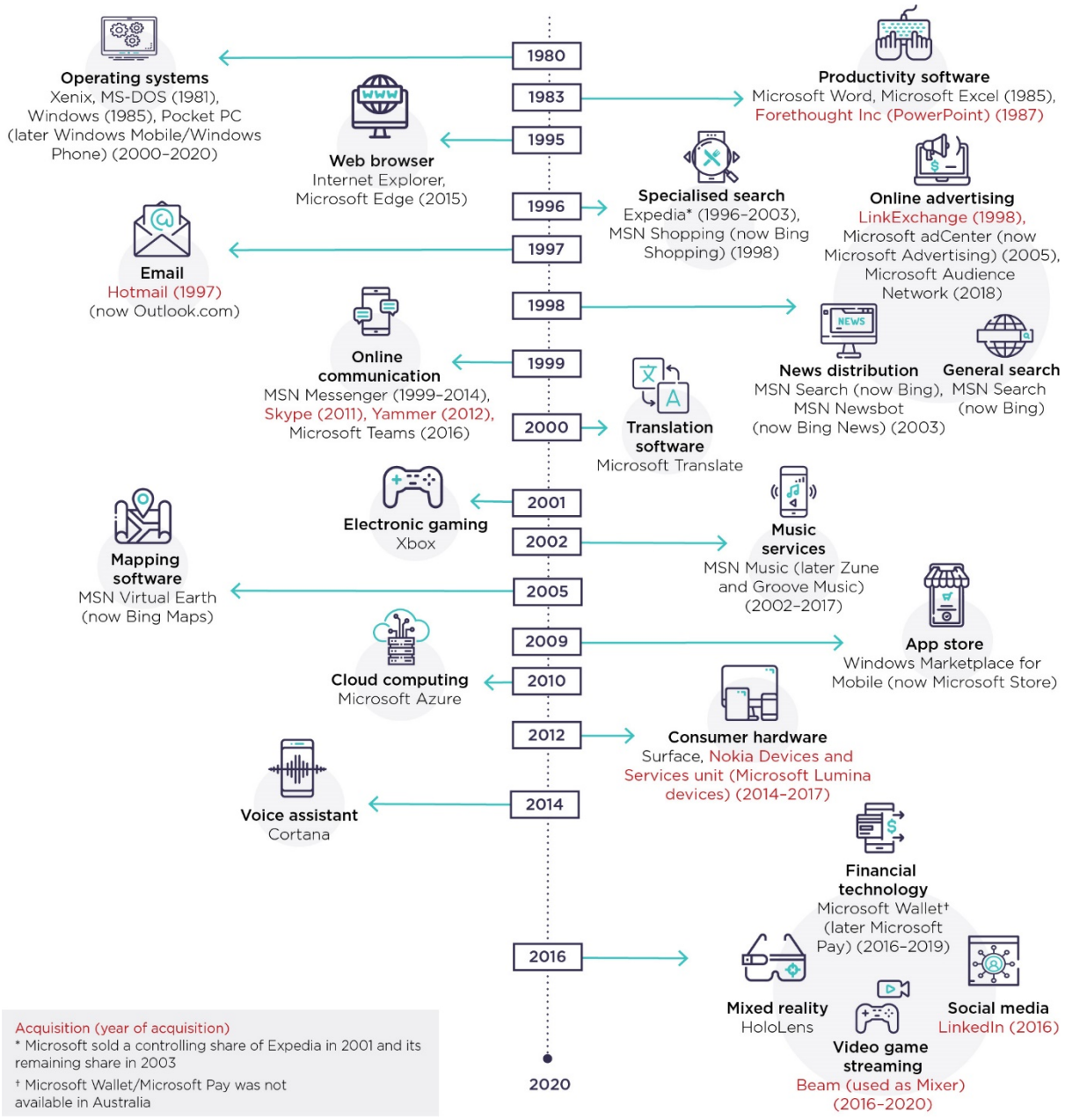

Source: ACCC analysis.

## Figure 6.3: Examples of Google's expansion




Source: ACCC analysis.

**Figure 6.4: Examples of Microsoft's expansion**




Source: ACCC analysis.

In addition to expanding their consumer and business facing activities (discussed further below), there appears to be a more recent trend of large platforms integrating vertically into various parts of the telecommunications infrastructure supply chain, either by acquisition or organic expansion, as outlined in box 6.1 below.

**Box 6.1: Platforms' expansion into the telecommunications supply chain**

Facebook, Google, Microsoft and Amazon now have a range of partnerships with telecommunications providers in overseas markets. Given the reliance of these platforms on telecommunications networks, they have a clear incentive to ensure the telecommunications services on which they rely are reliable and far-reaching.[372] Integration in the supply chain for these services may also bring efficiencies for platforms through lower costs and more control over the quality and capacity of their services running over the network.[373]

Some examples of platform partnerships and investment in overseas telecommunications markets are outlined below.

**Telecommunications companies**: Both Facebook and Google recently acquired shares in an Indian telecommunications company, making Facebook the largest minority shareholder.[374] Google is also working with that company on a customised version of Android operating system to develop low-cost entry level smartphones for sale in India.[375] India is considered to represent a significant potential user base for platforms with a large offline population.[376]

**Telecommunication satellites**: Facebook, Amazon and Google are reported to have plans to deploy low earth orbit (LEO) satellite networks, which can provide internet access to remote and underserved areas, such as in parts of Africa and Asia. Amazon is reported to be most advanced of the three (in terms of number of satellites).[377] Platforms would have the option to offer retail internet services directly to users, or alternatively to sell wholesale services to retailers.

**Submarine cables**: Submarine cables connect internet services between countries and may also connect to data centres. Google, Facebook, Microsoft and Amazon are reported to own or lease nearly half of the submarine cable bandwidth.[378] Google and Facebook are working with partners to improve or build new submarine cables to support growth in data and content traffic between continents.[379]

**Mobile network infrastructure**: Facebook has a number of partnerships to help build mobile network infrastructure in countries including Peru.[380]

---

372 In their 2019 Annual Reports, Facebook, Alphabet (Google) and Snap acknowledged the need to ensure the reliability of their networks and infrastructure for their users. See Alphabet Inc., Form 10-K lodged with the United States Security and Exchange Commission, for the fiscal year ending December 31 2019, p. 15; Facebook Inc., Form 10-K lodged with the United States Security and Exchange Commission, for the fiscal year ending December 31 2019, p. 26; Snap Inc., Form 10-K lodged with the United States Security and Exchange Commission, for the fiscal year ending December 31 2019, p. 10.

373 For example, Google has stated that its submarine cables are necessary to lower prices on carrying traffic and to connect various data centres internationally. See D Shepardson and A Shalal, U.S. approves Google request to use segment of U.S.-Asia undersea cable, *Reuters*, 9 April 2020, accessed 22 September 2020.

374 D Fischer and A Mohan, Facebook invests $5.7 Billion in India's Jio Platforms, Facebook Newsroom, 21 April 2020, accessed 22 September 2020.

375 M Singh, Google invests $4.5 billion in India's Reliance Jio Platforms, *Tech Crunch*, 15 July 2020, accessed 22 September 2020.

376 R Agrawal, Why Facebook is betting big on India, *Foreign Policy*, 23 April 2020, accessed 22 September 2020.

377 P Buddle, The race for global broadband satellite internet is on, *Independent Australia*, 3 June 2020, accessed 22 September 2020.

378 M Singh, Facebook, telcos to build huge subsea cable for Africa and Middle East, *Tech Crunch*, 14 May 2020, accessed 22 September 2020.

379 Google is working with Orange Telxius (part of Telefonica Group) on backhaul extensions for the Dunant submarine cable, which connects the United States to the French Atlantic Coast, and aims to launch late 2020. Facebook is partnering with several companies to build a subsea cable to connect Europe, Africa and the Middle East (the 2Africa project), expected to be live by 2023 or 2024. See Orange, Orange and Telxius are teaming up on Dunant submarine cable, a Google project, to provide each other with terrestrial backhaul extensions in France and in the US, Press Release, 18 February 2020. M Singh, Facebook, telcos to build huge subsea cable for Africa and Middle East, *Tech Crunch*, 14 May 2020, accessed 22 September 2020.

380 In Peru, Facebook is partnering to launch 'Internet para Todos (IpT) Peru', which aims to develop an open access wholesale rural mobile infrastructure operator in Latin America. See Facebook, 'Expanding broadband connectivity in rural Peru with Internet Para Todos', 6 August 2019, accessed 22 September 2020.

### 6.1.1. Acquisitions by large digital platforms risk adverse competitive effects and require scrutiny

While some of the acquisitions by large digital platforms may have been benign or beneficial for consumers, concerns have been raised that some of the acquired firms could have provided much-needed competition as rivals to the incumbent platforms. In particular, some acquisitions may have helped to cement platforms' position in their core market, and led to harm to rivals in the platforms' core and related markets.[381] For example, while specific acquisitions by Facebook may not have amounted to a substantial lessening of competition, there appears to be a pattern of Facebook acquiring businesses in related markets, which may or may not have evolved into potential competitors. This has the effect of entrenching Facebook's market power.[382]

There are concerns that where a platform occupies a strong gateway position and acquires a business in a related market, the platform may have the ability and incentive to harm downstream rivals through high fees or restricted access.[383] Moreover, acquisitions of data-driven businesses could further entrench the data endowments of incumbent platforms, which could create a competitive advantage that makes it even more difficult for platforms' rivals to compete.[384]

Acquisitions by large digital platforms of businesses in related markets, such as Facebook/Instagram, Google/DoubleClick, Google/Waze and Microsoft/LinkedIn, have generated significant attention, either during initial consideration of the acquisition or following subsequent retrospective consideration. Facebook's acquisition of Instagram in particular, highlights an inherent challenge for competition agencies reviewing potential acquisitions by digital platforms—the need to forecast changing digital habits of consumers, and the likelihood of firms to grow and develop to match those changing habits in the absence of a proposed acquisition.[385]

Concerns surrounding the market outcomes of past acquisitions by digital platforms and the challenges of assessing such mergers have led to calls for a greater understanding and scrutiny of such transactions in Australia and elsewhere.

In Australia, the ACCC recommended that large platforms agree to a voluntary merger notification protocol to give the ACCC advance notice of proposed transactions to address the issue of strategic acquisitions contributing to a platform's market power.[386] The ACCC is working towards a protocol, which is subject to negotiation between the ACCC and large digital platforms.

Internationally, the UK CMA commissioned Lear to review past merger decisions in the digital sector, including how competition authorities generally assess potential competition theories of harm in digital markets, and evaluating market evolution since some digital mergers.[387]

---

381 J Furman et al, Report of the Digital Competition Expert Panel, Unlocking digital competition, 13 March 2019, p. 92.
382 ACCC, DPI Final Report, 26 July 2019, p. 81.
383 J Furman et al, Report of the Digital Competition Expert Panel, Unlocking digital competition, 13 March 2019, pp. 92–93.
384 E Argentesi et al, Ex-post assessment of merger control decisions in digital markets: final report, document prepared by Lear for the Competition and Markets Authority, 9 May 2019, p. ii.
385 ACCC, DPI Final Report, 26 July 2019, p. 81.
386 ACCC, DPI Final Report, 26 July 2019, p. 30.
387 Competition and Markets Authority, Assessment of merger control decisions in digital markets, 3 June 2019, accessed 22 September 2020.

In addition, the Furman Report[388] made recommendations regarding the CMA's consideration of mergers involving digital platforms including that:

- the CMA should further prioritise scrutiny of mergers in digital markets and closely consider harm to innovation and impacts on potential competition in its case selection and in its assessment of such cases,
- digital companies that have been designated with 'strategic market status' should be required to make the CMA aware of all intended acquisitions, and
- the CMA's Merger Assessment Guidelines should be updated 'to reflect the features and dynamics of modern digital markets, to improve effectiveness and address under enforcement in the sector.'

In the United States, the FTC is also looking at past acquisitions by large technology companies, and has sought information from Alphabet Inc. (including Google), Amazon.com Inc., Apple Inc., Facebook Inc., and Microsoft Corp. about prior acquisitions not reported to antitrust agencies.[389]

In Europe, the 'Competition Policy for the Digital Era' report prepared for the European Commission proposed a new theory of harm to fill a perceived gap in the currently accepted theories of harm.[390] This new theory of harm intends to capture the potential adverse competition effects of acquisitions by large digital platforms of innovative, quickly growing start-ups. It would involve consideration of potential defensive strategies by large platforms, including where the merger could strengthen the position of the acquirer's ecosystem through new services and increased network effects, which could reduce the risk of users leaving the acquirer's ecosystem as a whole. The report, however, did not go so far as to recommend legislative changes to the EU merger regime.[391]

### 6.1.2. The growth of platform based ecosystems and potential risks for competition and consumers

Through organic expansion and acquisitions, large platforms are increasingly providing integrated suites of hardware and software, effectively creating and expanding 'ecosystems' of products and services that interoperate with each other. Within these ecosystems, software owned by the same company is often preinstalled or set as default in other software or hardware.

The CMA observed a defining feature of Google and Facebook's businesses to be the large ecosystems of complementary products and services they have built around their core service.[392] This practice is increasingly common across digital markets.

---

388 J Furman et al, Report of the Digital Competition Expert Panel, Unlocking digital competition, 13 March 2019, pp. 138–139.

389 Federal Trade Commission, FTC to Examine Past Acquisitions by Large Technology Companies, Press Release, 11 February 2020.

390 The perceived gap in theories of harm refers to instances where an operator with a dominant position in a core market buys up a firm that is active in a separate, but related market and has the potential to grow into a competitive threat beyond that market. See J Cremer, Y-A de Montjoye and H Schweitzer, Competition policy for the digital era, European Commission, 2019, p. 116–117.

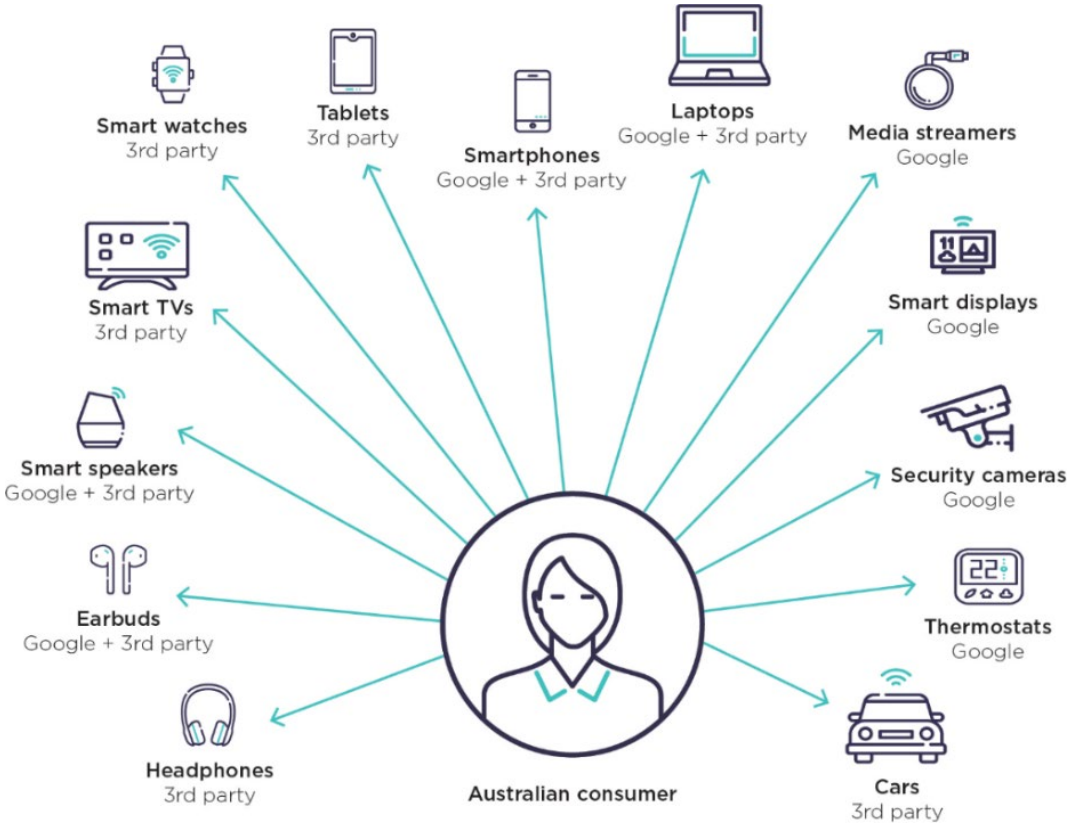
391 J Cremer, Y-A de Montjoye and H Schweitzer, Competition policy for the digital era, European Commission, 2019, pp. 122–124.

392 Competition and Markers Authority, 'Online platforms and digital advertising – Market study final report' 1 July 2020, p. 18.

Tech companies like Microsoft[393] and Apple[394] have traditionally followed this model, offering a range of hardware and software products and services to consumers that work with each other, and may have the effect of encouraging users to stay within their ecosystem. This is more pronounced with Apple as these devices operate within a relatively closed ecosystem, which historically has had limited compatibility with third party products.

Google has a suite of consumer facing hardware and software products that interoperate with each other, with the hardware often offering a bundle of Google software products, including Google Assistant. As shown in figure 6.5, Google software is preinstalled on a broad range of hardware, manufactured by both Google and third parties, including computers, smartphones, tablets, smart speakers and smart TVs (noting that the figure is a non-exhaustive illustration of Google's ecosystem). This growing range of products and the need to access services with a Google Account may have the effect of keeping users within Google's ecosystem, particularly as users become reliant on Google's products and services.

**Figure 6.5: Hardware on which Google software is pre-installed**




Source: ACCC analysis.

---

393 Microsoft produces the Windows operating system, which often comes with a range Microsoft consumer facing and business-focused software products pre-installed including the Microsoft Office suite (known as the Microsoft 365 apps, consisting of Word, Excel, PowerPoint, Teams and others), the Microsoft Edge web browser, the Microsoft Pay digital wallet and Skype. Microsoft also owns LinkedIn, a professionally oriented social networking platform, and Microsoft Azure, a cloud-computing platform. From Version 1902 onwards, Microsoft Teams will be pre-installed as part of the Microsoft 365 apps and installed on existing Microsoft 365 apps on devices running Windows. See Microsoft, Deploy Microsoft Teams with Microsoft 365 Apps, 10 June 2020, accessed 22 September 2020; Microsoft, Understand the different apps included in Windows 10, 9 May 2020, accessed 22 September 2020.

394 Apple produces desktops, laptops, smartphones, tablets, wearables and smart speakers (among others), as well as digital services such as the Apple Music streaming service. Apple has recently announced that users are able to set their own default email and browser apps, rather than setting default email and browsers for the user. See Apple, Australian online store, accessed 22 September 2020; T Warren, Why are iOS 14 default apps limited to just browser and email apps?, *The Verge*, 24 June 2020, accessed 22 September 2020.

Google is also increasingly offering enterprise or education facing products and services, such as the Google G Suite for Education, a suite of tools for students and teachers to connect via email, chat and video, to collaborate on documents, spreadsheets and presentations, and to organise tasks, among a number of other functions designed for education.[395]

Furthermore, as shown in box 6.2, Google's terms and conditions are increasingly being incorporated into the terms of separate services, including those offered by third parties.

**Box 6.2: Incorporation of Google terms into a wide range of services including third party products and services**

A growing number of consumers may be bound by Google's data collection policies as Google's terms and conditions are increasingly being incorporated into the terms of other services, including essential third party products and services. In some cases, there is little or no opportunity to opt out of these terms and conditions. For example:

- A number of businesses utilise services such as Google Maps and Google Ads, and require their customers to agree to Google's terms.[396]
- Google's Terms of Service and Privacy Policy are applicable to its virtual voice-activated Google Assistant, which may be integrated with third party products and services, including a number of essential products and services, such as energy and banking.[397]
- Google's Terms of Service extend to its educational product, G Suite for Education, and Google's Privacy Policy allows it to combine personal information from one service—such as G Suite for Education—with information, including personal information, from other Google services.[398]
- Google's reCAPTCHA service, which helps protect websites from spam and abuse by blocking malicious software, is also subject to Google's Privacy Policy and Terms of Service.[399] Tech statistics website Built With estimates there are more than 5 million live websites using reCAPTCHA.[400]

Facebook is also reportedly looking to consolidate its ecosystem further by introducing interoperability between its existing core services (Facebook Messenger, WhatsApp and Instagram). This would allow users to message each other without switching apps and likely see users spend more uninterrupted time within the Facebook family of services.[401] Facebook already collects and uses information collected from users and their devices across its products[402] and is also reported to be developing its own operating system and voice assistant.[403] This would be used in its growing range of consumer hardware devices (such as Portal Home and Oculus headsets), to reduce its reliance on Google's Android

---

395 Google, G Suite for Education, accessed 22 September 2020.

396 The customer service agreement of NSW toll roads and e-tag provider Linkt (owned by Transurban) states that, by using Linkt's online services, users agree to be bound by Google's Terms of Service. See Linkt, Tagless Account Customer Service Agreement, accessed 17 June 2020; see also smaller businesses, such as Alliance Pharmacy App Terms of Use, accessed 22 September 2020; Australian Native Food Co Privacy Policy, accessed 22 September 2020; Medic Relief Terms of Use, accessed 22 September 2020.

397 AGL, AGL Action for Google Assistant, Terms and Conditions, accessed 12 June 2020. Westpac, Voice Banking Terms of Service, accessed 23 July 2020; see also Google, Google Assistant Overview, accessed 14 July 2020.

398 Google, Privacy Policy, accessed 14 July 2020.

399 Google, reCAPTCHA, accessed 22 September 2020.

400 Built With, reCAPTCHA Usage Statistics, accessed 22 September 2020.

401 M Isaac, Zuckerberg Plans to Integrate WhatsApp, Instagram and Facebook Messenger, *The New York Times*, 25 January 2019, accessed 22 September 2020.

402 Facebook, Data Policy, accessed 22 September 2020.

403 A Heath, To control its destiny, Facebook bets big on hardware, *The Information*, 19 December 2019, accessed 22 September 2020; S Rodriguez, Facebook is working on a voice assistant to rival Amazon Alexa and Apple Siri, *CNBC*, 17 April 2019, accessed 22 September 2020.

operating system.[404] This would likely enable Facebook to collect more data from users, and benefit (as Apple and Google do) from being in control of both its hardware and software services and products.

In addition, Amazon is looking to extend its ecosystem beyond its core marketplace platform, with an expanding range of first and third party consumer connected devices (such as smart speakers, smart home devices, headphones, smart wrist band and car integration) that are compatible with its voice assistant Alexa. Amazon also offers subscription services such as Amazon Prime, a video-on-demand service.

### 6.1.3. Potential risks to competition and consumer outcomes

For consumers, the ecosystem of a platform may be beneficial if it conveniently fulfils many consumer wants at once by increasing the ease with which consumers can access multiple services as well as reducing friction between those services. Additionally, by bundling or tying[405] hardware and software, platforms can improve the quality control of their products, potentially improving the product for consumers.

However, as noted by the CMA, if a platform retains a consumer within its ecosystem, potentially through a combination of default settings, limited interoperability with rivals, or other forms of bundling or tying, then rivals may need to incur significant costs and offer an increased range of services to attract users.[406] This can make it difficult for suppliers of standalone products or services to compete and can create barriers to entry,[407] particularly where a platforms' service becomes the default for a piece of hardware. As such, competition is likely to be impacted if a platform is able to tie or bundle services in a way that allows it to leverage substantial market power from one market into another.

The expansion of digital ecosystems may also give rise to competition concerns where a platform is able to insulate its core service from future competition by eliminating the risk that a target may expand and attract users away from the platform.

Finally, by expanding their ecosystem platforms may benefit from additional opportunities to gather data from new sources or be able to engage in self-preferencing behaviour.[408] For example, Lina Khan notes the potential for dominant platforms who enter multiple markets to combine and control data from multiple sources, which may help the platform attain or maintain its power across many products.[409]

---

404 A Heath, To control its destiny, Facebook bets big on hardware, *The Information*, 19 December 2019, accessed 22 September 2020.

405 Bundling occurs when a supplier only offers two products as a package or for a lower price if the two products are purchased as a package. Tying occurs when a supplier sells one good or service on the condition that the purchaser buys another good or service from the supplier. See ACCC, Guidelines on misuse of market power, August 2018, p. 14.

406 Competition and Markets Authority, Online platforms and digital advertising market study, Appendix E: Ecosystems of Google and Facebook, 1 July 2020, p. E3.

407 L M. Khan, The Separation of Platforms and Commerce, Columbia Law Review, Vol. 119, No. 4, May 2019.

408 Competition and Markets Authority, Online platforms and digital advertising market study, Appendix E: Ecosystems of Google and Facebook, 1 July 2020, pp. E2–E3.

409 L M. Khan, The Separation of Platforms and Commerce, Columbia Law Review, Vol. 119, No. 4, May 2019.

## 6.2. Growth of voice activated services allows more extensive data collection and raises potential consumer harms

- **Voice assistants and connected devices bring convenience for consumers, but the ACCC has identified reports of problematic data collection and use, as well as reduced choice for consumers resulting from 'lock-in' to particular ecosystems.**

Consumer devices that connect to the internet (known as 'connected devices' or 'smart devices'), many of which offer a voice assistant feature, are part of the 'Internet of Things' ecosystem.[410] These devices can offer consumers an enhanced experience, responsive services and greater convenience, and as technology develops more devices are being brought into this connected ecosystem.

However, connected devices also raise a number of potential risks to competition and consumer welfare, such as problematic data collection practices and reduced choice stemming from platforms' ability to lock consumers in to a particular ecosystem, which are discussed further below.

The ACCC will continue to monitor take-up and use of these devices and services where there is potential for anti-competitive conduct and reduced consumer welfare, such as from data collection practices or self-preferencing.

### 6.2.1. Growing use of connected device assistants in Australia

Consumer research has found a continued growth in take-up of connected devices and voice assistants more generally in Australia.

This research estimates that in 2019:

- 12 per cent of households owned a smart speaker (up from 9 per cent in 2018) and sales of wrist wearables (smartwatches and smart wristbands) were up 15 per cent from 2018.[411]
- Australian households had an average of 18.9 connected devices, an increase from 17 devices in 2018.[412]
- Younger generations used voice-enabled digital assistants the most, with 29 per cent of 14-29 year olds using voice across any of their devices (phones, smart speakers, headphones) at least once a week.[413]
- Engagement with these devices is likely to increase in the future as more devices become compatible with various voice assistants.[414]

Consumers are increasingly engaging with voice assistants and connected devices supplied by platforms that also provide online private messaging, social media and/or search services

---

410 The internet of things generally refers to 'an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world'. See OECD, The Internet of Things: Seizing the benefits and addressing the challenges, 7 June 2016, p. 8.

411 Deloitte, Media Consumer Survey 2019, 2019, p. 14.

412 Telsyte, Telsyte launches Australian Digital Consumer Study 2020, 25 February 2020.

413 Compared to 27 per cent for 30-35 years, 20 per cent for 36-52 years, and 22 percent for 53–71 years. See Deloitte, Media Consumer Survey 2019, 2019, p. 14.

414 For example, Telsyte forecasts an increase 30 devices by 2022 with growth driven by adoption of smart speakers, energy and lighting devices and security devices and a 2020 study by Juniper Research estimates that consumers will interact with voice assistants on over 8.4 billion devices by 2024, compared to the 4.2 billion devices expected to be in use by the end of 2020. See Telsyte, Telsyte launches Australian Digital Consumer Study 2020, 25 February 2020; Juniper Research, Number of Voice Assistant Devices in Use to Overtake World Population by 2024, 2020.

to Australian consumers, such as Google, Facebook, Apple and Amazon. An overview of some of the devices available in Australia is at figure 6.6.

In Australia, estimates indicate that Google's smart speakers are the most popular, with Deloitte reporting that in 2019, 74 per cent of Australian households with smart speakers had Google Home speakers.[415] In the United States, however, Amazon Echo is the most popular smart speaker device with nearly 70 per cent of smart speaker owners using an Echo device.[416]

Google has indicated that every month more than 500 million people globally are using Google Assistant across smart speakers, smart displays, phones, TVs, cars and other devices.[417] Juniper Research estimates the use of voice assistants will triple in the next few years, from 2.5 billion assistants in use in 2018 to 8 billion by 2023. The majority of these assistants will live on smartphones, and thus be Google Assistant (on Android phones) or Apple's Siri (on iPhones).[418]

**Figure 6.6: Examples of connected devices and voice assistants available in Australia**


Source: ACCC analysis. Amazon, Alexa built-in devices, accessed 22 September 2020. Google, Just start with 'Hey Google', accessed 22 September 2020. Apple, Home accessories, accessed 22 September 2020.

### 6.2.2. Potential consumer harms associated with connected devices and voice assistants

Voice assistants rely on data to constantly improve and personalise their service for users, including to enhance their speech recognition features. While data collection may be necessary, as discussed elsewhere in this report, data collection poses a number of potential risks to consumers, particularly where the data is used for other purposes beyond providing or improving the service. These risks are discussed below.

---

415 Deloitte, Media Consumer Survey 2019, 2019, p. 14.
416 A He, Amazon Maintains Convincing Lead in US Smart Speaker Market, *eMarketer*, 18 February 2020, accessed 22 September 2020.
417 M Bronstein, A more helpful Google Assistant for your every day, *The Keyword (Google Blog)*, 7 January 2020, accessed 22 September 2020.
418 S Perez, Report: Voice assistants in use to triple to 8 billion by 2023, *TechCrunch*, 13 February 2019, accessed 22 September 2020.

### *Increased collection of personal information*

Connected home devices and voice assistants collect a wide variety of information about a user. In particular, connected home devices can contain a number of sensors that are used to provide various features, but which also collect a range of information about the user and their home. For example, Google Nest devices may contain various image sensors (camera), microphones, activity sensors, environmental sensors and control sensors.[419] Additionally, using Google's Nest Aware subscription service, users can teach their Nest camera device (such as Nest Cam IQ, Nest Hello Video Doorbell and Nest Hub Max) how to tell differences in faces of people they do and do not know, using face detection technology. Users are able to create a 'familiar face library' to help the camera recognise people. Google notes that it is the users' responsibility to get permission to store others' face data. Google also notes that the face detection feature is not available on the Nest Hub Max in the European Union or in Illinois.[420]

As noted above, the leading home devices and voice assistants are offered by or connected to a digital platform that also offers search, social media or private messaging services, such as Google, Amazon, Apple and Facebook. This gives these companies an opportunity to collect and use this data to enhance their core service offering, or, depending on the platform, to monetise the service and generate additional revenue through targeted advertising, as outlined in box 6.3. For example, Google states the Google Assistant and the Google Home app can access a users' search and location history. However, users are able to control what data is saved and used across Google services in their Google Account.[421]

**Box 6.3: How do platforms monetise the use of connected devices?**

There are various ways a platform can monetise a connected device including through hardware sales, collection of data and use of data for targeted advertising. For example:

- **Google** indicates that it may use the text of users' interactions with Google Assistant to inform the interests for ad personalisation, but does not use audio recordings for ad personalisation.[422] In some countries (including Australia), [423] Google also offers a paid subscription service called Nest Aware[424] described as a service that users can use with their Nest products to help keep users informed when motion or sound is detected in their home.[425]
- **Amazon's** Head of Hardware has been reported to indicate that Amazon seeks to monetise when customers use the products, not just when they buy them, and offers consumers a range of digital items like music and audiobook subscriptions to use with their device.[426] Amazon is also releasing a new health and wellness service, Amazon Halo, which includes a smart wrist band (Amazon Halo Band) and a paid-membership service that uses AI to offer insights to users.[427]

---

419 Google, Sensors in Google Nest devices, Google Nest Help, last updated 12 May 2020, accessed 22 September 2020.

420 Google, Learn about familiar face detection and how to manage your library', Google Nest Help, accessed 22 September 2020.

421 Google, 'Data security and privacy on devices that work with Assistant', Google Nest Help, accessed 22 September 2020.

422 Google states it does not use environmental and activity sensor data for ad personalisation though it may be used to 'serve a variety of purposes, such as helping your home take better care of you'. It also notes that users may opt-out of ad personalisation. See Google, Our commitment to privacy in the home, accessed 22 September 2020.

423 Google, Device Availability, Google Store Help, accessed 22 September 2020.

424 Nest Aware is a smart home camera and security system that provides alerts and camera history using certain Google Nest devices. Users pay for features including intelligent alerts and activity zones, event history and video history. See Google Store, Nest Aware, accessed 22 September 2020.

425 Nest devices start recording event clips when they detect motion or sound, and give users the clips. See S Plowman, The new Nest Aware is rolling out to Australia and New Zealand this week—one price for all your Nest cameras, Ausdroid, 13 May 2020, accessed 22 September 2020.

426 E Kim, As Amazon floods the market with Alexa devices, the business model is getting fresh scrutiny, *CNBC*, 28 September 2019, accessed 22 September 2020.

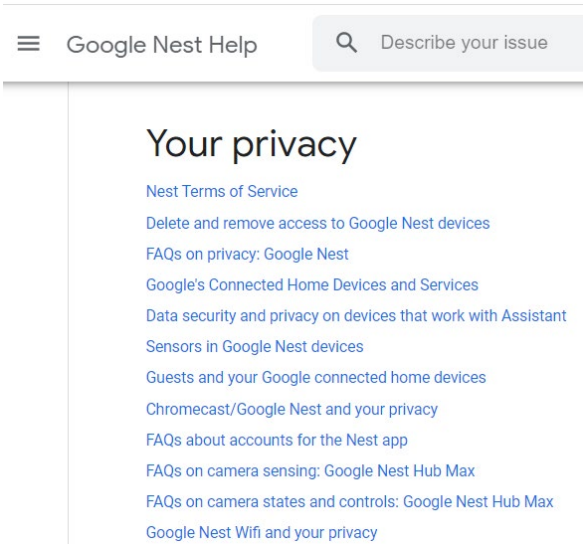
427 The Amazon Halo service, to be launched initially in the United States, collects information from a user through sensors in the Amazon Halo Band, which is used to provide insights into the users overall wellness via the Amazon Halo app. See Amazon, Introducing Amazon Halo and Amazon Halo Band – A new service that helps customers improve their health and wellness, Press Release, 27 August 2020.

- **Apple**, similar to Amazon, may seek to monetise devices beyond hardware sales through subscriptions to services such as Apple Music and Apple News+.[428]
- **Facebook** uses information about the use of Oculus products and account information to personalise ads on and off other Facebook company products.[429] Some commentators consider that Facebook views data collection as a way to make money from its hardware products (such as Oculus and Portal devices).[430]

As set out above, while consumers may benefit from the convenience of connected devices, they may not be fully aware of the extent of data collection enabled by such devices, which may limit their ability to exercise their preferred privacy controls. The increasing capture of information also exposes consumers to increased risks of profiling.[431]

Firstly, consumers may not always be aware of the amount and type of information being collected about them, and how this is used. For example, while Google has a range of information about its data collection and use in its Help Centre, it is cross-referenced and spread across a number of webpages (see figure 6.7).

**Figure 6.7: Example of some of the webpages Google provides in relation to Google's range of connected device and voice activated search pages**




Source: Google Nest Help, Your Privacy, accessed 22 September 2020

Secondly, the controls available to users to limit data collection through these devices are not always set as the default and may not reflect a consumer's privacy preferences. For example, Amazon does not appear to offer an option to opt out of voice recordings, but offers an option to delete voice recordings.[432] Facebook allows users to opt out of voice recordings, and Facebook has an option to turn off the automatic storage and transcription of voice interactions with its Portal devices, but these are not the set default.[433] Google, by default, does not retain user audio recordings, but provides an option for users to save their audio to help improve Google speech products.[434] Apple previously did not offer users an option to turn off voice recordings, but has since updated its policy and no longer collects

---

428 C Velazco, Apple's services are making more money than ever, *engadget*, 30 April 2019, accessed 22 September 2020.
429 Oculus, Privacy Policy, 27 December 2019, accessed 22 September 2020.
430 A Heath, To control its destiny, Facebook bets big on hardware, *The Information*, 19 December 2019, accessed 22 September 2020.
431 ACCC, DPI Final Report, 26 July 2019, pp. 445–446.
432 Amazon, Alexa and Alexa Device FAQs, accessed 22 September 2020. Amazon, Alexa Privacy Settings, accessed 31 July 2020.
433 Portal, How do I control how Portal handles my voice interactions, last updated 1 July 2020, accessed 22 September 2020.
434 Google, Data security and privacy on devices that work with Assistant, Google Nest Help, accessed 22 September 2020.

recordings of Siri interactions by default. However, Apple states it will continue to use computer-generated transcripts to improve Siri and offer users the ability to opt-in to help Siri improve with audio samples of their requests.[435]

Thirdly, platforms are continually updating their connected devices and voice assistants with new features for users (see box 6.4), which enable the potential for further data collection. The extent to which these new features come with consumer control is not always clear.

**Box 6.4: Examples of new features for connected devices and voice assistants**

**Google**

Google has added ultrasound sensing to its smart home Nest Hub and Nest Hub Max, which uses the devices speakers and microphones to determine the proximity of a person to show more personalised information, such as pending notifications (rather than waiting for a wake word).[436]

**Facebook**

Facebook is introducing Portal TV, which is able to automatically pan and zoom in on an active subject when it detects voice or motion. This is made possible by AI software that can map a user's body.[437]

Facebook is also reported to be developing its own AI voice assistant, which could replace Alexa on Facebook's Portal smart home devices.[438]

**Amazon**

Amazon has introduced a number of changes to Alexa, including a frustration detection feature where Alexa will apologise, for example, after it detects user frustration following an incorrect request.[439]

Amazon's new Halo Band has a number of sensors including an accelerometer, a temperature sensor and a heart rate monitor, as well as 'always-on' microphones, which listen to users to assess their mood and stress levels. Amazon reportedly states these microphones aren't connected to Alexa and recordings are analysed on the user's device, then deleted and are not uploaded to the cloud.[440]

---

435 A Hern, Apple contractors 'regularly hear confidential details' on Siri recordings, *The Guardian*, 27 July 2019, accessed 22 September 2020; C Gartenberg, Apple apologises for Siri audio recordings, announces privacy changes going forward, *The Verge*, 28 August 2019, accessed 22 September 2020.

436 A Udall, How ultrasound sensing makes Nest displays more accessible, Google Blog, 4 December 2019, accessed 22 September 2020.

437 C Nguyen, The Portal TV can track every move, but Facebook swears stalking isn't the goal, *Digital Trends*, 18 September 2019, accessed 22 September 2020.

438 S Rodriguez, Facebook is working on a voice assistant to rival Amazon Alexa and Apple Siri, *CNBC*, 17 April 2019, accessed 22 September 2020.

439 C Gartenberg, All the new features coming to Alexa, including a new voice, frustration mode, and Samuel L. Jackson, *The Verge*, 25 September 2019, accessed 22 September 2020.

440 A Hern, Amazon's Halo wristband: the fitness tracker that listens to your mood, *The Guardian*, 29 August 2020, accessed 22 September 2020.

### *Accidental activations and transcriptions*

The increase in data collection through devices and assistants also raises the risk of inadvertent or unintended disclosure of information, which may result in harms to consumers including decreased consumer welfare from reduced privacy.[441]

Since July 2019, there have been several reports of accidental activations of connected devices or voice assistants, where users were unaware they were being recorded and in some cases, this led to sensitive data leaks.[442] A 2020 report by Northeastern University in Massachusetts and Imperial College in London found that unintended activations could occur up to 19 times a day with regular use.[443] Another recent study found that there are more than 1000 terms that can activate a voice assistant (leading to potential accidental activations).[444]

Internationally, there have also been a number of reported cases where platforms including Amazon, Google and Apple, have been found to be transcribing audio conversations from connected devices,[445] including after a user chose to delete the audio files.[446] While platforms have indicated that this is to improve the products it provides, this may not always be transparent or understood by users.[447] The OAIC's Australian Community Attitudes to Privacy Survey 2020 found that 83 per cent of Australians feel their personal devices listening to their conversations and sharing data with other organisations without their knowledge is misuse, as well as an organisation collecting information about them in ways that they would not expect.[448]

While some platforms appear to be implementing measures to address these breaches and risks,[449] these are newly implemented and the effectiveness of these measures and take-up by consumers will need to be considered over time.

### *Cyber security threats*

Connected devices, as with other technologies, are vulnerable to cyber-attacks or hacking, and could impact consumers where it leads to reduced data control and targeting of vulnerable consumers. The IoT Security Alliance considers that IoT devices are not always designed with security in mind. This can create risks that devices can be subverted into

---

[441] For a discussion of these types of harms, see the ACCC, DPI Final Report, 26 July 2019, pp. 444-445.

[442] A Hern, Apple contractors 'regularly hear confidential details' on Siri recordings, *The Guardian*, 27 July 2019, accessed 22 September 2020. K Paul, Google workers can listen to what people say to its AI home devices, The Guardian, 12 July 2019, accessed 22 September 2020. M Day, G Turner and N Drozdiak, Amazon Workers Are Listening to What You Tell Alexa, Bloomberg, 11 April 2019, accessed 22 September 2020.

[443] D J Dubois et al, When Speakers Are All Ears – Understanding when smart speakers mistakenly record conversations, Mon(IoT)r Research Group, 14 February 2020.

[444] L Schonherr et al, "Unacceptable, where is my privacy?" Exploring Accidental Triggers of Smart Speakers, Ruhr University Bochum and Max Planck Institute for Security and Privacy, 2 August 2020.

[445] M Bridge, Google workers 'eavesdrop' on recorded conversations, *The Australian*, 13 July 2019, accessed 22 September 2020.

[446] M Kelly and N Statt, Amazon confirms it holds on to Alexa data even if you delete audio files, *The Verge*, 3 July 2019, accessed 22 September 2020.

[447] M Bridge, Google workers 'eavesdrop' on recorded conversations, *The Australian*, 13 July 2019, accessed 22 September 2020; A Hern, Facebook admits contractors listened to users' recordings without their knowledge, *The Guardian*, 14 August 2019, accessed 22 September 2020; M Day, G Turner, and N Drozdiak Amazon Workers Are Listening to What You Tell Alexa, *Bloomberg*, 11 April 2019, accessed 22 September 2020; A Hern, Apple contractors 'regularly hear confidential details' on Siri recordings, *The Guardian*, 27 July 2019, accessed 22 September 2020.

[448] OAIC, Australian Community Attitudes to Privacy Survey 2020, September 2020, p. 36.

[449] For example, Google added a new feature to help reduce unintentional hot word activations and tune how sensitive smart displays and speakers are to "Hey Google". This was announced in September 2019 and rolled out from April 2020. See Google, "Hey Google" sensitivity can now be configured, Google Assistant Help, 5 May 2020, accessed 22 September 2020; T Lyles, Google is rolling out a 'Hey Google' sensitivity feature for smart devices, *The Verge*, 21 April 2020, accessed 22 September 2020.

performing incorrect actions and could be used for distributed denial of service (DDoS)[450] attacks to take down websites and disrupt business operations.[451]

International reports indicate that incidents of global attacks on IoT devices, including smart hubs, have nearly doubled since 2018.[452] A recent report by the ACMA notes that the vulnerabilities in a connected device could potentially compromise an entire home network. It also noted that consumers need to be supported in understanding these issues and the actions being taken by industry to address them, and that improved digital literacy for consumers could help address this information asymmetry.[453]

Smart speakers or hubs may be particularly vulnerable to cyber-attacks as they typically have access to other connected devices in the home. In 2019, researchers reported finding vulnerabilities affecting Google and Amazon smart speakers, which could allow hackers to eavesdrop or phish users. While the research noted there was no evidence that this had actually occurred, it found it was possible to activate smart speakers to silently record users, or ask for the password to their Google account by uploading malicious software disguised as 'Skills' for Alexa or 'Actions' for Google.[454]

In Australia, the Department of Home Affairs has released a voluntary Code of Practice: Securing the Internet of Things for Consumers, which includes voluntary measures for industry that the Australian Government recommends as the minimum standard for IoT devices.[455]

### 6.2.3. Potential impacts on competition from use of connected devices and voice assistants

#### *Consumer lock-in to an ecosystem*

Connected devices are typically linked to a particular platform ecosystem and voice assistant. This means consumers are susceptible to being locked into one ecosystem, particularly as they adopt more devices supplied by the same platform.[456] However, this may be driven in part by consumer preferences to ensure multiple connected devices in the home can interact. Research of American consumers in 2018, for example, found that when shopping for a smart home device or product, 89 per cent indicated they were influenced by its compatibility with their voice assistant and 85 per cent indicated a smart device they owned influenced what kind of voice assistant they used/purchased.[457] Consumer lock-in can reduce competition as it can create barriers to entry or expansion for rival suppliers as consumers are less able or willing to shop around and try new products and services.

---

[450] A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic (like an unexpected traffic jam). DDoS attacks utilise multiple compromised computer systems as sources of attack traffic, including computers and IoT devices. See Cloudflare, What is a DDoS Attack?, accessed 22 September 2020.

[451] There have also been earlier reports of connected home devices being used in DDoS attacks on websites, including Twitter, Spotify and Reddit. See IoT Cybersecurity Alliance, Demystifying IoT Security White Paper, 2017, pp. 2-3; BBC News, 'Smart' home devices used as weapons in website attack, *BBC News Technology*, 22 October 2016, accessed 22 September 2020.

[452] According to Tech Accord, in the first half of 2019 there were 2.9 billion cyber attacks on IoT devices compared to 813 million in the second half of 2018. See Tech Accord, Facts & Figures, accessed 22 September 2020.

[453] Australian Communications and Media Authority, Internet of Things in media and communications – Occasional Paper, July 2020, p. 16.

[454] J Porter, Security researchers expose new Alexa and Google Home vulnerability, *The Verge*, 21 October 2019, accessed 22 September 2020.

[455] The Code of Practice comprises 13 principles. The Australian Government recommends industry prioritise the top three principles because action on default passwords, vulnerability disclosure and security updates will bring the largest security benefits in the short term. The Code of Practice will be reviewed on a regular basis to ensure it remains fit for purpose. See Department of Home Affairs, Code of Practice: Securing the Internet of Things for Consumers, September 2020, p. 1.

[456] The potential for lock-in derives from both the lack of compatibility between devices with different ecosystems as well as consumers' preference to stay within one ecosystem for convenience and efficiency.

[457] PWC, Consumer Intelligence Series: Prepare for the voice revolution, 2018, p. 7.

At present, device manufacturers must choose a protocol (such as Apple Home Kit, Google Weave, Amazon Alexa Smart Home) and voice assistant to support their device.[458] Some devices may support multiple protocols/voice assistants, such as Sonos smart speakers (compatible with Amazon and Google).

Additionally, in 2020 Sonos reportedly alleged that despite its patented technology to allow two voice assistants to work alongside each other, Google and Amazon have required Sonos to make users select one assistant when setting up their speaker. However, Amazon reportedly denied this and reportedly later changed its position and joined an alliance with Sonos and other companies, to make virtual assistants function together.[459]

There are reports of industry initiatives to improve compatibility of smart home devices by implementing an open standard, to make it easier for device manufacturers to build devices that are compatible with different ecosystems.[460] Amazon, Apple and Google are reportedly involved with this, but at present, if consumers want to use a particular device, they are generally required to adopt a particular platform ecosystem.

### *Increasing consumer preferences for voice search may entrench position of existing platforms*

As consumers engage more with voice assistants on smartphones, wearables and smart speakers particularly, search queries are increasingly likely to be undertaken using the voice assistant. In the future, the ability to provide high-quality results for voice activated search may become a more important parameter of competition in the supply of search services more generally.

Voice activated searches differ to text searches, and tend to be more location-specific, including phrases like 'near me' or 'close by',[461] placing more emphasis on the ability of a search provider to provide results of this nature. In the event a search engine provider does not offer reliable and useful responses to voice assistant search queries, it may impact its competitive position in markets for connected devices and voice assistants.

Google has several advantages in providing voice activated search services. It has broad access to location data, by virtue of its Android operating system on smartphones, and the prevalence of Google Maps, which could help improve the quality of search results. Google Search is also the default provider of web searches for both Google Assistant and Apple's Siri,[462] whereas Amazon's Alexa uses Bing.[463]

As Google provides the search services for both default voice assistants on Android and Apple smartphones, it is likely to have a significant share of voice activated search services. This may give Google a competitive advantage in this market (similar to its position in the general search services market) and creates a risk that Google could extend its dominance in search into broader markets for connected devices and voice assistants. Smart device services like voice assistants is one area that will be explored in the EC's antitrust competition inquiry into the consumer IoT.[464]

---

458 M Simon, Alexa, Siri and Google Assistant might soon all speak the same smart home language, *Tech Hive*, 18 December 2019, accessed 22 September 2020.

459 J Nicas and D Wakabayashi, Sonos, Squeezed by the Tech Giants, Sues Google, *The New York Times*, 7 January 2020, accessed 22 September 2020.

460 Project Connected Home over IP, accessed 22 September 2020.

461 A Oziemblo, Why You Should Optimize For Voice Search Now To Stay Ahead Of Your Competition, *Forbes*, 16 October 2019, accessed 22 September 2020.

462 M Panzarino, Apple switches Bing to Google for Siri web search results on iOS and Spotlight on Mac, *Tech Crunch*, 26 September 2017, accessed 22 September 2020.

463 C Pitt, Voice search optimisation for Alexa, Siri and Cortana, *The Drum*, 5 March 2019, accessed 22 September 2020.

464 European Commission, Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT), Press Release, 16 July 2020.

### *Increasing availability and use of voice commerce may impact consumer choice*

Another way consumers are increasingly using voice assistants and connected devices is to interact with companies[465], including to make purchases.[466]

Voice assistants on connected devices that have access to relevant personal data of users are well placed to make relevant personalised recommendations. However, there is potential to distort competition if voice assistants preference one brand over another, such as their own brand or a sponsored brand. Such a practice may also reduce consumer choice and welfare, particularly if users are only presented with one search result, and they are unaware they are being recommended a sponsored product.

For example, at the United States House of the Judiciary Antitrust Subcommittee hearing in July 2020, Amazon CEO Jeff Bezos stated that:

> *'…I'm sure there are cases where we do promote our own products, which is of course a common practice in business, so it wouldn't surprise me if Alexa sometimes does promote our own products.'* [467]

This statement follows a 2017 test by researchers Bain and Co, which found that in categories where Amazon offered a private-label product, Alexa recommended those products 17 per cent of the time, where these goods only represented about 2 per cent of total volume sold.[468] Bain and Co also found that Alexa did not disclose product listings as sponsored and according to the New York Times, Alexa allegedly only offered consumers one option when they asked Alexa to 'buy batteries' (an Amazon branded product).[469]

Brands may also collaborate with platforms to make it easier for customers to place verbal orders using voice assistants. While convenient for consumers, this may also limit consumer choice if only affiliated products are recommended and may disadvantage brands who do not have access to such a partnership.[470]

---

465 Research conducted by Capgemini found that around a quarter of respondents would rather use a voice assistant than a website in 2018. In the next three years, this is expected to increase to 40 per cent. See Capgemini, Voice assistants set to revolutionize commerce and become a dominant mode of consumer interaction in the next three years, 11 January 2018, accessed 22 September 2020.

466 Deloitte's Media Consumer Survey 2019 found that 29 per cent of respondents reported that making purchases was their most highly valued use of voice. See Deloitte, Media Consumer Survey 2019, 2019, p. 14.

467 G Fowler, The 5 biggest little lies tech CEOs told Congress — and us, *The Washington Post*, 30 July 2020, accessed 22 September 2020. For unofficial transcript, see Rev, Big Tech Antitrust Hearing Full Transcript July 2019, 29 July 2020, accessed 22 September 2020.

468 A Cheris, D Rigby and S Tager, Dreaming of an Amazon Christmas?, *Bain and Company*, 9 November 2017, accessed 22 September 2020.

469 J Creswell, How Amazon Steers Shoppers to its Own Products, *The New York Times*, 23 June 2018, accessed 22 September 2020.

470 For example, Nike partnered with Google Assistant in the United States to supplement TV ads shown during NBA games, which encouraged consumers to 'Ask Google' about limited edition basketball shoes. See E Hal Schwartz, Nike Voice Sale for Sneaker Launch Runs Away with Cannes Lions Awards, voicebot.ai, 1 July 2019, accessed 22 September 2020; D LaRue, The First Voice-Activated Sneaker Drop, RAIN, accessed 22 September 2020.

## 6.3. New products and services, including augmented and virtual reality offered by platforms

- **Online private messaging, social media and search platforms are increasingly offering services using augmented and virtual reality technology. While these may bring positive experiences for consumers, consumer harms can result from increasing data collection by these services.**

Augmented and virtual reality technology offer consumers the ability to combine digital and physical experiences. The applications and services made possible by this technology continue to become more available and accessible to consumers, driven in part by device improvements and advancements in supporting networks, such as 5G mobile networks.

Augmented reality (AR) technology uses the existing environment and overlays new information on top of it, to experience existing reality in a heightened way.[471] It uses computer vision, simultaneous localisation, mapping and depth tracking (sensor data calculating distance to objects), which allows cameras to collect, send and process data to show digital content relevant to what the user is looking at.[472] Smartphones are a common consumer platform for AR applications and features.[473] Some examples of AR experiences are discussed in part 6.3.1.

Virtual reality (VR) technology offers a digital recreation of a real life setting, and replicates a real or imagined environment. It is a completely immersive, multi-sensory experience that blocks out the real world so users are unaware of the environment around them. VR requires the user to have specialist equipment, such as a VR headset.[474] Some examples of VR experiences are discussed in part 6.3.2.

According to a Juniper Research forecast, mixed reality apps (those that have AR or VR features) will more than quintuple their advertising revenue to $11 billion by 2024 (from $2 billion in 2019), as they reach audiences with more engaging mobile experiences. Social media platforms, like Facebook and Snapchat, are expected to drive much of the growth in mixed reality downloads and ad spending.[475]

AR and VR technologies facilitate the collection of vast user and non-user data depending on the application or service, and there is potential for consumer harm if this data is misused, as discussed in part 6.3.3.

### 6.3.1. Augmented reality experiences

AR features can bring benefits to consumers including entertainment, convenience and enhancing existing features of online private messaging, social media and search

---

471 S Kanuganti, Augmented reality benefits us all, *Forbes*, 16 August 2019, accessed 22 September 2020.

472 AR can be implemented in a number of ways, such as by using simultaneous localisation and mapping technology, using complex algorithms and data from sensors; image recognition through a camera that detects a predefined marker and triggers particular computer generated content, and by using GPS data and the compass, accelerometer and gyroscope built into a mobile phone to trigger geolocation based markers.

473 The anticipated high throughput speeds and low latency made possible by 5G networks will facilitate better quality AR experiences, and may see an increase in take-up by more platforms and users.

474 Deloitte, How much is that virtual doggie in the virtual window? Virtual and augmented reality – a guide for Australian retailers, 2017, p. 6.

475 R Williams, Mixed reality apps will quintuple ad revenue to $11B by 2024, study says, *Mobile Marketer*, 12 November 2019, accessed 22 September 2020.

services.[476] Deloitte reports AR use on mobile devices has nearly doubled since 2018, with usage and popularity largely driven through social media.[477]

### *Use of AR in advertisements on social media platforms*

AR is increasingly being used in advertising on platforms, particularly in the United States. Google, Facebook, Instagram and Snapchat all offer the ability for AR use in advertisements, which enable users to interact with the product they are browsing. Snap Inc. (owner of Snapchat) reportedly expects significant potential revenue to come from AR advertisements, and is reportedly focusing on scaling its platform to make AR more personalised and to help the company make money from the technology.[478]

This type of advertising typically seeks to use a consumer's image to interact or 'try on' products on a search or social media platform. For example, YouTube has an 'AR Beauty Try-On' feature, which lets viewers virtually try on makeup while following along with a YouTube creator. Brands are able to partner with YouTube creators as part of an advertising campaign.[479]

In addition to offering similar 'try-on' features of products using AR, Instagram and Snapchat have also introduced the option for users to purchase the item they are browsing by clicking a button in the ad.[480] Some examples of these features are shown in figure 6.8 below, noting some may be limited to the United States at this time.

Another type of advertising, predominately used by Snapchat, involves using consumer images and allowing users to overlay an advertiser's logo or product on their photo as a filter. Advertisers may pay platforms for sponsored lenses that are available for a specific period of time, [481] as shown in figure 6.9. TikTok also launched an AR advertising product that allows users to add interactive visual effects from advertisers to their video that interact with the physical environment around them.[482]

---

476 For example, Facebook Messenger, Instagram and Snapchat users can add various filters to a photo or video taken through the app and in Google Search, users can view and interact with 3D objects from the Search page and place them directly into the real world, to give a sense of scale and detail. Google also offers an AR feature in Google Maps 'Live View' where arrows and directions are placed in the real world to guide a user and better identify directions. See Google, Experience 3D & augmented reality in Search, Google Search Help, accessed 22 September 2020; Google, Introducing Live View, the new augmented reality feature in Google Maps, Google Maps Help, 9 August 2019, accessed 22 September 2020.

477 A V Cook, L Ohri and L Kusumoto, Augmented shopping: The quiet revolution, *Deloitte Insights*, 10 January 2020, accessed 22 September 2020.

478 A Carman, Snap is slowly growing, but it's banking on augmented reality to sustain it, *The Verge*, 22 October 2019, accessed 22 September 2020.

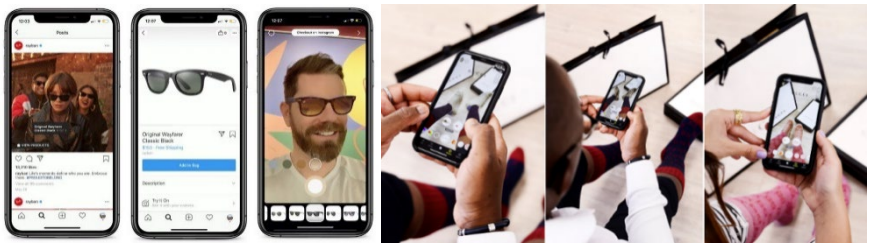
479 A Luber, Immersive branded experiences in YouTube and display ads, Google Marketing Platform, 18 June 2019, accessed 22 September 2020.

480 These features may be limited to some brands depending on the platform. See A Hutchinson, Snapchat Launches New Shoppable AR 'Try-On' Campaign with Gucci Shoes, *Social Media Today*, 29 June 2020, accessed 22 September 2020; R Stewart, Snapchat has launched an in-app AR shopping, with Adidas and Coty among the first sellers, *The Drum*, 18 April 2018, accessed 22 September 2020; K Bell, Instagram now lets you shop with augmented reality, 4 October 2019, *Mashable Australia*, accessed 22 September 2020

481 R Williams, Mixed reality apps will quintuple ad revenue to $11B by 2024, study says, *Mobile Marketer*, 12 November 2019, accessed 22 September 2020.

482 L O'Reilly, TikTok is coming after Snapchat with a new augmented reality ad format, *Digiday*, 8 May 2020, accessed 22 September 2020.

**Figure 6.8: Examples of AR shoppable ads on Instagram and Snapchat**



Source: Instagram via K Bell, Instagram now lets you shop with augmented reality, 4 October 2019, *Mashable Australia*, accessed 22 September 2020. A Hutchinson, Snapchat Launches New Shoppable AR 'Try-On' Campaign with Gucci Shoes, *Social Media Today*, 29 June 2020, accesssed 22 September 2020.

**Figure 6.9: Example of sponsored Lens on Snapchat**

Source: Image available on C Francis, Win the Battle of Attention in 3 Easy Steps with Snapchat's Geofilters, *ETRAFFIC Web Marketing*, 24 March 2016, accessed 22 September 2020.

There is potential for reduced consumer welfare if consumers are unaware they are being subjected to or engaging with advertising, particularly given the immersive nature of AR ads. A survey conducted by Boston University found that most people could not tell native advertising apart from an actual news article.[483] This confusion could be exacerbated as native and display advertising offerings increasingly include AR features.[484]

## *AR consumer wearables*

An evolving trend is the use of AR in consumer wearables, such as smart glasses, which are typically a transparent device that generates AR content within the scene of a consumer's viewpoint. A consumer can see their physical surroundings in the same way as normal glasses, but can superimpose content onto their view. An early example of this technology was Google Glass, however, advances in technology are driving development of newer devices.[485]

In particular, several platforms are developing consumer AR smart glasses in house, through acquisition or partnerships. This includes Snapchat (which has integrated AR in its third-generation Spectacles glasses), [486] Alphabet Inc. (Google) (which has acquired a Canadian

---

483 K J Mcalpine, Fewer than one in 10 people can distinguish online sponsored content from news articles, Boston University, 1 February 2019, accessed 22 September 2020.

484 For example, Verizon Media has introduced AR features to its 'Moments' native ad format. See Verizon, Verizon Media expands successful native ad format with AR, Press Release, 23 September 2019.

485 M Sawh, The best AR glasses and smartglasses 2020: Snap, Vuzix and more, *Wareable*, 1 July 2020, accessed 22 September 2020

486 These come with an added camera so users can overlay AR effects on their content to upload to Snapchat. See C Newton, Snap announces Spectacles 3 with an updated design and a second HD camera, *The Verge*, 13 August 2019, accessed 22 September 2020.

smart glasses start-up, 'Focals by North')[487], Amazon (through services including Vuzix—see figure 6.10)[488] and Facebook.[489]

**Figure 6.10: Example of view through Vuzix Blades**


Source: Image available on C Fink, First Impressions of the New Vuzix Blade AR Glasses, *Forbes*, 3 January 2019, accessed 22 September 2020.

In addition to Facebook's hardware partnerships, it is also reported to be working on wearable sensors that can detect simple words when people think them, which could be used to control the smart glasses.[490]

### 6.3.2. Virtual reality experiences

In recent years, consumer VR experiences have typically focused on gaming, however there is a growing shift towards broader applications and services, including educational tools and retail experiences. This is facilitated by improvements to device technology making them more accessible and affordable for consumers, and improvements to networks (such as 5G mobile networks) to enhance their ability to support the speeds and latency needed for VR applications, which may enable a higher quality experience.[491]

Some platforms continue to invest and develop new VR applications. Facebook, for example, intends to launch a new VR social platform—Facebook Horizon—that will be accessible through Oculus headsets.[492] CSS Insights estimates that market demand for VR devices will grow sixfold over the coming years from 10 million units in 2019 to 60 million units in 2023.[493]

### 6.3.3. Potential concerns with AR and VR technologies

#### *Privacy and security concerns*

The more immersive nature of AR and VR technologies may create greater risk of consumer identity theft or fraud. A 2019 European Data Protection Supervisor Technology report on

---

487 R Osterloh, Our focus on helpful devices: Google acquires North, *The Keyword (Google Blog)*, 30 June 2020, accessed 22 September 2020.

488 Amazon has also partnered with Vuzix to integrate Alexa into Vuzix's Blade AR smart glasses, in addition to launching its own smart glasses 'Echo Frames', which do not incorporate AR at this stage. See N Statt, Vuzix Blade AR glasses are the next-gen Google Glass we've all been waiting for, *The Verge*, 9 January 2018, accessed 22 September 2020; Amazon, Echo frames, accessed 22 September 2020.

489 Facebook is reportedly working with Luxottica (the owner of Ray-Ban and Oakley) on a pair of AR smart glasses, which would allow users to take calls, project information to the wearer with a small display, access a voice assistant with AI, and livestream the wearer's viewpoint on social media sites in real time. See S Rodriguez, Facebook working on smart glasses with Ray-Ban, code-named 'Orion', *CNBC*, 17 September 2019, accessed 22 September 2020.

490 Facebook, Imaging a new interface: Hands-free communication without saying a word, *Tech@Facebook,* 30 March 2020, accessed 22 September 2020.

491 B Marr, The 5 Biggest Virtual and Augmented Reality Trends in 2020 Everyone Should Know About, *Forbes*, 24 January 2020, accessed 22 September 2020.

492 In this platform, users design their own avatars and are transported to public spaces and new worlds through portals. Users can play games and engage in multi-player experiences built by Facebook. See Oculus, Introducing 'Facebook Horizon,' a New Social VR World, Coming to Oculus Quest and the Rift Platform in 2020, Oculus Blog, 25 September 2019, accessed 22 September 2020.

493 M Koytcheva, VR and AR Market is Heating Up, *CCS Insight*, 3 December 2019, accessed 22 September 2020.

smart glasses and data protection outlined a number of potential privacy and security concerns with smart glasses including:

- Non-authorised recordings of data subjects' actions and activities of the device users and others in their view[494] and incorporation of facial or voice recognition systems and the collection and storage of users' metadata.[495]
- Security loopholes that can actively be exploited to steal data or run unauthorised software.[496]
- The trend in smart glasses design being indistinguishable from ordinary glasses increasing the risk of personal data of non-users being captured secretly and without effort.[497]

### *Wider collection of data points increases scope for hyper targeting*

AR and VR technologies facilitate the collection of vast user and non-user data depending on the application or service being used. In most cases, data collected may go beyond that which can be collected through everyday use of a social media or search service.

For example, AR filters, offered by various social media and online private messaging platforms may collect detailed information about a users' environment and location.[498] As detailed in Snap Inc.'s privacy policy, it collects a range of information from user device sensors such as accelerometers, gyroscopes, compasses, microphones, as well as location information, with user permission, about their precise location using methods including GPS, wireless networks, cell towers, and Wi-Fi access points.[499]

It is unclear however, whether these AR filters are able to collect biometric data, such as details of a users' face where they overlay images on a users' selfie. An ACCC review of Facebook[500], Google[501] and Snap Inc.'s[502] privacy policies found no specific reference to the collection of biometric data. However Snap Inc.'s policy referred to the use of 'object recognition' for its Lenses feature, an algorithm designed to help a computer generally understand what objects are in an image rather than recognising features of an individual's face.[503]

AR wearables, such as smart glasses, have the ability to collect constant user data through various sensors including cameras and microphones as they capture the worldview of the user. VR devices, such as headsets,[504] enable the collection of more personal user data including device movements, biometric tracking data (such as micro-movements of head,

---

494 As the sensors may record environmental information, including video streams of users' view field, audio recordings and localisation data. See European Data Protection Supervisor, Technology Report No 1 – Smart glasses and data protection, January 2019, p. 3.

495 European Data Protection Supervisor, Technology Report No 1 – Smart glasses and data protection, January 2019, p. 4.

496 European Data Protection Supervisor, Technology Report No 1 – Smart glasses and data protection, January 2019, p. 3.

497 European Data Protection Supervisor, Technology Report No 1 – Smart glasses and data protection, January 2019, p. 11.

498 Snapchat, Business Center – Lenses Specifications, accessed 22 September 2020.

499 Snap Inc., Privacy Policy, Effective 18 December 2019, accessed 22 September 2020.

500 Facebook's data policy also does not specifically reference biometric data but does reference its use of facial recognition technology—'If you have it turned on, we use face recognition technology to recognise you in photos, videos and camera experiences. The face recognition templates that we create may constitute data with special protections under the laws of your country'. See Facebook, Data Policy, accessed 22 September 2020.

501 Google's privacy policy does not include a specific reference to any biometric information beyond 'voice and audio information when you use audio features'. See Google, Privacy Policy, effective 21 March 2020, accessed 11 August 2020.

502 Snap Inc.'s privacy policy does not mention biometric data or facial recognition technology. See Snap Inc., Privacy Policy, Effective 18 December 2019, accessed 11 August 2020.

503 Snap Inc., Privacy by Product – Lenses, accessed 11 August 2020.

504 For example, Facebook's Oculus privacy policy states it collects information from users including information about the users' environment, physical movements and dimensions when they use an XR (extended reality) device, and information received through the device settings that the user chooses, such as photos or audio content. See Oculus, Oculus Privacy Policy, last updated 27 December 2019, accessed 22 September 2020.

hands, eyes) and information about a user's activities in an application.[505] One study estimated that a 20-minute VR gaming session could record 2 million data points.[506]

The detailed nature of data collected by various AR and VR applications and devices could be used to deliver 'hyper-targeted' advertising to a user, particularly given the potential for more extensive and accurate location data to be collected.[507] For example, Snap Inc. states it uses some information to tailor the user's Snapchat experience, based on where they are and what is happening around them, such as special lenses and filters for an event they are at.[508]

In December 2019, Facebook disclosed that data from Oculus VR activity will be used for advertising if a user has logged into their Facebook account on Oculus.[509] In August 2020, Oculus subsequently announced it will be removing support for separate Oculus accounts starting in October 2020, with first time users required to log in with a Facebook account to access full functionality with their Oculus device.[510] After 1 January 2023, Oculus will end support for separate Oculus accounts. Oculus will also be adopting Facebook's Community Standards, including a new VR-focused policy, which will replace Oculus' existing separate Code of Conduct.[511]

## 6.4. Potential for personalised pricing in online markets

- **Online markets can provide retailers with the information and technology to set different prices for different customers in a way that may not be as readily available to offline retailers.**
- **Personalised pricing may have the effect of making some consumers better off if they are charged lower prices based on their lower willingness to pay and are able to purchase more goods or services as a result.**
- **Personalised pricing has the potential to disadvantage consumers overall by reducing their share of the value or surplus created by market transactions. This could occur where firms are able to set personalised prices closer to consumers' maximum willingness to pay and where consumers have difficulty seeking better offers from alternative suppliers (for example if there are few suppliers). Personalised pricing may also raise concerns if it erodes trust between consumers and businesses, or disadvantages vulnerable consumers.**
- **While there is significant potential for personalised pricing online, to date there have been few studies into this practice in Australia and there is limited evidence of personalised pricing in Australia or internationally. However, the ACCC will continue to monitor pricing practices through the Digital Platform Services Inquiry.**

505 J Outlaw and S Persky, 'Industry review boards are needed to protect VR user privacy', World Economic Forum, 29 August 2019, accessed 22 September 2020.
506 J Bailenson, Protecting Nonverbal Data Tracked in Virtual Reality, *JAMA Pediatrics*, October 2018. See also here, accessed 22 September 2020.
507 F Cook, Augmented Reality, Advertising and Practical Legal Considerations, Kilpatrick, Townsend & Stockton LLP, 31 January 2019, p. 6.
508 Snap Inc., How we use your information, accessed 31 July 2020.
509 Oculus, Introducing new features from Facebook to help people connect in VR and an update to our privacy policy, Oculus Blog, 11 December 2019, accessed 22 September 2020.
510 Within their Facebook account, users will be able to create or maintain a unique VR profile. See Oculus, A single way to log into Oculus and unlock social features, Oculus Blog, 18 August 2020, accessed 22 September 2020.
511 Oculus, A single way to log into Oculus and unlock social features, Oculus Blog, 18 August 2020, accessed 22 September 2020.

### 6.4.1. Personalised pricing in online markets

Personalised pricing is the practice where businesses use information about individuals' conduct or characteristics to set different prices for different consumers based on what the business thinks they are willing to pay.[512] It is a form of price discrimination.

As noted by the CMA, the increasing availability of data and use of sophisticated pricing algorithms, particularly by online retailers, raises the possibility that such retailers would be able to engage in highly personalised pricing, effectively sorting customers into ever finer categories (to target with personalised prices).[513]

Despite the potential for personalised pricing, there has been limited evidence to date that these practices are widespread in Australia or overseas. This practice may attract greater scrutiny in the future as digital markets continue to expand.

Australian and overseas studies have found limited evidence of different prices being offered to different consumers, and even more limited evidence that these price differences are due to differences in consumers' willingness to pay. For example, one such study conducted in Australia is discussed in box 6.6.

However, some studies found more instances of product search results being ordered in a different way for different consumers (while prices remained the same across consumers). Although, they were also typically unable to identify whether the differences in product search results were the result of firms showing higher priced goods to consumers with a higher willingness to pay.[514]

**Box 6.6: Example of study in Australia**

In Australia, a 2020 investigation by Choice found that the online dating app Tinder charged different prices to consumers for their premium service Tinder Plus.

Using 60 mystery shoppers, Choice found that people over the age of 30 were offered prices that were more than double the prices of those aged under 30. It also found price variations within those age groups, however, Choice were unable to identify a pattern that could explain these price variations. Choice were also unable to ascertain how Tinder set prices.[515]

### 6.4.2. Role of platforms in personalised pricing

Platforms like Google, Amazon and Facebook have the ability to use their large collections of data about users to conduct profiling for commercial reasons, which can be used to influence consumer behaviour.[516]

---

512 Office of Fair Trading, Personalised Pricing - Increasing Transparency to Improve Trust, May 2013, p. 20.

513 In the extreme, the CMA noted that the outcomes of highly personalised pricing may approach those of perfect or 'first-degree' price discrimination, in which every customer is offered an individual price equal to their maximum willingness to pay. See Competition and Markets Authority, Pricing algorithms – Economic working paper on the use of algorithms to facilitate collusion and personalised pricing, 8 October 2018 p. 36.

514 Competition and Markets Authority, 'Pricing algorithms – Economic working paper on the use of algorithms to facilitate collusion and personalised pricing', 8 October 2018, p. 38. European Commission, Consumer market study on online market segmentation through personalised pricing/offers in the European Union, June 2018, pp. 93-94; A Hannak, G Soelle, D Lazar, A Mislove, and C Wilson, Measuring Price Discrimination and Steering on E-commerce web sites, 2014; Z Sheftalovich and G Smith, Online dating site and app reviews, CHOICE, 11 February 2020, accessed 11 August 2020.

515 E Turner, Op-ed: Tinder's secret pricing shows how companies use our data against us, CHOICE, 11 August 2020, accessed 22 September 2020; L Hobday, Older men charged more for using Tinder's premium service, Choice mystery shoppers find, ABC News, 12 August 2020, accessed 22 September 2020; S Jeong, Tinder charges older people more, CHOICE, last updated 11 August 2020, accessed 22 September 2020.

516 ACCC, DPI Final Report, 26 July 2019, pp. 445–446.

Google and Facebook currently offer remarketing (or retargeted)[517] and dynamic ad[518] services that could be used to personalise prices since these services allow promotional prices or discounts to be targeted at specific consumers based on their online behaviour and demographic data. For example, in search advertising, differential pricing may take the form of web coupons offered to some people but not others based on their behaviour and demographic data.[519] There is also potential for AI to be used to create personalised pricing based on data obtained through an individual's search or social media use.[520]

Furthermore, as search, social media and online private messaging platforms are progressively moving into e-commerce and offering retail products through their platforms, there is also potential for personalised pricing to occur on the platforms themselves.

While there is limited evidence of personalised pricing occurring in Australia, the OAIC's Australian Community Attitudes to Privacy Survey 2020 found that 79 per cent of Australians would consider it a misuse of their personal information if the tracking of their online activity led to a variation in the price of a good or service.[521]

### 6.4.3. Potential outcomes of personalised pricing and regulatory response

Personalised pricing has the potential to improve overall consumer welfare as, for example, it may result in firms reducing prices to consumers with a low willingness to pay, enabling efficient trades that may not have otherwise occurred. It can also benefit consumers where firms are able to target customers of other firms with more competitive price offers.

However, personalised pricing has the scope to disadvantage consumers overall. If done effectively, personalised pricing can result in the business 'appropriating' most of the value consumers would otherwise gain from the market transactions. This could occur where firms are able to set personalised prices closer to consumers' maximum willingness to pay and where consumers have difficulty seeking better offers from alternative suppliers. In particular, if consumers are unable to shop around they are unable to apply competitive pressure on firms to gain a greater share of the surplus from trade. This could occur if consumers have no or few alternative suppliers to switch to, or are less inclined or able to shop around for a better offer (for example, if they cannot easily or accurately compare offerings due to the presence of personalised pricing).[522]

International organisations have raised concerns that a lack of transparency around personalised pricing may lead to a reduction in consumer trust in online markets, and subsequently a reduction in online purchases.[523] Further, even if the overall benefit to consumers of price discrimination were positive, personalised pricing may still raise

---

517 This type of ad is shown to people who have previously visited a particular retail website but may have not completed a purchase, and intends to remind the consumer to return to the store, and encourage them to make a purchase. It is available on Facebook and Google ads. See C Ferreira, '19 Ways to use offers, coupons, discounts, and deals to generate more sales', Shopify Blog, 13 November 2019, accessed 22 September 2020.

518 This type of ad automatically shows products to consumers who have expressed interest on a retailer's website, app or elsewhere on the internet. For example, Facebook dynamic ads can promote a hotel ad on Facebook that matches the dates and destination a user may have been browsing but didn't make a booking. See Facebook, 'Dynamic Ads—Personalise your ads without the manual work', Facebook for Business, accessed 22 September 2020.

519 N Newman, 'How Big Data enables economic harm to consumers, especially to low-income and other vulnerable sectors of the population', p. 4.

520 For example, algorithms could predict the top price a consumer might pay for a product, and facilitate tailored pricing based on behaviours and preferences.

521 The Australian Community Attitudes to Privacy Survey 2020 found that 81 per cent of Australians consider an organisation asking them for personal information that doesn't seem relevant to the purpose of the transaction and recording information on the websites they visit without their knowledge to be a misuse. This is particularly the case if the tracking of online activity leads to the price of a good or service being varied (79 per cent). See OAIC, Australian Community Attitudes to Privacy Survey 2020, September 2020, p. 36.

522 Office of Fair Trading, The Economics of Online Personalised Pricing, May 2013.

523 Office of Fair Trading, Personalised Pricing - Increasing Transparency to Improve Trust, May 2013, p. 20.

concerns if the group who were disadvantaged by price discrimination were considered vulnerable.

There are a number of potential mechanisms, some discussed by the OECD, that may help avoid adverse consumer outcomes from price personalisation such as improving transparency so consumers are aware of and understand these pricing practices, and enabling and empowering consumers to compare alternative offers before purchasing.

In Australia, there is no provision in the *Competition and Consumer Act 2010* or the Australian Consumer Law (ACL) explicitly prohibiting price or product personalisation by retailers. However, in some circumstances price personalisation may have the potential to raise issues under the ACL such as where there are representations or expectations set by an ordinary and reasonable consumer that those visiting a particular website will be offered the same prices for the same products, or shown the same product lines on each screen throughout the on-line session at that retailer.[524]

The ACCC will continue to monitor pricing practices throughout the Digital Platform Services Inquiry where there is potential for issues under the ACL as well as to understand personalised pricing behaviour more generally as digital markets continue to evolve.

[524] The ACCC's Digital Platforms Inquiry and Customer Loyalty Schemes Review recommended strengthening personal data protection regulation across the economy (under the Privacy Act) and with digital platforms (through a specific Code). The Australian Government's Response to the Inquiry in December 2019 supported or supported in principle these recommendations, indicating actions to be undertaken in 2020.

# 7. International regulatory proposals and developments

Internationally, governments and regulators are increasingly focusing on the role and practices of digital platforms and developing a better understanding of the market dynamics to proactively identify any potential issues that could give rise to competition concerns or consumer harms.

The global nature of services offered by large platforms gives rise to similar competition and consumer protection issues across different jurisdictions. Some of the key issues identified include the ability of large digital platforms with market power to act as 'gatekeepers' between businesses and their prospective customers, the practice of large digital platforms acquiring smaller businesses or platforms in adjacent markets or acquiring a nascent competitor, and the introduction of new features and functionality that closely resemble those of competitors.

Many of these issues were discussed in the July 2020 United States House of the Judiciary Antitrust Subcommittee hearing 'Examining the Dominance of Amazon, Apple, Facebook and Google'. This included, for example, Facebook's acquisition of Instagram, with documents gathered through the Subcommittee's investigation showing that Facebook viewed the then nascent Instagram as a competitive threat and sought to acquire it.[525]

While common concerns have been identified, a variety of proposals have been put forward to address some of these key issues, as shown in the examples outlined in box 7.1.

For a more detailed discussion of regulatory proposals and developments, see appendix G.

**Box 7.1: Common issues and proposals by international regulators and lawmakers**

**Ensuring a level-playing field in digital markets**

Market imbalances caused by large digital platforms acting as gatekeepers and the importance of ensuring a level playing field are one set of a broader range of issues that the European Commission is exploring in its proposed Digital Services Act package.[526] Additional rules on platforms of a certain scale aimed at preventing self-preferencing and/or tailored obligations for specific gatekeepers regarding data access and/or interoperability are also being considered.

In the UK, the Furman Report proposed an enforceable code of conduct to apply to platforms with 'strategic market status' (likely to be 'gatekeepers') which would seek to complement existing competition law with an easily applied set of standards which can resolve disputes and enforce solutions rapidly.[527] The CMA's report into Digital Platforms and Online Advertising[528] supported this finding.

Governments across the world have also recognised the need for greater transparency and fairness in the dealings between large platforms and business users and have looked to address these concerns with ex ante regulation. In the European Union, the recent Platform-to-Business (P2B) Regulation places obligations on large platforms to create a fair and transparent business

---

525 Email produced to the House Committee on the Judiciary hearing on 'Online Platforms and Market Power: Examining the Dominance of Amazon, Apple, Facebook and Google' - Email from Mark Zuckerberg to David Ebersman, accessed 22 September 2020.

526 European Commission, Commission launches consultation to seek views on Digital Services Act package, Press Release, 2 June 2020.

527 Digital Competition Expert Panel, Unlocking digital competition, March 2019, p. 9 and pp. 59–63.

528 Competition and Markets Authority, Online platforms and digital advertising – Market study final report, 1 July 2020, p. 336.

environment, and similar legislation is being adopted or considered in Japan529 and South Korea.530

**Increasing scrutiny of platforms' acquisitions**

There is growing acknowledgement and concern about the perceived and actual difficulties faced by competition authorities in scrutinising and, where required, blocking anti-competitive acquisitions by major digital platforms. In particular, there are challenges when the target is a nascent competitor and its activities do not directly overlap with the platform.

In response to these concerns, many international jurisdictions have put in place or are considering merger law reform in order to ensure increased scrutiny on acquisitions by large digital platforms. Regulators are considering reforms to both *which* transactions are reviewed as well as *how* they will be reviewed. For example, new thresholds have been introduced in some countries to specifically deal with the concern of large technology businesses buying smaller innovative businesses with low or no turnover. Additionally, in a number of countries, there are proposals or current law requiring large digital platforms to notify the competition regulator of all their intended acquisitions regardless of value or market impact.[531]

In Australia, following the Australian Government's response to Recommendation 2 of the ACCC's Digital Platforms Inquiry[532], the ACCC is working towards a merger notification protocol, which is subject to negotiation between the ACCC and large digital platforms. As set out in the Digital Platforms Inquiry, these protocols would require each platform to provide the ACCC with information in advance on certain proposed acquisitions.[533]

**Developing expertise and understanding of digital markets**

Digital markets are dynamic and complex. To enhance their expertise, many governments and regulators have undertaken reviews into various digital markets to develop a better understanding of the market dynamics and proactively identify any potential issues that could give rise to competition concerns or consumer harms.[534] Specialist digital markets units are also being established or proposed in many jurisdictions in recognition of the ongoing need to monitor these markets.

In addition to the ACCC's Digital Platforms Branch, the Japanese Government has established a Headquarters for Digital Market Competition. The Federal Trade Commission has a Technology Enforcement Division and both the Furman Report and the CMA's Report into Online Platforms and Digital Advertising recommended the creation of a Digital Markets Unit to focus on delivering pro-competitive outcomes and delivering the recommendations outlined in those reports.[535]

A 'Digital Economy Unit' has also been announced in France, as well as taskforces or units looking at aspects of antitrust policy and enforcement in digital markets being contemplated or established in Austria, Portugal and South Korea.[536]

Noting the developments in box 7.1 and as detailed in appendix G, there are a range of regulatory proposals and developments being considered across different countries. The impact of these newly implemented developments or draft proposals on competition and consumer concerns will be observed over time.

---

529 T Dokei, H Nakajima and T Onki, Bill for Improving Transparency and Fairness of Digital Platforms, White & Case, 7 February 2020, accessed 22 September 2020.

530 K Jae-Heun, 'KFTC drafts policy to prevent platform monopolies', *The Korea Times*, 29 June 2020, accessed 22 September 2020.

531 See appendix G for examples of these proposals and changes.

532 Australian Government, Regulating in the digital age – Government response and implementation roadmap for the Digital Platforms Inquiry, 12 December 2019, p. 15.

533 ACCC, DPI Final Report, 26 July 2019, p. 30.

534 For example, in November 2019, the Swedish Competition Authority commenced a sector inquiry into digital platforms, across various markets to understand platforms' influence on market structure and competition, and identify potential regulatory reforms. See P Torbol et al, Swedish Sector Inquiry into Digital Platforms, K&L Gate, 8 November 2019, accessed 22 September 2020.

535 In March 2020, a temporary Digital Markets Taskforce (led by the CMA) was established to advise the UK Government.

536 A Bavasso, L Tolley and J Bowring, UK sets up new digital markets taskforce, Allen & Overy, 13 March 2020, accessed 22 September 2020.

The identification and existence of similar competition and consumer protection issues across international jurisdictions presents an opportunity for regulators and lawmakers to work together to develop effective solutions. While different jurisdictions may take different approaches, there may be benefits from collaboration and learning from each other's experiences to help develop fit-for-purpose measures that suit each individual jurisdiction.

The ACCC will continue to proactively monitor regulatory developments and responses by platforms to understand the impact on competition and consumer outcomes in digital markets. In particular, we will observe the extent to which a new regulation or law in one jurisdiction results in positive competition and consumer outcomes in another jurisdiction.

The ACCC recognises there is an ongoing opportunity for regulators to learn from each other and collaborate across international jurisdictions to address common challenges in digital markets. A collaborative approach may bring more benefits if it reduces the risk of disjointed markets, where competition and/or consumer issues are exacerbated in some jurisdictions but not others (for example, if platforms respond differently to regulations in different jurisdictions). A fragmented international approach to regulation may also impose a greater regulatory burden and costs on platforms, which could create additional competition and consumer harms.

As the European Commission, Executive Vice-President, Margrethe Vestager expressed:

> *…it is unrealistic to expect that there will be a precise, one-size-fits-all solution to address the range of issues that digital platforms present. Having said that, if we can formulate appropriate policy responses around the world on the basis of shared experiences and knowledge and if possible, common visions, I consider that that can only be beneficial, both for citizens and businesses.* [537]

Accordingly, the ACCC will continue to proactively engage with international regulators to identify and where needed, work collaboratively to address similar issues and challenges raised by platforms and markets.

---

[537] M Vestager, Statement by Margrethe Vestager to Committee on the Judiciary, Subcommittee on Antitrust, Commercial and Administrative Law, p. 8.

# Appendix A: Ministerial direction

**Competition and Consumer (Price Inquiry—Digital Platforms) Direction 2020**

I, Josh Frydenberg, Treasurer, give the following direction to the Australian Competition and Consumer Commission.

Dated: 10 February 2020

Josh Frydenberg
Treasurer

Authorised Version F2020L00130 registered 14/02/2020

# Contents

# Part 1—Preliminary

## 1 Name

This instrument is the *Competition and Consumer (Price Inquiry—Digital Platforms) Direction 2020*.

## 2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

**Commencement information**

| Column 1 | Column 2 | Column 3 |
|---|---|---|
| **Provisions** | **Commencement** | **Date/Details** |
| 1. The whole of this instrument | The day after this instrument is registered. | |

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

## 3 Authority

This instrument is made under the *Competition and Consumer Act 2010*.

## 4 Definitions

Note: Expressions have the same meaning in this instrument as in the *Competition and Consumer Act 2010* as in force from time to time—see paragraph 13(1)(b) of the *Legislation Act 2003*.

In this instrument:

***Australian law*** means a law of the Commonwealth, a State, or a Territory (whether written or unwritten).

***data broker*** means a supplier who collects personal or other information on persons, and sells this information to, or shares this information with, others.

***digital content aggregation platform*** means an online system that collects information from disparate sources and presents it to consumers as a collated, curated product in which users may be able to customise or filter their aggregation, or to use a search function.

***digital platform services*** means any of the following:

(a) internet search engine services (including general search services and specialised search services);

(b) social media services;
(c) online private messaging services (including text messaging; audio messaging and visual messaging);
(d) digital content aggregation platform services;
(e) media referral services provided in the course of providing one or more of the services mentioned in paragraphs (a) to (d);
(f) electronic marketplace services.

***electronic marketplace services*** means a service (including a website, internet portal, gateway, store or marketplace) that:
(a) facilitates the supply of goods or services between suppliers and consumers; and
(b) is delivered by means of electronic communication; and
(c) is *not* solely a carriage service (within the meaning of the *Telecommunications Act 1997*) or solely consisting of one of more of the following:
(i) providing access to a payment system;
(ii) processing payments.

***exempt supply*** has the meaning given by subsection 95A(1) of the Act.

***goods*** has the meaning given by subsection 95A(1) of the Act.

***inquiry*** has the meaning given by subsection 95A(1) of the Act.

***services*** has the meaning given by subsection 95A(1) of the Act.

***State or Territory authority*** has the meaning given by subsection 95A(1) of the Act.

***supply*** has the meaning given by subsection 95A(1) of the Act.

***the Act*** means the *Competition and Consumer Act 2010*.

# Part 2—Price inquiry into supply of digital platform services

## 5 Commission to hold an inquiry

(1) Under subsection 95H(1) of the Act, the Commission is required to hold an inquiry into the markets for the supply of digital platform services. The inquiry is *not* to extend to any of the following:

(a) the supply of a good or service by a State or Territory authority;

(b) the supply of a good or service that is an exempt supply;

(c) reviewing the operation of any Australian law (other than the Act) relating to communications, broadcasting, media, privacy or taxation;

(d) reviewing the operation of any program funded by the Commonwealth, or any policy of the Commonwealth (other than policies relating to competition and consumer protection).

(2) For the purposes of subsection 95J(1), the inquiry is to be held in relation to goods and services of the following descriptions:

(a) digital platform services;

(b) digital advertising services supplied by digital platform service providers;

(c) data collection, storage, supply, processing and analysis services supplied by:

(i) digital platform service providers; or

(ii) data brokers.

(3) Under subsection 95J(2), the inquiry is not to be held in relation to the supply of goods and services by a particular person or persons.

## 6 Directions on matters to be taken into consideration in the inquiry

Under subsection 95J(6) of the Act, the Commission is directed to take into consideration all of the following matters in holding the inquiry:

(a) the intensity of competition in the markets for the supply of digital platform services, with particular regard to:

(i) the concentration of power in the markets amongst and between suppliers; and

(ii) the behaviour of suppliers in the markets, including:

(A) the nature, characteristics and quality of the services they offer; and

(B) the pricing and other terms and conditions they offer to consumers and businesses; and

Example: Terms and conditions relating to data collection and use.

(iii) changes in the range of services offered by suppliers, and any associated impacts those changes had or may have on other markets; and

(iv) mergers and acquisitions in the markets for digital platform services; and

(v) matters that may act as a barrier to market entry, expansion or exit, and the extent to which those matters act as such a barrier;

(b) practices of individual suppliers in the markets for digital platform services which may result in consumer harm, including supplier policies relating to privacy and data collection, management and disclosure;

(c) market trends, including innovation and technology change, that may affect the degree of market power, and its durability, held by suppliers of digital platform services;

(d) changes over time in the nature of, characteristics and quality of digital platform services arising from innovation and technological change;

(e) developments in markets for the supply of digital platform services outside Australia.

### 7 Directions as to holding of the inquiry

(1) Under subsection 95J(6) of the Act, the Commission is directed to do the following in holding the inquiry:

(a) regularly monitor the markets for the supply of digital platform services for changes in the markets, particularly focussing on the matters referred to in section 6 of this instrument; and

(b) give to the Treasurer an interim report on the inquiry by 30 September 2020, and then further interim reports every 6 months thereafter, on:

(i) any changes observed by the Commission in the markets since the last report; and

(ii) any other matter, within the scope of the inquiry, the Commission believes appropriate.

(2) Under subsection 95P(3) of the Act, the Commission is directed not to make available for public inspection, copies of any interim report until the Treasurer, in writing, authorises the Commission to do so.

### 8 Period for completing the inquiry

For the purposes of subsection 95K(1) of the Act, the inquiry is to be completed, and a report on the matter of inquiry given to the Treasurer, by no later than 31 March 2025.



Authorised Version F2020L00130 registered 14/02/2020

# Appendix B: Update on market power assessment in search, social media, search advertising and display advertising services

***Search and search advertising***

- **Google continues to have substantial market power in general search. Further, Google is one of only two suppliers of upstream search services (supplied also by Bing) in which there are considerable economies of scale. This provides Google and Bing with a degree of bargaining power in their dealings with downstream search engines. Google also continues to have substantial market power in the supply of search advertising.**

***Social media and display advertising***

- **Facebook continues to have substantial market power in social media and the overall supply of display advertising.**

This appendix provides a more detailed analysis of the ACCC's market power assessment of the supply of general search, social media, search advertising and display advertising in Australia, since the publication of the DPI Final Report.

The ACCC notes that the market shares listed in this report are the ACCC's best estimates, based on information from a number of sources. Where the ACCC has requested information from firms on advertising revenue, it has done so on the basis of the revenue received from advertisers in Australia. This may include some portion of expenditure that is spent by Australian advertisers targeted at users located outside Australia. Conversely, it does not include expenditure by advertisers located overseas that is targeted at users in Australia. As with all estimates, there is a potential that this may under or overstate the actual market share of each firm or the total size of the market.

## B.1 Search services

As discussed in the DPI Final Report, there are two types of online search services.[538] The first is general search that are supplied in Australia by, for example, Google, Bing, Yahoo and DuckDuckGo. The second is specialised search, which provide answers to search queries related to particular sectors, such as retail, travel and e-commerce. There are large range of suppliers in this latter category in Australia, including Amazon, Expedia and eBay.

The ACCC remains of the view that there is limited substitutability between generalised search and specialised search and that Google continues to have substantial market power in general search services.

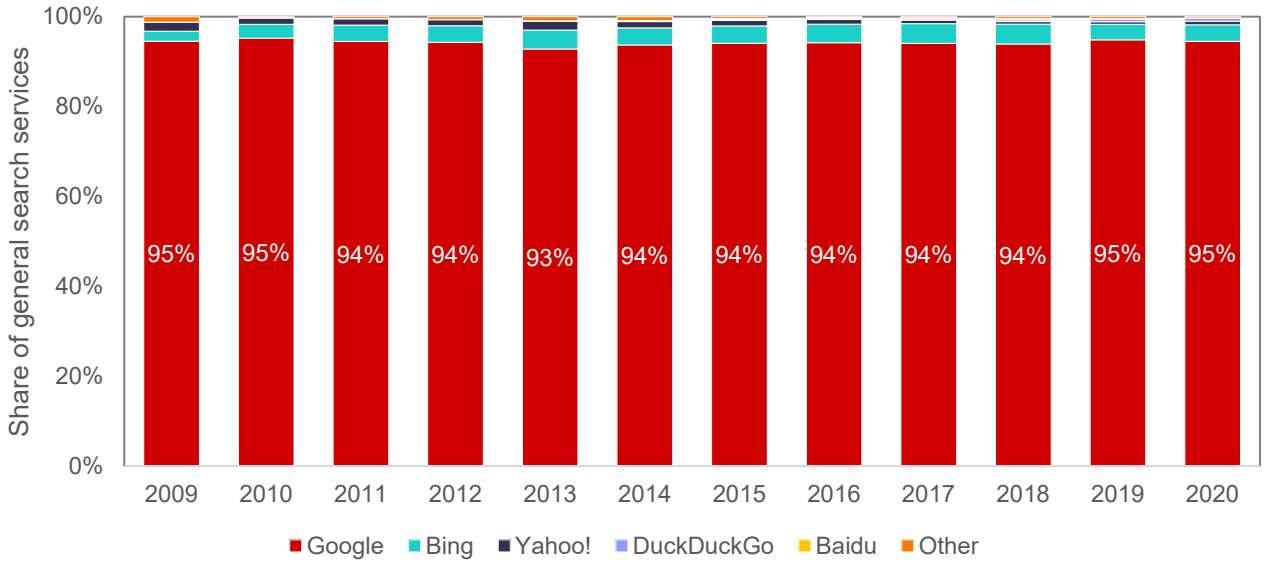
While the ACCC briefly considers some suppliers of specialised search in this report, it has not undertaken a market power assessment of specialised search services. However, some specialised search will be subject to examination as part of the ACCC's interim reports in the Inquiry; for example, the ACCC will consider Amazon in more detail in its analysis of electronic marketplaces.

[538] ACCC, DPI Final Report, 26 July 2019, p. 64.

### B.1.1 Google's market share in general search

Following from the findings in the DPI Final Report, Google has maintained its large share of the supply of general search in Australia.[539] As indicated by figure B.1 below, Google's share of the market for general search remains between 93-95 per cent since 2009.

**Figure B.1: Market share of general search services in Australia**




Source: Statcounter, Search engine market share, accessed 17 September 2020.

Of the remaining search engines, Bing is the only search engine to have a market share of more than 1 per cent despite usage growth in other search engines, such as DuckDuckGo since 2019 (see chapter 1 for discussion of DuckDuckGo's growth).

The remainder of this section discusses:

- the competitive constraints posed by search engines that rely on syndicated links from either Google or Bing, to provide search results to consumers, and
- Google's role in specialised search.

#### *Competitive constraints posed by search engines reliant on syndicated search results*

As discussed in the DPI Final Report, a potential new entrant to the market for general search, or a small-scale competitor of Google, is likely to face several barriers to entry and/or expansion, including economies of scale.[540] Search platforms enjoy considerable economies of scale[541], given the substantial fixed costs faced by search platforms and the low marginal cost of additional users of search platforms. In particular, there appear to be

---

539 ACCC, DPI Final Report, 26 July 2019, p. 65.

540 ACCC, DPI Final Report, 26 July 2019, pp. 66–73. These include same-side network effects arising from data accumulation, cross-side network effects, customer inertia and the effect of default settings, branding, and extreme economies of scale and sunk costs.

541 The CMA's final report into online platforms and digital advertising notes that 'economies of scale arise where average costs decrease with increasing scale. These features can create a barrier to entry as, once a platform reaches a certain size, it can be extremely difficult for smaller new entrants to challenge them effectively'. See Competition and Markets Authority, Online platforms and digital advertising market study final report, July 2020, p. 11.
The ACCC notes that sunk costs (i.e. costs that are incurred and cannot be recovered in any way) are another type of barrier to entry. To the extent that the fixed costs are also 'sunk', they can give rise to further barriers to entry for a potential new entrant.

economies of scale to the crawling and indexing of webpages.[542] In its final report into online platforms and digital advertising (the CMA Final Report), the UK Competition and Markets Authority (CMA) considered there to be substantial scale economies in crawling and indexing and noted the importance of a search engine obtaining sufficient scale in search queries and click-and-query data[543]. Similarly, the European Commission had previously noted the value of scale in competing effectively in search services and search advertising.[544]

Search engines have also made public statements suggesting that the costs of crawling and indexing websites are significant, and that new entry is difficult. For example, Microsoft has estimated that its indexing investments added up to billions over time[545] and the European Commission has quoted DuckDuckGo and Yahoo as each suggesting that a search engine would need to invest hundreds of millions of dollars a year crawling and indexing websites.[546] Cliqz, a German search engine that operated its own crawling and indexing functions, stated that the infrastructure costs in serving a massive, constantly updated index at scale would be 'millions of euros each year to operate.'[547] On 29 April 2020, Cliqz announced the closure of its search engine, noting that 'in the long run, we have no chance against an overpowering opponent such as Google, which dominates the market in every aspect.'[548]

Accordingly, rather than incurring the significant costs required to crawl and index websites, some general search suppliers syndicate search results from existing search engines instead (either Google or Bing), through the negotiation of syndication agreements.

### Syndication agreements for crawling, indexing and ranking

Syndicated search results may be offered together with syndicated search ads—that is, a search engine may offer both the organic search results from its index and search advertising inventory from its own network.[549] For example, DuckDuckGo and Ecosia each have syndication agreements in place with Bing, which provides them with access to Bing's organic links and ads, which are then displayed to consumers utilising DuckDuckGo's and Ecosia's search engines.[550] As such, search engines can be distinguished between upstream providers to syndication agreements (i.e. Google and Bing) and downstream search engines that purchase search results from upstream providers (e.g. DuckDuckGo and Ecosia).

The ACCC understands that downstream search engines can also purchase syndicated search results from entities that do not produce their own search results, such as Verizon Media, effectively sub-syndicating search results from those providers. However, it appears that most downstream search engines syndicate organic search results directly from Google or Bing. Bing offers upstream search services to a number of downstream search engines referred to in the DPI Final Report (including Yahoo Search, DuckDuckGo, Qwant and

---

542 Crawling is the process by which search engines systematically and continuously search the internet for new pages and add them to their index of known pages so they can be surfaced in search results.
543 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, pp. 91, 95.
544 European Commission, Comp/M.5727—Microsoft/Yahoo! Search Business, 18 February 2010, pp. 25, 29.
545 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, p. 90.
546 European Commission, Case AT.39740—Google Search (Shopping), 27 June 2017, p. 66; European Commission, Comp/M.5727—Microsoft/Yahoo! Search Business, 18 February 2010, p. 24.
547 Cliqz, Building a search engine from scratch, 6 December 2019, *Tech @ Cliqz,* accessed 22 September 2020.
548 D Stommel, Cliqz closes areas for browser and search technologies, *Hubert Burda Media,* 29 April 2020, accessed 22 September 2020
549 Microsoft, Syndicated Partner Network, accessed 22 September 2020.
550 Microsoft, Syndicated Partner Network, accessed 22 September 2020; DuckDuckGo, Sources, accessed 22 September 2020.

Ecosia[551]). Google syndicates its organic search results with at least one downstream search engine, Startpage.[552]

Because of the high barriers to entry and expansion in upstream search services, the limited substitutes available and the existence of only two upstream providers of search results, upstream providers of search services are likely to have a stronger bargaining position in their dealings with downstream search engines.

Accordingly, the competitive constraint posed by downstream search engines may be constrained by conditions put in place by upstream providers.

### Effect of Google and Bing's strong bargaining position on downstream supply of general search

In the CMA Final Report, the CMA concluded that Google and Bing have a strong bargaining position with downstream providers:

> *As the only at-scale English-language web-crawling search engines, Google and Bing will naturally have a strong bargaining position in discussions with downstream search engines. As a result, they may choose not to offer agreements to some providers, or may insist on terms that limit the ability of downstream providers to compete.*[553]

To demonstrate the strong bargaining position of Google, the CMA also provided the example of Ecosia approaching Google to purchase syndicated search services from Google, which was consistently rejected.[554]

DuckDuckGo publicly stated that contracts for syndicated search services with upstream search engines often contain 'exclusivity provisions that would prevent them from using Google's click-and-query data'.[555]

The CMA further noted that none of the syndication agreements that they reviewed allowed downstream providers to re-rank the search results that they received, and that several downstream providers said that they would like to be able to modify search results, in order to improve their ability to differentiate.[556] These restrictions limit the extent to which downstream search engines can differentiate themselves from, and compete with, Google and Bing.

### Conclusion—competitive constraints posed by search engines reliant on syndicated search results

Given the degree of bargaining power upstream providers of search results have relative to downstream search engines, and the ability of upstream providers to influence downstream search engines' use of syndicated search results, the competitive constraint posed by the smaller downstream engines appears to be quite weak.

In light of the very limited competition faced by Google and the high barriers to entry and expansion described in the DPI Final Report, the ACCC considers that Google still has substantial market power in the market for general search, which is likely to endure in the short to medium term. Internationally, a number of measures have been proposed to

---

551 Microsoft, Syndicated Partner Network, accessed 22 September 2020; DuckDuckGo, Sources, accessed 22 September 2020; Qwant, How does Qwant index the web?, 1 October 2017, accessed 22 September 2020.

552 Startpage, What is the relationship between Startpage.com and Google?, 20 November 2018, accessed 22 September 2020.

553 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, p. 98.

554 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, p. 98.

555 DuckDuckGo, DuckDuckGo's Comments on the Market Study Interim Report: Online Platforms and Digital Advertising, 19 February 2020, p. 11.

556 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, p. 98.

improve the state of competition in the supply of general search services, discussed in the box below.

**Box B.1: Regulatory proposals to increase competition in the supply of general search services**

**Recommendations in the CMA report**

Increasing competition in upstream search services has the potential to enable greater competition in the supply of general search services. Currently, search engines realistically only have two options from which to obtain syndicated search results—Bing and Google. Reducing barriers to entry, and encouraging competition in upstream search services, could have the effect of increasing the number of upstream search service providers, which may then facilitate more competition in the supply of general search services.

To address these issues, the CMA recommended a number of regulatory interventions to improve competition in the general search services market.[557] These included demand-side remedies, aimed at facilitating consumer choice and improving access to consumers for rival search engines, and supply-side remedies, focused on providing third parties with access to data to improve the quality of search services offered (and therefore, improving their competitive offering). DuckDuckGo, Ecosia, Mojeek and Cliqz provided varying levels of support for these interventions.[558] These interventions include choice screens, the power to restrict default search engines from being installed on browsers devices and mandating third party access to search data.

**Android choice screen in Europe**

On 2 August 2019, Google announced that it would implement a choice screen for general search providers on all new Android phones and tablets shipped into the European Economic Area where the Google Search app is pre-installed.[559] The choice screen would contain four general search providers (including Google), which would be chosen by way of a fourth-price auction on a quarterly basis.[560] This followed the European Commission's finding that Google breached European Union antitrust laws by imposing restrictions on Android device manufacturers and mobile network operators between 2011 and 2014, to cement its dominant position in Europe in general internet search.[561]

DuckDuckGo indicated that while a search preference menu can deliver meaningful choice to consumers and increase competition in the search market, the design of Google's choice screen could be improved by increasing the number of search options available [562] and removing the auction system.[563] Qwant also reportedly expressed concerns about the requirement for rival search engines to pay Google to be featured on the choice screen.[564] Ecosia announced that it would boycott this auction and that it found the choice screen to be 'harmful for competition'.[565]

---

557 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, pp. 360-369.

558 DuckDuckGo, DuckDuckGo's Comments on the Market Study Interim Report Online Platforms and Digital Advertising, 19 February 2020; Ecosia, Response to Interim Report consultation, undated; Mojeek, 'Online Platforms and Digital Advertising' Interim Report Comments, 12 February 2020; Cliqz, Comments regarding the online platforms and digital advertising market study, interim report, 12 February 2020.

559 Android, About the choice screen, updated 1 June 2020, accessed 22 September 2020.

560 Android, About the choice screen, updated 1 June 2020, accessed 22 September 2020.

561 For further information, see European Commission, Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine, 18 July 2018.

562 DuckDuckGo, Search Preference Menu Immediately Increases Google Competitors' Market Share by 300-800%, 30 October 2019, accessed 22 September 2020, referred to in DuckDuckGo, DuckDuckGo's Comments on the Market Study Interim Report: Online Platforms and Digital Advertising, 19 February 2020, p. 9. On 10 August 2020, DuckDuckGo published the results of testing conducted with 12,000 people in the US, UK and Australia, using DuckDuckGo's proposed design for a choice screen (which includes more than 4 options). The testing indicated that that Google's mobile market share was likely to drop by 20 per cent, 22 per cent and 16 per cent in the US, UK and Australia respectively. See DuckDuckGo, Google Search Mobile Market Share Likely to Drop Around 20% through Search Preference Menus, 10 August 2020, accessed 22 September 2020.

563 DuckDuckGo, Search preference menus: no auctions please, 10 March 2020, accessed 22 September 2020.

564 N Lomas, Google to auction slots on Android default search 'choice screen' in Europe next year, rivals cry 'pay-to-play' foul, *TechCrunch,* 3 August 2019, accessed 22 September 2020.

565 Ecosia, Why you can't choose Ecosia on your new Android phone, 3 March 2020, accessed 22 September 2020.

**Following the Australian Government's response to the DPI Final Report, the ACCC will, through its Digital Platforms Branch, monitor the impact of the changes in Europe and provide further advice to the Government.[566]**

## Google's role in specialised search

The DPI Final Report noted the expansion of Google into specialised or vertical search and the potential for Google to leverage its market power in general search services to preference its specialised search services, to the detriment of competition in the relevant search vertical.[567] This potential for self-preferencing behaviour has been subject to ongoing inquiry in 2020.

In March 2020, the U.S. Senate Committee on the Judiciary, Subcommittee on Antitrust, Competition Policy and Consumer Rights held a hearing into self-preferencing by digital platforms. During this hearing, Yelp, a provider of local search results, provided a testimony submitting that Google attempted to control the flow of online traffic and preference its content by adding OneBoxes to the top of its search results pages, which exclusively contained content from Google's specialised search services.[568]

A July 2020 study considered the extent to which Google engages in self-preferencing on Google Search. It examined more than 15,000 recent popular queries and found that 41 per cent of the first page of search results on mobile devices were taken up by Google-owned properties and what it calls 'direct answers'.[569] It also surveyed the prevalence of Google Flights, in response to search queries for flights and found that Google frequently presented Google Flights at the top of search engine results pages, before links to other airlines and travel sites that may offer lower prices for the same flights.[570]

In addition to reporting concerns from specialised search providers on Google's self-preferencing behaviour,[571] the CMA noted that the expansion of Google's ecosystem into specialised search could have been motivated by an incentive to insulate Google's core services from future competition stemming from that adjacent market.[572] This is supported by an email from a 2012 Google employee published at the July 2020 hearing of the House Committee on the Judiciary, which also highlighted the value of specialised search services and the need for Google to remain competitive in these areas:

> *…there are a set of areas that are pretty fundamental to users day-to-day experiences and needs, and are very, very valuable – online shopping for goods and services (7% of total commerce and growing), local search (20% of desktop intent and 40% of mobile intent), and travel (>10% of our current revenues, [redacted] global market); if we don't have experiences in these areas that are compelling compared to increasingly concentrated and branded alternatives, we risk losing relevance overall…We don't have to own everything and we can work with partners,*

---

566 Australian Government, Regulating in the digital age – Government response and implementation roadmap for the Digital Platforms Inquiry, 12 December 2019, p. 8.
567 ACCC, DPI Final Report, 26 July 2019, pp. 529-530.
568 L Lowe, RE: Self-preferencing by dominant internet platforms, 10 March 2020, p. 4.
569 A Jeffries and L Yin, Google's top search result? Surprise! It's Google, *The Markup*, 28 July 2020, accessed 22 September 2020.
570 A Jeffries and L Yin, Google's top search result? Surprise! It's Google, *The Markup*, 28 July 2020, accessed 22 September 2020.
571 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, pp. 109-110.
572 Competition and Markets Authority, Appendix E to Online platforms and digital advertising market study final report, 1 July 2020, p. E3.

*but our bar has to be a great end-to-end experience instead of just handing users off.*[573]

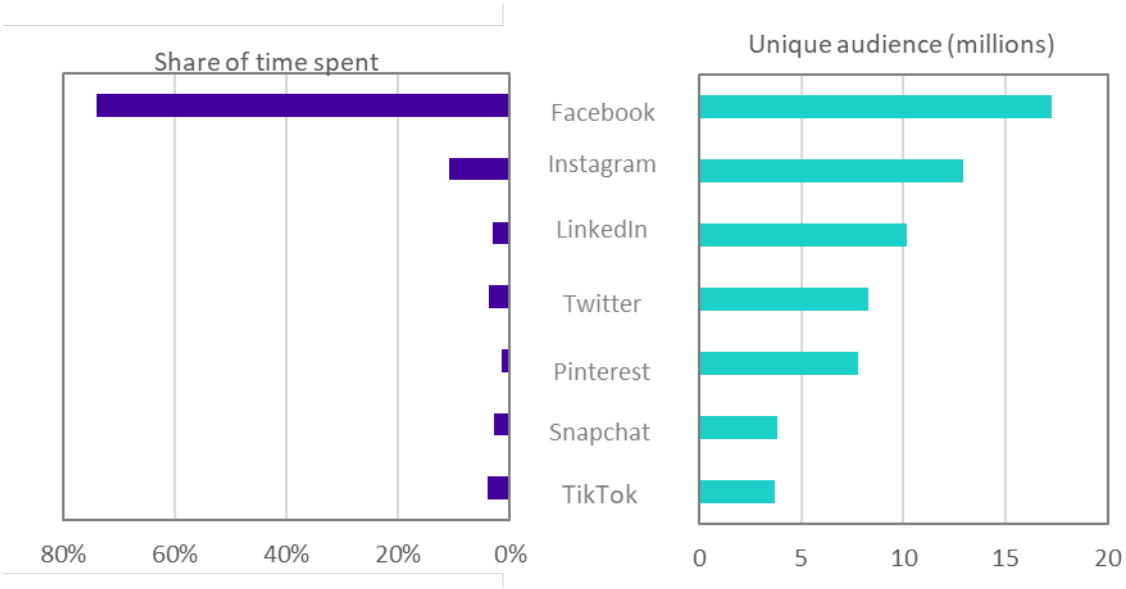
As discussed in chapter 7, a number of jurisdictions across the world have recognised the impact of incumbent platforms and their move into other markets, with some considering or introducing legislative proposals to address it. The ACCC will continue to monitor this issue.

## B.2 Social media

The ACCC considers that Facebook continues to have substantial market power in the supply of social media.

As discussed in chapter 1, use of some social media platforms outside of Facebook and Instagram has grown since the publication of the DPI Final Report. However, despite this growth, Facebook retains the majority of time spent by users on its platforms and no social media platforms appears to provide a meaningful constraint to Facebook. The significant time spent by Australian users on the Facebook platform and Instagram and their proportion of unique audience is illustrated in figure B.2 below.

**Figure B.2: The unique audience and time spent by Australians on selected social media platforms (June 2020)**




Source: Nielsen Digital Content Ratings, June 2020, Persons 13+, PC, Smartphone and Tablet, Unique audience and total time spent.

### Dynamic competition in social media

As social media services are often offered at a zero monetary price, suppliers of social media compete for users on the basis of the quality of, and features offered on, the social media service. When a social media service offers new or innovative features, competing services may imitate those features.[574] This 'feature competition' is an example of dynamic

---

573 Email from Jeff Huber to Alan Eustace, Re: URGENT – Naming – Strategy Issue – Vertical Search, 21 September 2012, p. 1, produced to the US House Committee on the Judiciary hearing on Online Platforms and Market Power: Examining the Dominance of Amazon, Apple, Facebook and Google, accessed 6 August 2020.

574 As Inge Graef states 'because users commonly have free access to online platforms, they choose their provider on the basis of aspects other than price such as quality and the level of innovation that a service offers'. See I Graef, Market definition and market power in data: the case of online platforms, World Competition: Law and Economics Review, Vol. 38, No. 4 (2015), p. 494.

competition.[575] In the DPI Final Report, the ACCC considered that Facebook is insulated from dynamic competition by barriers to entry and expansion, including advantages of scope that may result from its acquisition strategies.[576] Box B.2 provides a case study of feature competition of services provided by Snapchat and TikTok.

**Box B.2: Feature competition—Snapchat and TikTok**

**Snapchat** provides users with the ability to post, send and receive photos and messages, which are available for a short period of time before becoming inaccessible to their recipients; these posts are known as 'Stories'. When launched in 2011, it was seen as a competing service to Facebook, with many younger people adopting this service. In August 2016, Instagram launched a Stories feature which was very similar to that of Snapchat's Stories function (a feature that allows users to create stories with photos and videos that are available for 24 hours and then disappear thereafter).[577] Throughout 2016 and 2017, Instagram also launched face filters, location tags, stickers, drawing tools, and disappearing photo messages, all of which are very similar to features offered by Snapchat at the time.[578]

Users rapidly adopted Instagram Stories, with a reported 200 million daily active users using this feature worldwide in April 2017, compared to 166 million daily active users of Snapchat.[579] Snapchat's quarter on quarter growth also dropped from 17.2 per cent in Q2 2016 to 3.2 per cent in Q4 2016.[580] Other platforms have since introduced similar stories features, including Facebook and LinkedIn.[581] In a July 2020 hearing of the House Committee on the Judiciary, Mark Zuckerberg stated that had 'certainly adapted features' from others in response to a question regarding whether the company had copied features from competitors.[582] There are also documents to suggest that this was a strategy adopted by Facebook to compete against other social media platforms.[583]

As previously discussed, **TikTok** has been quickly gaining users and has been widely discussed as a competing service to the Facebook platform Instagram. In 2018, Facebook launched Lasso, an app that allowed users to post short videos and view them in an algorithmic feed. Lasso was widely considered to be a competing service to TikTok.[584] The app was only available in the US, Colombia, Mexico, Argentina, Chile, Peru, Panama, Costa Rica, El Salvador, Ecuador and Uruguay and shut down in July 2020, reportedly due to low usage and a shift in focus to another app by Facebook, Instagram Reels (Reels).[585] Reels, an Instagram feature that allows users to record, edit and share videos up to 15 seconds long, was launched on 5 August 2020 and made available in more than 50 countries including Australia. The Wall Street Journal reported that Instagram had approached a number of TikTok creators to use Reels, a sign 'that Facebook intends for its

---

575 D Evans, Multi-sided Platforms, Dynamic Competition and the Assessment of Market Power for Internet-based Firms, Coase-Sandor Institute for Law and Economics Working Paper, no. 753, March 2016, p. 27.

576 ACCC, DPI Final Report, pp. 78–84.

577 J Constine, Instagram launches "Stories," a Snapchatty feature for imperfect sharing, *Techcrunch,* 3 August 2016, accessed 22 September 2020.

578 A Hartmans, We compared Snapchat and Instagram to find out which app is better -- here's the winner, *Business Insider*, 7 August 2017, accessed 22 September 2020.

579 J Constine Snapchat hits a disappointing 166M daily users, growing only slightly faster, *Techcrunch,* 17 May 2017, accessed 22 September 2020; J Constine, Instagram Stories hits 200M users, surpassing Snapchat as it copies its AR stickers, *Techcrunch,* 14 April 2017, accessed 22 September ; J Constine, Instagram's growth speeds up as it hits 700 million users, *Techcrunch,* 26 April 2017, accessed 22 September 2020.

580 J Constine Snapchat hits a disappointing 166M daily users, growing only slightly faster, *Techcrunch* 17 May 2017, accessed 22 September 2020

581 N Bobby, LinkedIn tries more relaxed vibe with stories launch, *Australian Financial Review*, 18 June 2020, accessed 22 September 2020

582 L Eadicicco, Mark Zuckerberg was grilled over whether Facebook copied and threatened rivals, but the CEO says the social media giant just 'adapted features', *Business Insider,* 30 July 2020, accessed 22 September 2020.

583 See, for example, emails produced to the House Committee on the Judiciary hearing on Online Platforms and Market Power: Examining the Dominance of Amazon, Apple, Facebook and Google, July 2020, between Mark Zuckerberg, Mike Schroepfer, Chris Cox and others: email from Sheryl Sandberg to Mark Zuckerberg dated 30 March 2012, accessed 22 September 2020; email from unknown author to Mike Schroepfer and others dated 3 April 2012, accessed 22 September 2020.

584 See, for example, M Singh, Facebook is shutting down Lasso, its TikTok clone, *TechCrunch*, 2 July 2020, accessed 22 September 2020; J Porter, Facebook's TikTok clone Lasso will shut down this month, The Verge, 22 September 2020, accessed 22 September 2020; S Shead, Facebook is shutting down TikTok clone Lasso and Pinterest rival Hobbi, *CNBC*, 2 July 2020, accessed 22 September 2020.

585 M Singh, Facebook is shutting down Lasso, its TikTok clone, *TechCrunch*, 2 July 2020, accessed 22 September 2020. The article reported that 'Lasso had fewer than 80,000 daily active users on Android—the highest it has ever had—in Mexico — its biggest market — on June 1, according to mobile insights firm App Annie'.

Instagram Reels service to directly compete with ByteDance Ltd.'s TikTok'.[586] In addition, the Australian Financial Review reported that:

> *Instagram will be pushing Reels to the forefront of the user experience by completely overhauling its entire Explore page, which is the main way that people find new posts, content and social media influencers to follow and helps to keep them scrolling on the app for longer… the Explore page will instead autoplay a number of Reels in a manner that shares some of the vibe of TikTok's For You screen, which works by thrusting new video content constantly in the user's face in a heady onslaught of digital ecstasy and disorientation.*[587]

For a large platform with market power, such as Facebook, that is largely insulated by high barriers to entry (including economies of scope and network effects), the ability to imitate features offered by competing social media services and offer those features on their platforms may have the effect of limiting the competitive constraint posed by dynamic competition. In particular, by replicating features of other social media services, Facebook's behaviour may reduce the incentives for these social media services to innovate or invest in obtaining efficiencies.[588]

## B.3 Search advertising

Based on information provided to the ACCC, Google had a 97 per cent share of general search advertising revenue in Australia in 2018 and a 95 per cent share in 2019.[589]

The ACCC considers that Google continues to have market power in the market for general search advertising in Australia.

### Specialised search advertising provides a weak constraint on general search advertising

As discussed in the DPI Final Report, the ACCC considers that suppliers of specialised search advertising presently place little competitive constraint on Google.[590] Suppliers of specialised search advertising only provide advertising inventory for a specific range of products or services, and suppliers of specific search advertising still have a relatively small presence in the supply of search advertising, compared to Google. This is consistent with the findings in the CMA Final Report, though it noted the possible exception of Amazon in its supply of specialised search advertising services in the retail vertical. The CMA considered that while Amazon may compete more directly with Google in relation to retail search advertising, this type of advertising represented only a small portion of Google's revenue in search.[591]

As illustrated in figure B.3, there remains a significant disparity in overall global advertising revenue earned by Google compared to Amazon and Expedia,[592] both of which supply specialised search advertising in their respective verticals (retail and travel).

---

586 E Choi, Facebook Offers Money to Reel In TikTok Creators, *Wall Street Journal,* 28 July 2020, accessed 22 September 2020.

587 N Gillezeau, Instagram takes on TikTok with 'Reels' feature, *Australian Financial Review*, 6 August 2020, accessed 22 September 2020.

588 OECD, Start-ups, Killer Acquisitions and Merger Control – Background Note (for Item 2 of the 133rd Meeting of the Competition Committee on 10-12 June 2020), 12 May 2020, p. 22.

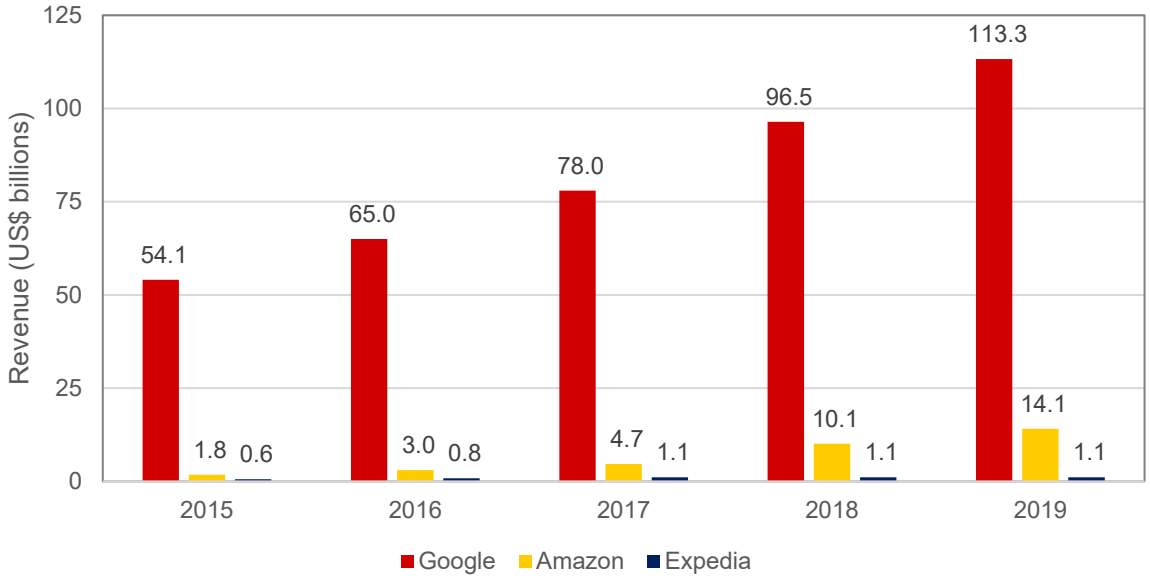
589 Information provided to the ACCC; figures are not comparable to information provided in the Final Report of the Digital Platforms Inquiry due to changes in calculation methodology.

590 ACCC, DPI Final Report, 26 July 2019, p. 96.

591 Competition and Markets Authority, Online platforms and digital advertising market study final report, 1 July 2020, pp. 88-89.

592 The data in figure B.3 is taken from the companies' 10-K financial statements. For Amazon and Expedia, the estimates represent upper bounds on their annual advertising revenue. The figure for Amazon is its 'other sales' item, which is primarily advertising revenue. The figure for Expedia is its 'advertising and media' component of its revenue, which includes third-party revenue from Trivago.

**Figure B.3: Global revenue from advertising (US$)**




Source: Google, Amazon and Expedia 2019 10-K forms. The figures for Amazon and Expedia are proxies for advertising revenue: the figure for Amazon is the 'Other' component of the 'Net Sales' item; the figure for Expedia is the 'Advertising and media item.

The ACCC will continue to monitor the position of Amazon's entry/expansion into advertising in Australia (following its entry in April 2019[593]) and notes PwC's 2020 predictions of growth:

> *Amazon are well positioned to offer addressable advertising solutions, built on a rich and growing database of consumer behaviour and purchase insights. Representing over four percent of the United States' total advertising market, and sitting at number three of the largest digital businesses, it is expected that Amazon will command strong investment from Australian brands.*[594]

The ACCC also notes that after Google, Facebook and Microsoft, Amazon has the greatest number of third party tracking scripts on the top 1000 websites in Australia (see figure 4.2 in chapter 4) and further, in the AppCensus commissioned report, was observed receiving data transmitted from around 4.4 per cent of the 1000 Android apps in Australia.[595] As discussed in the DPI Final Report, user data is an extremely valuable input to online advertising, providing suppliers of advertising services with the ability to target customers. For platforms that already collect user data on their platform, the ability to collect and combine that with data collected about users off their platform provides them with a competitive advantage in the supply of advertising services.

As noted above, Amazon's role as a specialised search service will be considered in more detail as part of the Inquiry.

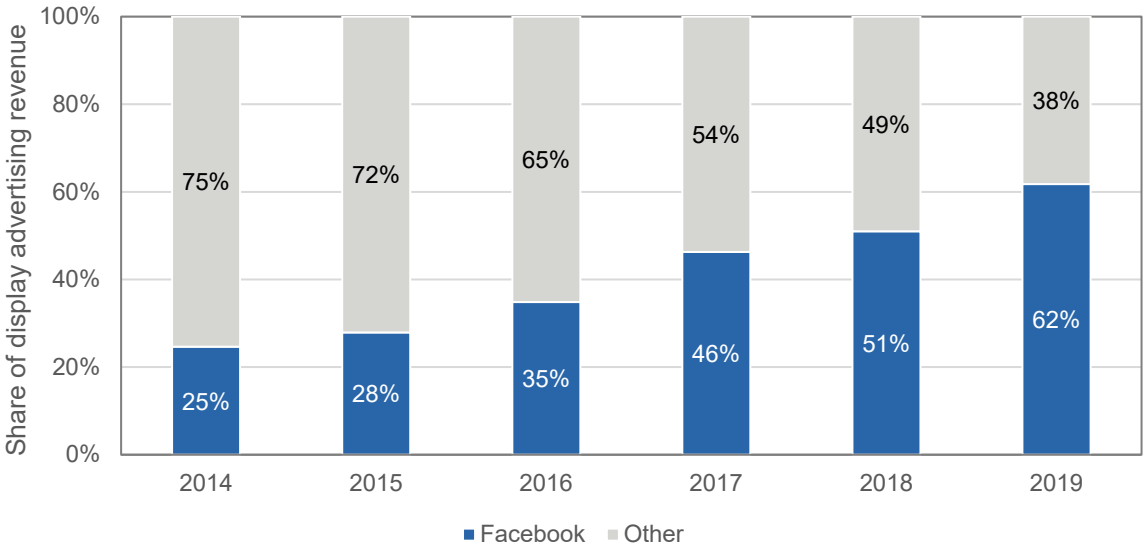
## B.4 Display advertising

Facebook continues to maintain a dominant share of the overall supply of display advertising in Australia[596], as set out in figure B.4 below.[597] Facebook's share of display advertising revenue earnt in Australia increased by 11 per cent from 2018 to 2019.

---

593 Amazon, Amazon Advertising launches in Australia, 5 April 2019, 5 April 2019, accessed 22 September 2020.
594 PwC Australia, Australian Entertainment & Media Outlook 2019-2023, Internet Advertising, accessed 22 September 2020.
595 AppCensus, 1000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 33.
596 Following the correlating finding in the DPI Final Report. See ACCC, DPI Final Report, 26 July 2019, pp. 97–99.
597 Information provided to the ACCC. Several assumptions are made to estimate the total Australian display advertising expenditure that could affect our market share estimates. Note that that the revenue attributed to Facebook includes not

**Figure B.4: Shares of display advertising revenue in Australia**




Source: Information provided to the ACCC.

Within the range of display advertising, there are differentiated offerings, such as advertising specifically on social media services (social media advertising[598]), video advertising and display advertising supplied through various channels (such as owned and operated properties, and open display). These offerings may be differentiated as some advertisers may see certain types of display advertising as closer substitutes than others.

Accordingly, the overall supply of display advertising could be segmented into narrower markets. For example, the CMA's final report into online platforms and digital advertising flagged the potential for display advertising services to be further segmented into video and non-video advertising; however, because the evidence of substitutability between video and non-video advertising was mixed, it does not make any conclusions regarding this market.[599] However, it did note that if this market were further segmented into video and non-video advertising, Facebook and Instagram have 50-60 per cent share of expenditure in video display advertising in the UK and 40-50 per cent of non-video display advertising, and that YouTube would have a 15-20 per cent share of expenditure in video display advertising.[600]

Similarly, in its announcement regarding the opening of an in-depth investigation into the proposed acquisition of Fitbit by Google, the European Commission noted Google's 'strong market position' in the supply of online display advertising services in a number of countries, and in particular, Google's position in relation to 'off-social networks display ads'.[601] This raises the possibility of a further segmentation in display advertising between display ads on social networks, and off social networks.

---

only revenue from display advertising on its Facebook and Instagram platforms but also from the Facebook Audience Network. Revenue from the Audience Network, however, makes only a relatively small contribution to this figure. The ACCC notes that Facebook's advertising revenue figures relate to the amount of advertising revenue from customers in Australia based on the location of the invoiced party (which may differ from the country in which the advertisements are shown). The ACCC understands that these figures are not recorded in the ordinary course of business by Facebook and are not audited, verified or otherwise reported on. As such, the ACCC considers that these are approximate estimates of relevant advertising revenue attributable to Australia for Facebook.

598 As set out in the DPI Final Report, social media advertising is a specific kind of display advertising which can be differentiated from other forms of display advertising due to the unique levels of engagement available on social media.

599 Competition and Markets Authority, Online platforms and digital advertising market study final report, July 2020, p. 244.

600 Competition and Markets Authority, Online platforms and digital advertising market study final report, July 2020, p. 247.

601 European Commission, Mergers: Commission opens in-depth investigation into the proposed acquisition of Fitbit by Google, 4 August 2020, accessed 22 September 2020.

The ACCC has not made any findings in relation to the segmentation of display advertising into video and non-video, and social media and non-social media, but notes that this is a possibility, particularly given the rise in advertising expenditure on video advertising in recent years, and the substantial advertising expenditure spent on social media platforms. The ACCC may consider this issue again in future interim reports.

## B.5 Conclusions—market power assessment in search, social media, search advertising and the overall supply of display advertising

The ACCC concludes that Google continues to have market power in the general search and search advertising markets, and that Facebook continues to have market power in the social media and in the overall display advertising markets. However, the ACCC will continue to monitor changes, and in particular, the impact of relatively new entrants such as Amazon.

# Appendix C: Functionalities and features of selected online private messaging services

This appendix sets out the functionalities and features of selected non-proprietary communications-focused online private messaging services offered in Australia, based on a desktop review conducted by the ACCC in September 2020.

| | | Facebook Messenger | WhatsApp | Signal | LINE | WeChat | Discord | Threema | Snapchat | Zoom | Skype | Microsoft Teams | Slack | iMessage | FaceTime |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Messaging/ call features** | **Text** | • | • | • | • | • | • | • | • | • | • | • | • | • | ⊗ |
| | **Voice** | • | • | • | • | • | • | • | • | • | • | • | • | •[602] | • |
| | **Video** | • | • | • | • | • | • | ⊗[603] | • | • | • | • | • | •[604] | • |
| | **Video call participant Limit** | 8[605] | 8[606] | 2 | 500[607] | 9[608] | 25[609] | ⊗ | 15[610] | 100[611] | 50 | 50[612] | 15[613] | ⊗ | 32[614] |

602 iMessage supports voice messaging where an audio message is recorded and sent to another user, but not voice calling. See Apple Support, Send photo, video or audio messages on your iPhone, iPad or iPod touch, accessed 23 September 2020.

603 Video calls on Threema were released from beta testing on 10 August 2020. See Threema Blog, Video Calls the Threema Way, 10 August 2020, accessed 23 September 2020.

604 iMessage supports video messaging where a video message is recorded and sent to another user, but not video calling. See Apple Support, Send photo, video or audio messages on your iPhone, iPad or iPod touch, accessed 23 September 2020. FaceTime, another app preinstalled on Apple devices, supports video calling. See Apple Support, Use FaceTime with your iPhone, iPad or iPod touch, accessed 23 September 2020.

605 Facebook has introduced Messenger Rooms, which allows group video calls of up to 50 people. See Facebook, Facebook Messenger Rooms, accessed 23 September 2020.

606 WhatsApp, Group Video and Voice Calls Now Support 8 Participants, *WhatsApp Blog,* 28 April 2020, accessed 23 September 2020.

607 LINE Group Video calls allows up to 500 participants on the conference call, and can be accessed via a link. See LINE Blog, With LINE Meeting, now you can join group video calls by URL!, 21 August 2020, accessed 23 September 2020.

608 WeChat Help Centre, How do I use Video & Voice Call for Groups?, accessed 23 September 2020.

609 Discord temporarily raised the server video chat limit from 10 people at a time to 25 people due to 'current events'. See Discord Help Centre, Server Video, accessed 22 September 2020.

610 Snapchat, Snapchat Support: Voice and Video Chat, accessed 23 September 2020.

611 The limit varies by package: the Business package allows up to 300 participants, the Enterprise package allows up to 500 participants, and the Enterprise Plus package allows up to 1000 participants. See Zoom, Choose a plan, accessed 23 September 2020.

612 The limit varies by package. Microsoft recently increased the maximum number of participants in its paid packages from 250 to 300. Teams for Government is still subject to the 250 participant limit. Microsoft also announced plans to expand the number of participants visible on screen at any one-time to 49 in a 7x7 grid. See Microsoft, Limits and specifications for Microsoft Teams, 14 August 2020, accessed 23 September 2020; Microsoft Education Blog, What educators have learned from remote learning prepares them for the new school year, 15 June 2020, accessed 23 September 2020.

613 The limit varies by package: the Free version (intended for 'small teams trying out Slack') allows 1-to-1 calls, the Standard/Plus/Enterprise packages allow up to 15 participants. See Slack, Slack Pricing, accessed 23 September 2020.

614 Apple Support, Use Group FaceTime on your iPhone, iPad and iPod touch, accessed 23 September 2020.

| | | Facebook Messenger | WhatsApp | Signal | LINE | WeChat | Discord | Threema | Snapchat | Zoom | Skype | Microsoft Teams | Slack | iMessage | FaceTime |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Device access point** | **Smartphone** | • | • | • | • | • | • | • | • | • | • | • | • | • | • |
| | **Tablet** | • | • | • | • | • | • | • | • | • | • | • | • | • | • |
| | **Computer** | • | • | ⊗ | • | • | • | • | ⊗ | • | • | • | • | •[615] | •[616] |
| **Network** | **Ownership** | Facebook | Facebook | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | Microsoft | Microsoft | ⊗ | Apple[617] | Apple[618] |
| | **Target audience/ demographic** | Facebook Users | Everyone | Everyone | Everyone | Everyone | Young, Gaming | Everyone | Young | Everyone, Enterprise | Everyone, Enterprise | Everyone, Enterprise | Everyone, Enterprise | Everyone | Everyone |
| | **Use by users outside Network** | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | • (can join via web browser) | • (can join via web browser) | • (can join via web browser) | ⊗[619] | ⊗ | ⊗ |
| **Privacy** | **E2EE/privacy** | ⊗[620] | • | • | • | ⊗ | ⊗ | • | • | ⊗ (paid feature)[621] | ⊗ (basic encryption) | • | ⊗ (basic encryption[622]) | • | • |
| **Chat/call** | **Group chat** | • | • | • | • | • | • | • | • | • | • | • | • | • | • |

615 In addition to smartphones, tablets and computers, iMessage can also be accessed on Apple's smartwatch device (Apple Watch). See Apple Watch User Guide, Send messages from Apple Watch, accessed 23 September 2020.

616 In addition to smartphones, tablets and computers, FaceTime audio call functionality can also be accessed on Apple's smartwatch device (Apple Watch) using the Walkie-Talkie app. See Apple Support, Use Talkie-Talkie on you Apple Watch, accessed 23 September 2020.

617 iMessage is only available on Apple operating systems.

618 FaceTime is only available on Apple operating systems.

619 Users require a separate account for each workspace they are a member of, and there is no limit to the number of Slack accounts a user can create with the same email address. See Slack, Join a Slack workspace, accessed 23 September 2020.

620 Facebook Messenger provides a 'secret conversations' feature which allows for end-to-end encryption. However, that feature is not provided by default and not available for group conversations. See Facebook Help Centre, Secret conversations, accessed 23 September 2020.

621 Zoom does not provide end-to-end encryption by default to free calls. However, on 17 June 2020, it announced that it will roll out end-to-end encryption to all users (including free users). See E Yuan, End-to-end encryption update, *Zoom Blog,* 17 June 2020, accessed 23 September 2020.

622 Slack secures users' messages both when they are in transit between parties and when they are at rest. Slack claims to further protect data with tools like Slack Enterprise Key Management, audit logs, and integrations with top data loss prevention (DLP) providers. See Slack, Security at Slack, accessed 23 September 2020.

| | | Facebook Messenger | WhatsApp | Signal | LINE | WeChat | Discord | Threema | Snapchat | Zoom | Skype | Microsoft Teams | Slack | iMessage | FaceTime |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **features** | **File transfer** | • | • | • | • | • | • (images only) | • | • (images only) | • | • | • | • | • | ⊗[623] |
| | **Read receipts** | • | • | • | • | ⊗ | ⊗ | • | • | ⊗ | ⊗ | • | ⊗ | • | ⊗ |
| | **Delete sent messages** | • | • | • | • | ⊗ | • | • | • (exploding messages) | • | ⊗ | ⊗ | •[624] | ⊗ | ⊗ |
| | **Stickers/GIFs** | Stickers, Gifs | Stickers | Stickers, Gifs | Stickers, Gifs | Stickers | ⊗ | Gifs | Cameos | Stickers, Gifs | ⊗ | Stickers | Stickers, Gifs, Custom Emoji | Stickers, Gifs | ⊗ |
| | **Screen share** | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | • | • | • | • | ⊗ | ⊗ |
| | **Location tracking** | • | • | • (Location Pins) | • | • | ⊗ | ⊗ | • (Snap Map) | ⊗ | ⊗ | ⊗ | ⊗ | • | ⊗ |
| | **Payment service** | ⊗ | ⊗ | ⊗ | • | • | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ |
| | **Other notable features** | Polls, Games | | | Games | | Teams | Polls | Games | Polls, Waiting Rooms, screen sharing, co-annotation on shared screen, scheduled meetings | | Teams, screen sharing, scheduled meetings | Persistent chat rooms (channels), workspace, screen sharing, third-party service integration | | Memoji and Animoji, Live Photos captured during a video call[625] |
| **Pricing** | **Upfront charges/ subscription** | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ | Free; Discord Nitro is | $4.99 | ⊗ | Basic package is $0; plans with additional | $0[626] | Free; plans with additional | Basic package is $0; plans with | Preinstalled on Apple | Preinstalled on Apple |

[623] FaceTime does not support file transfer, however it comes preinstalled on the same Apple devices as iMessage, which does support file transfer.

[624] On Slack, it is not possible to bulk delete messages. Further, Workspace Owners and Admins can set message editing and deletion permissions for members, thereby removing the ability to delete sent messages. See Slack Help Centre, Edit or delete messages, accessed 23 September 2020.

[625] Apple Support, Use FaceTime with your iPhone, iPad or iPod touch, accessed 23 September 2020.

[626] While Skype is offered for free, Skype for Business (Microsoft's professional online meeting solution) can be purchased at various price points. Skype for Business, Microsoft's previous professional online meeting solution, is being replaced by Microsoft Teams. See Skype, A communication tool built for businesses to connect anywhere, anytime, accessed 23 September 2020.

| | | Facebook Messenger | WhatsApp | Signal | LINE | WeChat | Discord | Threema | Snapchat | Zoom | Skype | Microsoft Teams | Slack | iMessage | FaceTime |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **fees** | | | | | | $4.99 /month /user | | | features at various costs | | features at various costs[627] | additional features at various costs[628] | devices[629] | devices[630] |
| | **Notable paid features** | | | | Purchase Stickers and Emojis | Purchase Stickers | | | Premium SnapChat | E2E Encryption, meeting recordings, live phone support,[631] dial-in functionality.[632] | Skype credit to make calls to mobiles | Meeting recordings, live phone support, dial-in functionality.[633] | Full message history, group voice and video calls, 24/7 tech and admin support; identity management (SAML-based SSO)[634] | | |

627 Paid versions of Microsoft Teams are only offered as part of the Microsoft 365 bundles which comprise a variety of office applications. See Microsoft, Microsoft 365 Business, accessed 23 September 2020; Microsoft, Microsoft Teams, accessed 23 September 2020.
628 For Standard, Plus, and Enterprise Grid packages. See Slack, Slack Pricing, accessed 23 September 2020.
629 Apple Support, About iMessage and SMS/MMS, accessed 23 September 2020
630 Apple Support, Delete built-in Apple apps on your iOS 12, iOS 13 or iPadOS device or Apple Watch, accessed 23 September 2020.
631 For Business and Enterprise packages. See Zoom, Zoom Pricing, accessed 23 September 2020.
632 Available as an add-on. See Zoom, Zoom Pricing, accessed 23 September 2020.
633 Available as an add-on. See Microsoft, Compare Microsoft Teams Options, accessed 23 September 2020.
634 Available as an add-on. See Slack, Slack Pricing, accessed 23 September 2020.

# Appendix D: Review of online private messaging platforms' sign-up processes, policies, features and potential harm arising from data collection practices

This appendix provides an overview of the analysis undertaken by the ACCC in relation online private messaging services and potential consumer harms arising from the data collection practices of online private messaging, search and social media platforms.

- **Section D.1** provides an overview of the ACCC's review of the sign-up processes for selected online private messaging services.
- **Section D.2** provides an overview of the ACCC's review of selected online private messaging's consumer-facing terms and privacy policies.
- **Section D.3** considers the application of end-to-end encryption to a range of popular online private messaging services.
- **Section D.4** considers the potential harms to consumers arising from the ability of platforms providing online private messaging, search and social media services to collect consumer data, including as permitted in their terms and policies.

Our findings are based on the ACCC's review and analysis of the:

- sign-up processes and relevant terms and privacy policies applicable to consumers for selected online private messaging services from May to July 2020, and
- application of end-to-end encryption[635] on selected online private messaging services.

Details of the methodology for each of these reviews are provided as relevant below.

## D.1 ACCC's review of sign-up processes for online private messaging services

- **The ACCC's review of Facebook Messenger, Google Hangouts, WeChat, WhatsApp, Viber, Signal and Zoom found that most of these private messaging services used click-wrap agreements where a user proceeding with sign-up was deemed to have accepted the relevant terms and policies.**

As part of the Digital Platforms Inquiry, the ACCC conducted a review of sign-up processes for digital platforms providing social media and search services. The Digital Platforms Inquiry's review found that many platforms sought consumer consent to data practices using clickwrap agreements[636] that contain take-it-or-leave-it terms and bundle a wide range of consents.[637] The DPI Final Report concluded that this deepens information asymmetries between digital platforms and consumers, and prevents consumers from providing meaningful consents to the collection, use and disclosure of their data.[638]

As part of this Inquiry, the ACCC undertook a similar desk-based review of sign-up processes for consumer facing online private messaging services (online private messaging sign-up review), which found that clickwrap agreements and broad consumer consents

635 End-to-end encryption is a method of protecting data and is offered by some online private messaging services.
636 Clickwrap agreements are online agreements that use digital prompts and which typically allow users to 'accept' to the terms and policies by clicking 'I Agree' or a similar icon.
637 ACCC, DPI Final Report, 26 July 2019, p. 394. The DPI Final Report reviewed the sign-up process for Google's Gmail, Facebook, Twitter and Apple (Apple ID).
638 ACCC, DPI Final Report, 26 July 2019, p. 394.

(often implied consents provided by proceeding with sign-up and/or using the service) were commonplace. This suggests that the consent practices identified in the DPI Final Report extend to the sign-up processes for online private messaging services.

### D.1.1 Methodology

In May to June 2020, the ACCC reviewed the sign-up processes for new Australian users[639] of Facebook Messenger, Google Hangouts, WeChat, WhatsApp, Viber, Signal, and Zoom. This group of online private messaging services reflects some of those most widely used in Australia, as discussed in chapter 2.

To create new accounts, the following steps were taken on an Apple iPhone:

- The relevant online private messaging app was downloaded from the Apple App Store.
- The prompts to create an account were followed in each app. Any links within the account creation process, such as to the 'Privacy Policy', were followed and screenshots were recorded.
- Where relevant, screenshots of the sign-up processes from the ACCC's review are extracted below. The ACCC notes that the apps and any webpages accessed through the apps may have since been updated. Each screenshot below is accompanied by a reference stating the date the screenshot was taken.

At the time of the online private messaging sign-up review, Google Hangouts and Facebook Messenger required users to sign-in with an existing Google and Facebook account respectively. As set out in part D.1.2, the sign-up processes for Google Hangouts and Facebook Messenger appeared largely unchanged since the previous review undertaken during the Digital Platforms Inquiry.

### D.1.2 Sign-up process walkthrough

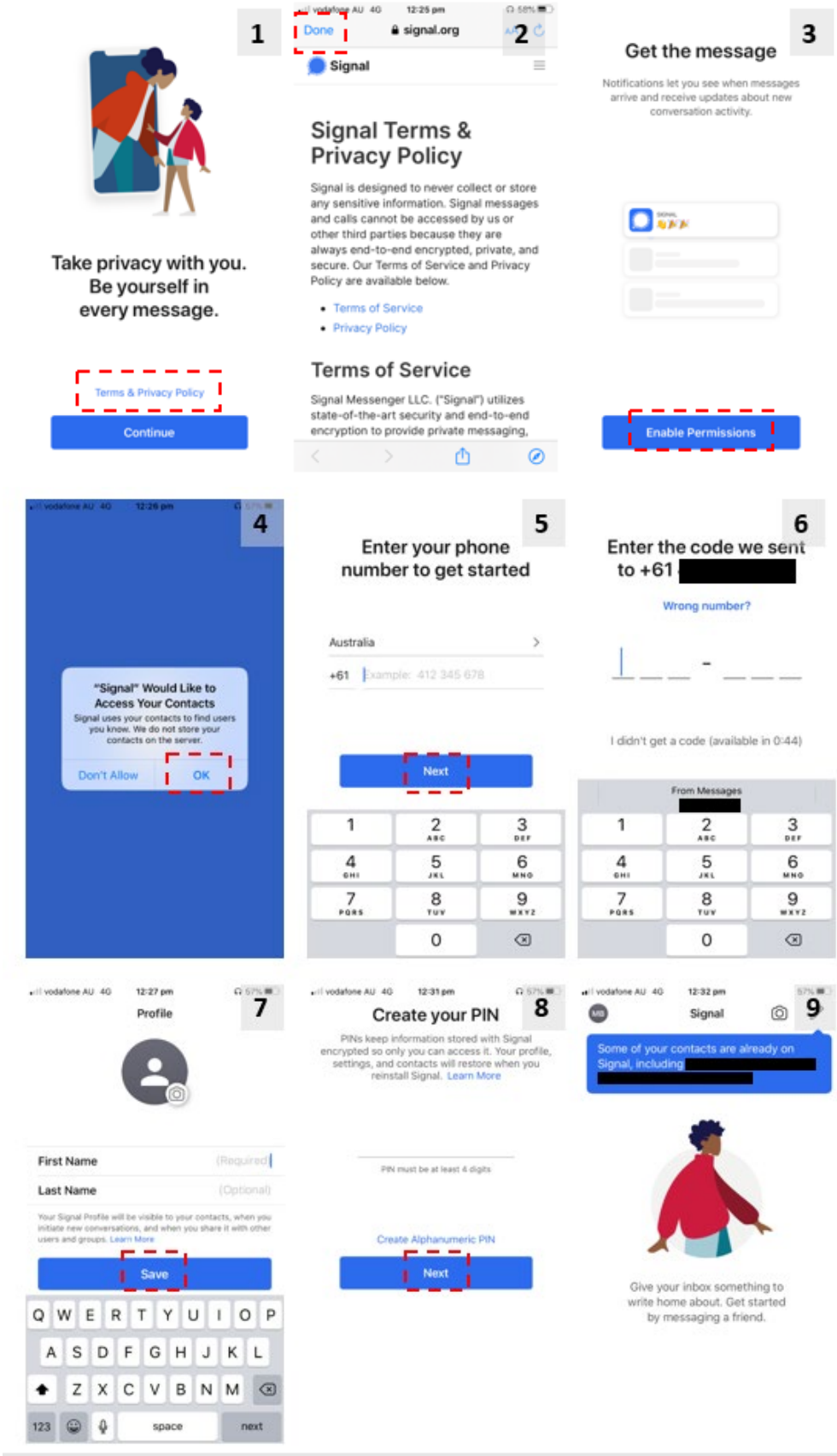
By way of example to illustrate the sign-up process a user goes through when using an online private messaging service for the first time, the below screenshots (figure D.1 and figure D.2) show these processes for Signal and WhatsApp. The screenshots provide an overview of the sign-up process from start to end, numbered sequentially, with red boxes indicating what was selected in order to reach the following screenshot.

The sign-up process varied between different services and screenshots for other online private messaging services reviewed by the ACCC are set out as relevant later in this section.

[639] That is, users accessing the relevant app from a device located in Australia with an associated Australian mobile number.

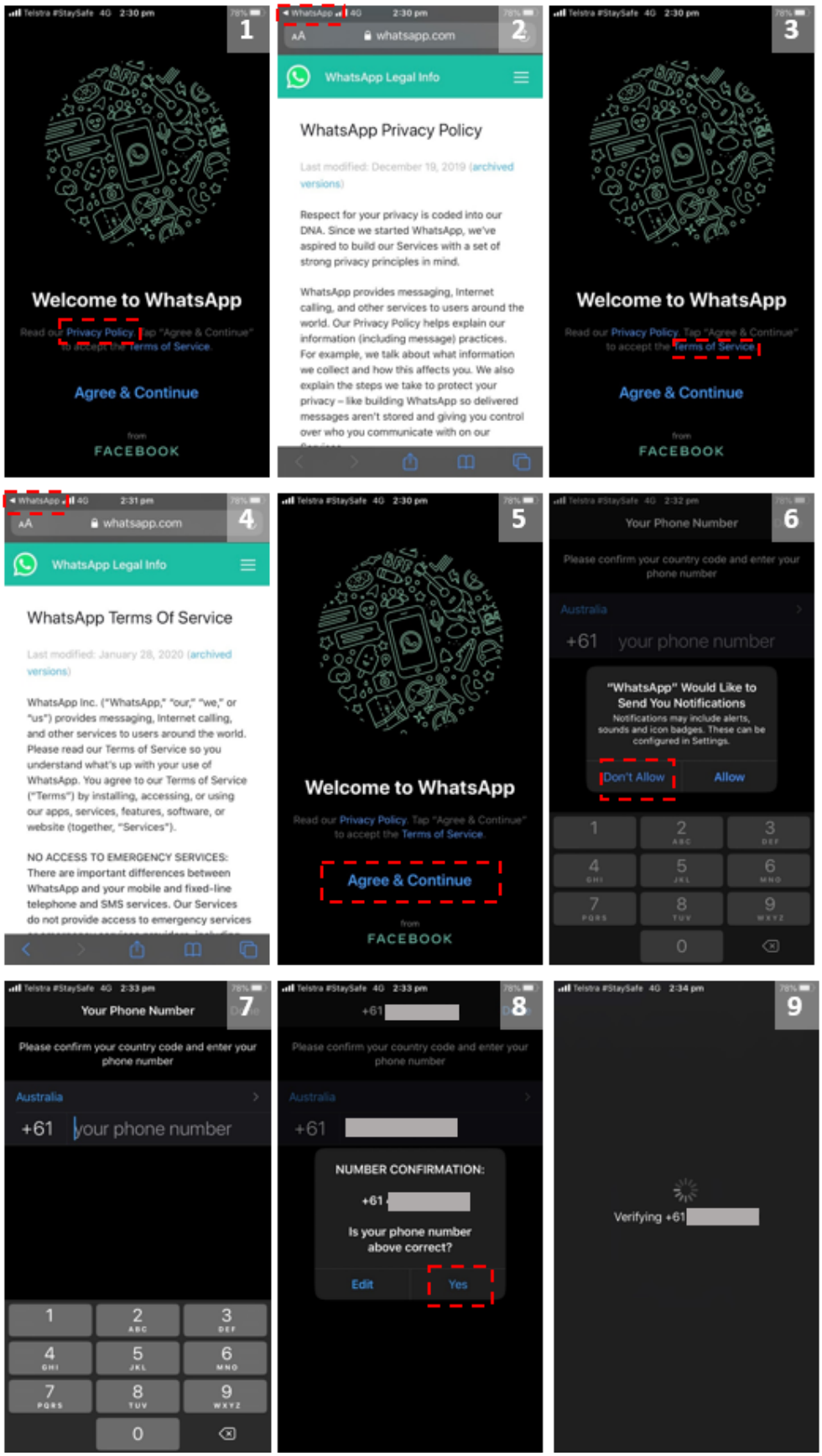
## *Signal sign-up process*

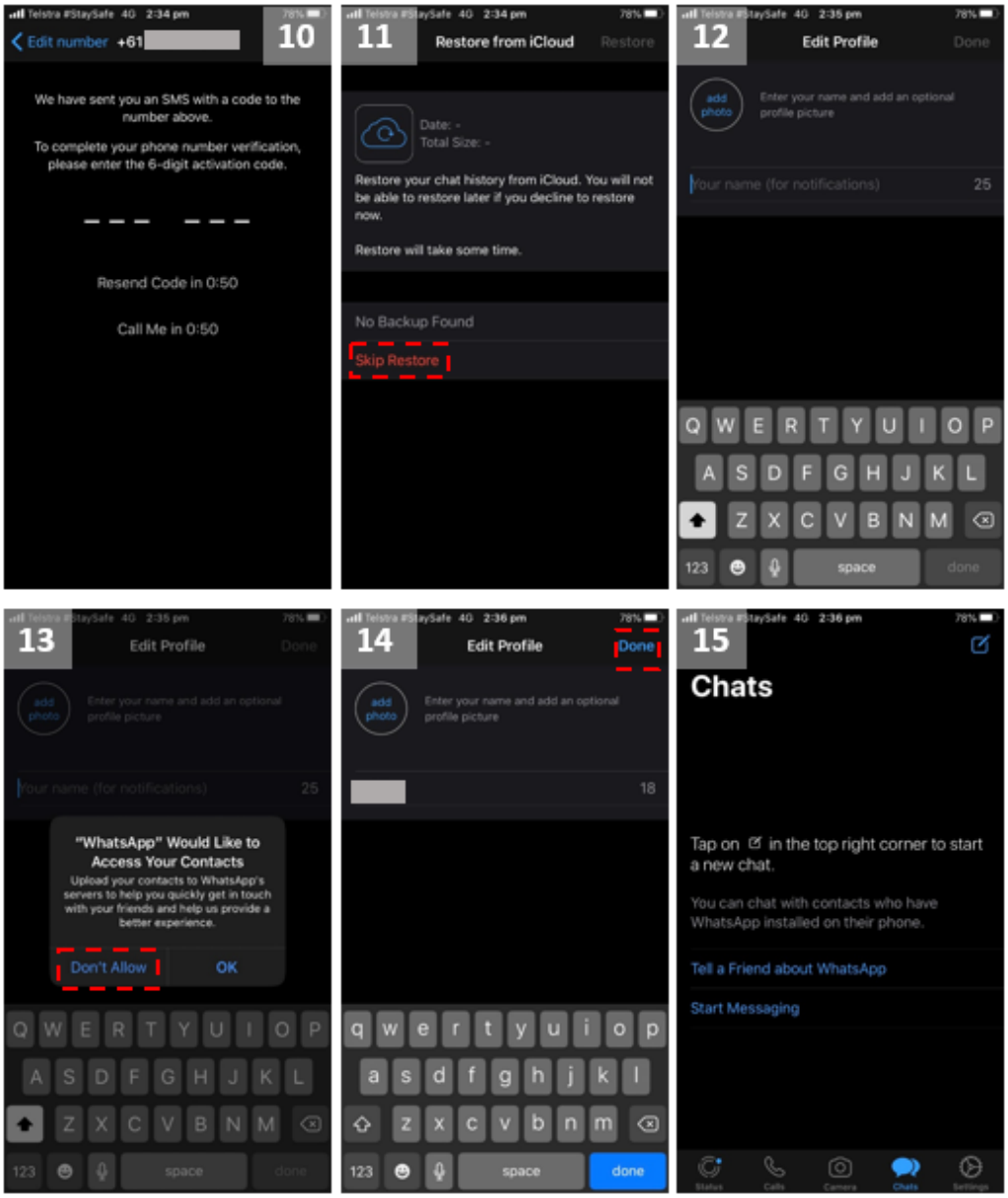
**Figure D.1: Screenshots of Signal's sign-up process – accessed 29 May 2020**



## *WhatsApp sign-up process*

**Figure D.2: Screenshots of WhatsApp's sign-up process—accessed 11 June 2020**






### D.1.3 Clickwrap agreements

The online private messaging sign-up review found that many sign-up processes involved clickwrap agreements (see section D.2 of this appendix). Users could sign up to use the service without explicitly indicating that they have read the relevant terms and conditions. Acceptance of the terms and conditions was taken to have occurred when the user proceeds with sign-up and/or uses the service.

#### *Signal, Viber, WeChat, WhatsApp and Zoom*

Of these online private messaging services, only **WeChat** had a sign-up process that required users to actively indicate that they had read and accepted the terms of service before proceeding to sign up to it, in this case by ticking a box that indicated they had done so (see figure D.3).

Of the other services, the sign-up processes all had the effect of users being able to sign-up without explicitly indicating they had read or accepted the relevant terms of policies, though the presentation of information about terms and policies differed slightly between services:

- **WhatsApp** and **Zoom's** sign-up processes allowed potential users to click on links to their respective terms of service and privacy policy. These links were embedded within sentences informing the user that proceeding with signup would mean they agreed to those terms and policies (figure D.2 and figure D.4).
- **Viber's** sign-up process informed the user that tapping 'Continue' indicated the user agreed to its 'Terms & Policies' (figure D.5). Unlike WhatsApp and Zoom, the screen that this text was on did not contain any embedded links to the terms and policies referred to, although a separate hyperlink to the privacy policy did appear in small font in the footer of the screen.
- **Signal's** sign-up process provided a hyperlink to 'Terms & Privacy Policy' above a 'Continue' button to proceed with sign-up, though unlike WhatsApp, Zoom and Viber, Signal did not include any explanatory text indicating that the user accepted the terms by signing up or using the service (figure D.1).[640]

**Figure D.3: Screenshot of WeChat's presentation of acceptance of terms—accessed 4 June 2020**

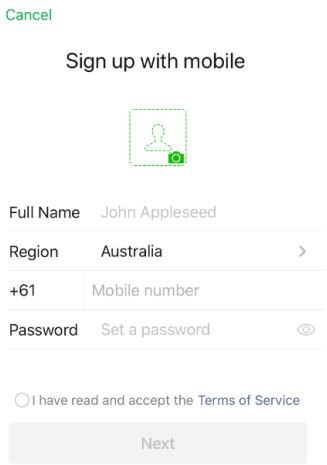
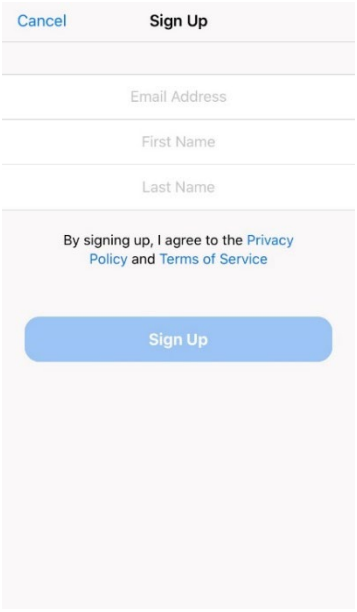
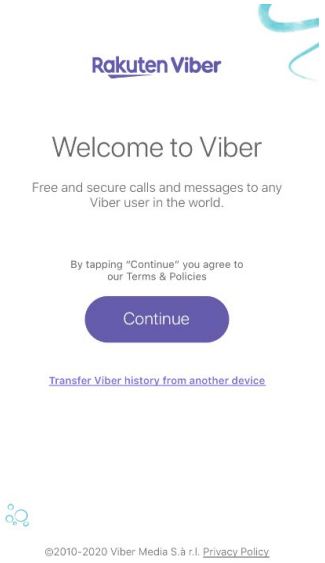



**Figure D.4: Screenshot of Zoom's presentation of acceptance of terms—accessed 11 June 2020**




[640] This is specified in the linked Terms of Service, which state: 'You agree to our Terms of Service ("Terms") by installing or using our apps, services, or website (together, "Services").' Signal, Terms & Privacy Policy, accessed 15 July 2020.

**Figure D.5: Screenshot of Viber's presentation of acceptance of terms – accessed 29 May 2020**




## *Google Hangouts and Facebook Messenger*

As noted above, use of Facebook Messenger and Google Hangouts required an existing Facebook and Google account respectively. Therefore Facebook Messenger and Google Hangouts did not require users to indicate that they had accepted the terms and policies separate to the general sign-up process for Facebook and Google respectively. Users were deemed to have accepted Facebook and Google's general terms and policies by proceeding with the general sign-up process. The online private messaging sign-up review found that:

1. **Google Hangouts** opening app screen did provide hyperlinks to Google's Terms of Service and Privacy Policy (figure D.6), but required the user to have already gone through, or to go through, Google's general account sign-up process to use the service (figure D.7). As at August 2020, the presentation and acceptance of Google's terms during the Google account sign-up process appeared unchanged since the review set out in the DPI Final Report (figure D.8 and figure D.9).[641]
2. **Facebook Messenger** required users to sign-in with an existing Facebook account, or their phone number (figure D.10)**Error! Reference source not found.**.[642] As such, clicking 'Create New Account' opened Facebook's sign-up page in a mobile web browser, requiring new users to accept Facebook's terms and policies as part of its general sign-up process. As shown in figure D.11, the presentation and acceptance of

---

641 ACCC, DPI Final Report, June 2019, pp. 576–577. The DPI Final Report found that Google's sign-up process used a clickwrap agreement where new users were deemed to have accepted Google's terms by proceeding with sign-up. The sign-up process stated 'To create a Google Account, you'll need to agree to the Terms of Service below. In addition, when you create an account, we process your information as described in our Privacy Policy…' where the Terms of Service and Privacy Policy were hyperlinked. Google also provided a list of 'key points' which summarised aspects of its Privacy Policy and data practices. As shown in

Figure D. and **Error! Reference source not found.**, this presentation remained the same as at August 2020. However, the ACCC notes that the actual content of the Terms has been updated since the DPI Final Report, see further at section D.2 of this appendix.

642 The ability to sign in with a phone number reflects that it was previously possible for users to sign-up to Messenger without a Facebook account by providing only their phone number. See K Wiggers, Facebook Messenger now requires a Facebook account to sign up, *Venture Beat,* 26 December 2019, accessed 22 September 2020; A Bradford and C de Looper, How to use Facebook Messenger without a Facebook account, *Digital Trends,* 6 April 2020, accessed 22 September 2020. However, this functionality has since been removed, so all new Messenger users must now have an existing Facebook account or create one. See Facebook, Can I sign up for Messenger if I don't have a Facebook account?, accessed 22 September 2020

terms when signing up for Facebook in August 2020 appeared unchanged since the review set out in the DPI Final Report.[643]

**Figure D.6: Screenshot of Google Hangouts' presentation of acceptance of terms – accessed 29 May 2020**

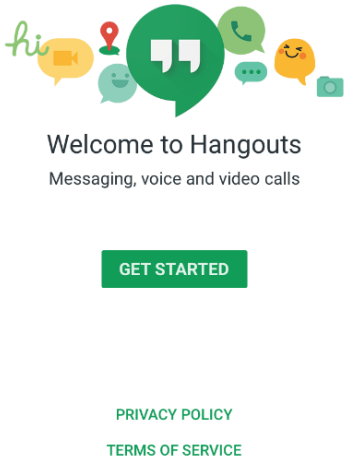
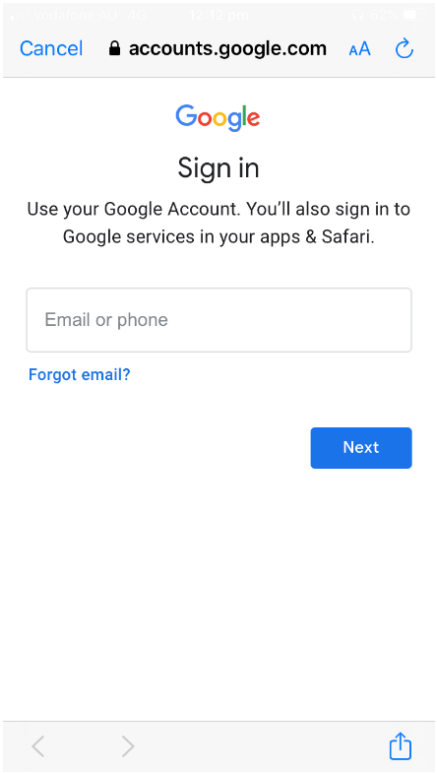
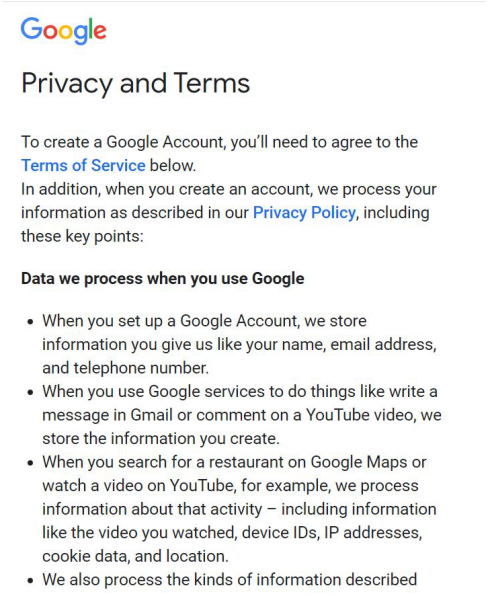



**Figure D.7: Screenshot of Google Hangouts' pop up Google sign-in page (after clicking 'Get Started' in figure D.6) – accessed 29 May 2020**




[643] ACCC, DPI Final Report, June 2019, pp. 576-577. The DPI Final Report found that Facebook's sign-up process used a clickwrap agreement where new users were deemed to have accepted Facebooks terms by proceeding with sign-up, with the 'Create an Account' page stating 'By clicking Sign-Up, you agree to our Terms, Data Policy and Cookie Policy' in small font where the terms and policies were hyperlinked. As at August 2020, this representation on Facebook's sign-up page remained unchanged, as shown in **Error! Reference source not found.**.

## Figure D.8: Google's presentation of acceptance of terms during Google account sign-up process (in browser, top of page) – accessed 13 August 2020




## Figure D.9: Google's presentation of acceptance of terms during Google account sign-up process (in browser, after scrolling to end of page) – accessed 13 August 2020

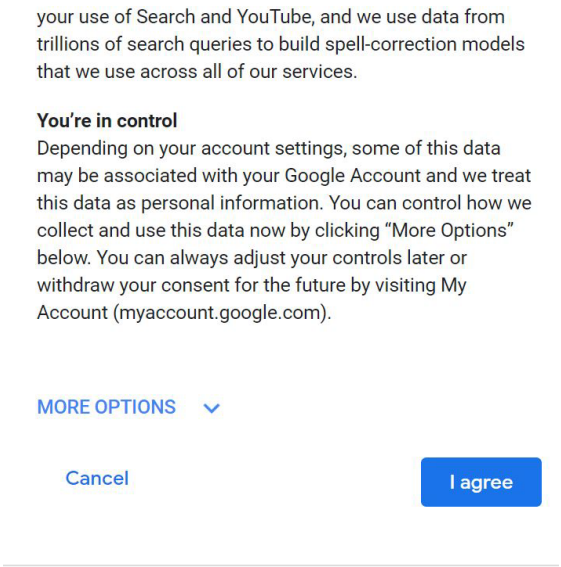


**Figure D.10: Screenshot of Facebook Messenger's sign-in page—accessed 11 June 2020**

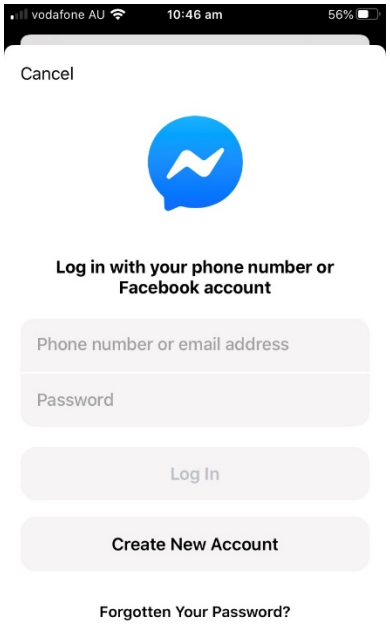
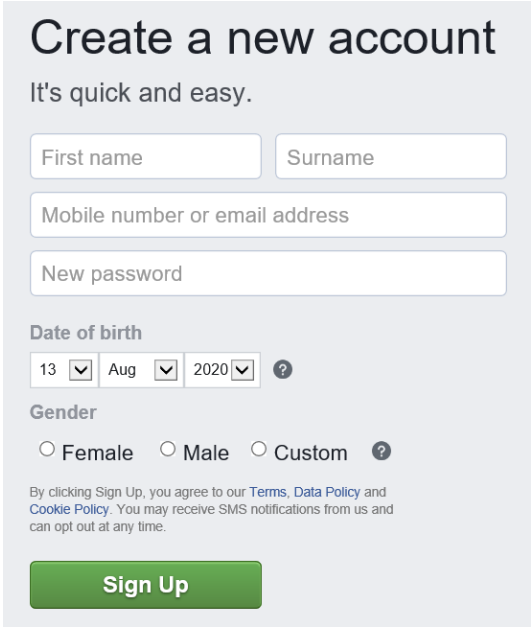



**Figure D.11: Facebook's presentation of acceptance of terms during Facebook account sign-up—accessed 13 August 2020**




## D.2 ACCC review of consumer facing terms of use and privacy policies of online private messaging services

**The ACCC's review of the consumer facing terms and privacy policies of Apple iMessage, Facebook Messenger, Google Hangouts, Signal, Viber, WeChat, WhatsApp, and Zoom found that:**

- **Many of these policies were lengthy and used complex language. The ACCC found that the policies were generally between 2,500 to 9,500 words and would take the average reader between 12 to 47 minutes to read.[644]**
- **Unclear or very broad language was common in many policies, creating ambiguity with respect to how user's data may be used, including for the purposes of targeted advertising and sharing with third parties.**
- **Most policies reviewed allow the platform to collect an extensive range of user data. Many policies also permitted the platform to change any terms with minimal, if any, direct notification to users.**

During the Digital Platforms Inquiry, the ACCC reviewed the terms and conditions that bind consumers and digital platforms providing social media and search services. These

644 The exception to these observations was Signal, whose privacy policy was 554 words and would take the average reader about two minutes to read.

platforms included Facebook, Google, Twitter, Microsoft, Apple, WhatsApp, Instagram and Snapchat.[645] This review found that many privacy policies:

- were long, complex, vague and difficult to navigate
- used different descriptions for fundamental concepts that were likely to cause significant confusion for consumers, and
- generally permitted extensive data collection practices.[646]

These observations informed the DPI Final Report's findings in relation to the extent and impact of information asymmetry between digital platforms and consumers.

As part of this Inquiry, the ACCC undertook a similar research project to examine the terms of use and privacy policies of platforms providing online private messaging services (online private messaging terms and policy review). The purpose of the review was to consider the extent to which the DPI Final Report's findings in relation to the terms and policies of key platforms also apply to online private messaging services.

The online private messaging terms and policy review found similar practices to those observed in the DPI Final Report's review, including that most online private messaging services' privacy policies are long and complex. Most online private messaging services, as with social media and search platforms, indicated that they collect a broad range of user data (including personal information, technical device information and location information), yet the ACCC found that many used ambiguous and vague language which do not provide sufficient clarity to users about the purpose and the collection, use and disclosure of user data.

This section is set out as follows:

- **Part D.2.1** sets out the methodology for the ACCC's review, including a list of the policies reviewed by the ACCC as part of the online private messaging terms and policy review.
- **Part D.2.2** sets out the length and complexity of online private messaging services' policies, as well as the digital platforms' policies reviewed in the DPI Final Report.
- **Part D.2.3** sets out various examples of unclear or broad language giving rise to ambiguity in online private messaging services' policies, including with respect to the use of user data for targeted advertising and sharing user data with third parties.
- **Part D.2.4** sets out the types and purposes of information permitted to be collected by online private messaging platforms' in their policies.
- **Part D.2.5** sets out the extent to which users can exert control over the collection and use of their personal data by online private messaging services.
- **Part D.2.6** sets out the way in which various online private messaging services incorporate international data protection regulation.

---

645 The DPI Final Report considered the terms of use and privacy policies in effect at 31 July 2018. The terms of use reviewed were Facebook, Google, Twitter, Apple, WhatsApp, Instagram and Snapchat. The privacy policies reviewed were Facebook, Google, Twitter, Microsoft, Apple, WhatsApp, Instagram and Snapchat.

646 ACCC, DPI Final Report, June 2019, p. 374.

### D.2.1 Methodology

From May to July 2020, the ACCC reviewed the consumer facing terms of use and privacy policies of Apple iMessage, Facebook Messenger, Google Hangouts, Signal, WeChat, WhatsApp, Viber and Zoom[647] (see table D.1).

In some cases, the terms of use and privacy policies that apply to online private messaging services may also apply to search, social media, or other services provided by the same platform. This was the case for Facebook Messenger, Google Hangouts and Apple iMessage.

The online private messaging terms and policy review considered:

- the terms and policies that were in effect at the time of review, as well as previous versions over the historical period from 2017 to the time of review (where available) in order to compare changes over time
- the actual content of the terms and policies (including the extent to which they allowed the platform to collect and share user data), as well as features such as the length, language and use of embedded terms that may affect a user's ability to understand the terms and policies. The ACCC analysed each policy to produce an estimated reading time,[648] and an indication of complexity of the language using the Flesch-Kincaid reading score,[649] and
- any similarities in the terms and features across platforms providing online private messaging services.

[647] Zoom updated its Terms of Service and Privacy Policies several times in the period from February to July 2020. The ACCC has noted the relevant terms and/or privacy policies where relevant in this appendix.

[648] Estimated reading time was calculated using an estimated average reading speed of 200 words per minute, using the Niram Read-O-Meter.

[649] The Flesch Readability Score calculates readability of a document based on the average number of words per sentence, and the average number of syllables per word. It is an inverse scoring system; the higher the score, the easier a document is to read. Documents that score between 50.0-60.0 are classified as 'fairly difficult to read', which translates to around a US 10th to 12th grade school level; documents scoring between 30.0-50.0 are 'difficult to read', at a US college reading level. The online private messaging terms and policy review calculated the Flesch Readability score using the Good Calculators Flesch Kincaid Calculator.

**Table D.1: Online private messaging services' terms and policies reviewed by the ACCC between May to July 2020**

| Online private messaging service | Terms and policies reviewed |
|---|---|
| Apple iMessage | Apple Media Services Terms and Conditions<br>Privacy Policy |
| Facebook Messenger | Facebook Terms of Service[650]<br>Facebook Data Policy<br>Facebook Cookies & Other Storage Technologies Policy |
| Google Hangouts | Google Terms of Service<br>Google Privacy Policy<br>Classic Hangouts Acceptable Use Policy |
| Signal | Terms of Service<br>Privacy Policy |
| Viber | Terms of Use<br>Privacy Policy<br>Ads, Cookies & Tracking Technologies Policy |
| WeChat | Terms of Service<br>Privacy Policy |
| WhatsApp | Terms of Service (European Economic Area (EEA))<br>Terms of Service (non-EEA)<br>Privacy Policy (EEA)<br>Privacy Policy (non-EEA) |
| Zoom | Terms of Service<br>Privacy Policy<br>K-12 Schools and Districts Privacy Policy |

[650] The ACCC notes that in September 2020, Facebook announced that it would update its Terms of Service, effective 1 October 2020. See Facebook, Terms of Service, as at 3 September 2020. The analysis in this appendix relates to the previous version in force at the time of the review.

### D.2.2 Length and complexity of language

The DPI Final Report found that social media and search services' terms of use and policies were often long and complex; and often incorporated numerous policies. The ACCC's review of online private messaging services made similar findings.

#### *Online private messaging services*

The online private messaging terms and policy review found that with the exception of Signal, the policies were generally between 2,500 to 9,500 words and would take the average reader between 12 to 47 minutes to read (table D.2).

When considered with the Flesch-Kincaid reading score, most of the policies (with the exception of Google Hangouts) required at least a US college level of reading. However, as noted below, while Google's privacy policy (which applies to Google Hangouts) has become easier to read, it has increased in length by approximately 2,700 words.

WeChat's privacy policy was the longest at almost 9,500 words, and also one of the most complex with a readability score of 37.8. In contrast, Signal's privacy policy was significantly shorter than the other privacy policies, with its policy taking an average reader just 2 minutes to read.

**Table D.2: Online private messaging services – estimated reading time and reading level of privacy policies reviewed May to June 2020**

| Platform | Word count (current privacy policy) | Estimated reading time | Flesch readability score[651] |
|---|---|---|---|
| **Apple iMessage**[652] | 4 181 | 20 minutes | 33.1 |
| **Facebook Messenger**[653] | 4 173 | 20 minutes | 41.4 |
| **Google Hangouts**[654] | 6 725 | 33 minutes | 54.2 |
| **Signal**[655] | 554 | 2 minutes | 43.2 |
| **WeChat**[656] | 9 429 | 47 minutes | 37.8 |
| **WhatsApp**[657] | 2 446 | 12 minutes | 45.2 |
| **Viber**[658] | 5 409 | 27 minutes | 42.5 |
| **Zoom**[659] | 3 764 | 18 minutes | 43.1 |

651 Flesch Kincaid Calculator, accessed 30 June 2020.
652 Apple, Privacy Policy, accessed 30 June 2020
653 Facebook, Data Policy, accessed 30 June 2020.
654 Google, Privacy Policy (PDF version), accessed 30 June 2020.
655 Signal, Privacy Policy, accessed 6 July 2020.
656 WeChat, Privacy Policy, accessed 6 July 2020.
657 WhatsApp, Privacy Policy, accessed 30 June 2020
658 Viber, Privacy Policy, accessed 6 July 2020.
659 Zoom, Privacy Statement, accessed 6 July 2020.

### *Platforms providing search or social media services from the DPI Final Report's review*

- While the online private messaging terms and policy review focused on online private messaging services, the ACCC also reviewed the current versions (as at May or June 2020) of the privacy policies considered in the DPI Final Report to compare any changes in length and estimated reading time since that review.
- The ACCC found that since the DPI Final Report's review, the policies of platforms providing search or social media services continued to be long and difficult to read, despite some platforms making changes to simplify their policies.[660] In particular:
- Microsoft's privacy policy[661] has increased by 9000 words—from 2523 words to 11 837 words, taking almost one hour to read, compared to 13 minutes for its previous policy. Microsoft's policy remained at a similar level of complexity, with a readability score of 36.9 from 38 (noting that a higher score indicates that a document is easier to read).[662]
- Google's privacy policy increased in length from approximately 4000 words to 6700 words, and took over 30 minutes to read (compared to 20 minutes for its previous version). However, despite being longer, Google's policy had improved in readability, from a score of 44.5 to 54.2.[663]
- Facebook's privacy policy was slightly shorter, decreasing from 4266 words to 4173 words but remained at a similar level of complexity (going from a score of 42.4 to 41.4).

**Table D.3: DPI (previous policy) and DPSI (policy as at June 2020)—estimated reading time and reading level of privacy policies reviewed June 2020**

| Platform | Word count (previous policy) | Word count (current policy) | Estimated reading time | Flesch readability score[664] |
|---|---|---|---|---|
| **Google**[665] | 4 047 | 6 725 | 33 minutes | 54.2 |
| **Facebook**[666] | 4 266 | 4 173 | 20 minutes | 41.4 |
| **Instagram**[667] | 4 266 | 4 114 | 20 minutes | 41.2 |
| **WhatsApp**[668] | 2 475 | 2 446 | 12 minutes | 45.2 |
| **Twitter**[669] | 4 364 | 4 919 | 24 minutes | 54.8 |
| **Apple**[670] | 3 642 | 4 181 | 20 minutes | 33.1 |

660 Facebook, Submission in response to the CMA's Interim Report on Online Platforms and Digital Advertising Market Study, 14 February 2020, pp. 17–19; Google, Submission in response to the CMA's Interim Report on Online Platforms and Digital Advertising Market Study, 18 December 2019, p. 4.

661 In September 2020, Microsoft updated its Privacy Statement. The analysis in this appendix relates to the previous version in force at the time of the review. See Microsoft, Privacy Statement, accessed 8 September 2020.

662 Since DPI's review of Microsoft's privacy policy, numerous changes have been made to the policy. For example, changes were made in January, February, May and June 2020 of this year. These included additional sections on certain products, such as Microsoft Edge and Microsoft Teams; as well as edits throughout the policy 'intended to improve transparency and readability'. See Microsoft, Change History for Microsoft Privacy Statement, accessed 9 July 2020.

663 Google noted that key updates to its Terms of Service (effective 31 March 2020) include the additions of the following sections 'Your relationship with Google', 'Taking action in case of problems' and 'Key Terms'. See, Google, Summary of changes to Google's Terms of Service, accessed 7 September 2020.

664 Flesch Kincaid Calculator, accessed 30 June 2020.

665 Google, Privacy Policy (PDF version), accessed 30 June 2020.

666 Facebook, Data Policy, accessed 30 June 2020.

667 Instagram, Data Policy, accessed 30 June 2020

668 WhatsApp, Privacy Policy, accessed 30 June 2020

669 Twitter, Privacy Policy, accessed 30 June 2020

670 Apple, Privacy Policy, accessed 30 June 2020

| | | | | |
|---|---|---|---|---|
| **Snap**[671] | 3 906 | 3 675 | 18 minutes | 47.2 |
| **Microsoft**[672] | 2 523 | 11 837 | 59 minutes | 36.9 |

### D.2.3 Ambiguous language on the collection, use and disclosure of user data

The DPI Final Report found that the privacy policies of digital platforms supplying social media or search services provided little clarity to users on the extent of the collection, use and disclosure of their data. This was due to ambiguity created by unclear or broad language. The online private messaging terms and policy review found that similar observations also apply to the online private messaging services reviewed.

#### *Broad language was commonly used*

The DPI Final Report highlighted the use of 'may' as an example of vague language used in many privacy policies to describe how digital platforms collect, use and share users' data.[673] As noted in the DPI Final Report, the word 'may' gives digital platforms significant discretion, and therefore prevents a consumer reading the policy from accurately determining the scope or use of user data being collected from them. The online private messaging terms and policy review similarly identified this as a common practice in the privacy policies of online private messaging services. For example:

- **Apple's** Privacy Policy used the word 'may' 63 times, most notably in relation to the collection and use of personal and non-personal data. For example, Apple's Privacy Policy stated that:

  *You may be asked to provide your personal information anytime you are in contact with Apple or an Apple affiliated company. Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising (emphasis added).*[674]

- **Google's** Privacy Policy used the word 'may' 22 times. For example, it stated that:

  *If you use our services to make and receive calls or send and receive messages, we may collect telephony log information like your phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls (emphasis added).*[675]

  The policy also stated that, depending on account settings, 'your activity on other sites and apps **may** be associated with your personal information in order to improve Google's services and the ads delivered by Google,' and that Google '**may** also collect information about you from trusted partners' (emphasis added).[676]

- **Viber's** Privacy Policy used the word 'may' 65 times. This includes in relation to its collection of activity information, stating:

  *When you interact with Public Accounts, bots and Communities on our Service, we **may** obtain information about the messages you have liked, comments you have left and also* websites *you've viewed through links in them or otherwise links you have viewed from*

---

671 Snap, Privacy Policy, accessed 30 June 2020
672 Microsoft, Privacy Policy, accessed 30 June 2020 (up to 'How to contact us' and excluding product specific information).
673 ACCC, DPI Final Report, 26 July 2019, pp. 405-406.
674 Apple, Privacy Policy, accessed 11 August 2020.
675 Google, Privacy Policy, accessed 11 August 2020.
676 Google, Privacy Policy, accessed 11 August 2020.

*within Viber. When you send links through messages, with your permission, we **may** collect data about such links you have visited (emphasis added).*[677]

- **WeChat's** Terms of Service used the word 'may' 71 times, including in relation to what information third parties may access, stating 'Third parties that provide third party services **may** collect your Information (including your Personal Information and Log Data), and set cookies on your computer, or device to enable such features to function properly' (emphasis added).[678]

### *Some privacy policies made ambiguous representations about advertising, including targeted advertising, on the service*

The supply of online advertising services is a key source of revenue for a number of popular platforms which supply online private messaging services.[679] However, the online private messaging terms and policy review found that disclosures regarding advertising varied between the platforms reviewed, and for some platforms, over the time period reviewed.

Some online private messaging services made clearer representations about the use of users' personal information for advertising on the service, for example:

- **Viber's** Privacy Policy made several disclosures regarding advertising, including a separate section on its advertising partners. Additionally, targeted advertising is one of the reasons provided by Viber for collecting users' information.[680]
- **Signal's** terms contained a list of instances where Signal may share user data, which does not include advertising, and also stated that it never sells, rents or monetises user data or content.[681] Separately, its home page stated that 'there are no ads, no affiliate marketers and no creepy tracking in Signal'.[682]

Other online private messaging services used vague language to describe the use of user information for advertising, listed it after other purposes for collecting user data, or else framed advertising as a benefit to users. For example:

- **WhatsApp's** Privacy Policy stated that it did not allow third party banner ads on WhatsApp, but it does allow for commercial messaging, including for the purposes of 'marketing' on its platform.[683]
- **Zoom's** Privacy Policy (dated July 2020) stated that 'There are no interest-based advertising cookies on Product Pages'[684] (such as webpages users are taken to after clicking a link to join a meeting). However, Zoom stated that it does use data obtained

---

677 Viber, Privacy Policy, accessed 11 August 2020.
678 WeChat, Privacy Policy, accessed 11 August 2020.
679 ACCC, DPI Final Report, 26 July 2019, pp. 377–381.
680 Viber's Privacy Policy stated that it uses users' registration and account information to 'personalize your experience by providing content (such as games) on the Service, including targeted advertising of Viber services and other 3rd party services that we believe may be of most interest to you.' See Viber, Privacy Policy, accessed 8 July 2020.
681 Signal, Privacy Policy, accessed 6 July 2020.
682 Signal, Signal: Speak Freely, accessed 8 July 2020.
683 WhatsApp's Privacy Policy stated: 'We will allow you and third parties, like businesses, to communicate with each other using WhatsApp, such as through order, transaction, and appointment information, delivery and shipping notifications, product and service updates, and *marketing*' (emphasis added). See WhatsApp, Privacy Policy, accessed 8 July 2020. The ACCC understands that at this stage, WhatsApp does not monetise the marketing channel, but potentially could do so if this functionality was added to their Business API product. Reports noted that WhatsApp was considering introducing advertising, but announced that it would no longer proceed after receiving criticism. See C Welch, Facebook backs off plan to plaster ads all over WhatsApp, *The Verge*, 16 January 2020, accessed 22 September 2020. At this stage, the WhatsApp Business API is still in a 'limited public preview'. See Facebook, Facebook for Business, accessed 22 September 2020.
684 Zoom, Privacy Statement, accessed 10 July 2020.

from its 'marketing websites' (such as zoom.us and zoom.com) for advertising.[685] This distinction was absent from Zoom's policies prior to 29 March 2020.

- **Facebook's** Data Policy, which applies to Facebook Messenger, stated that it works with third party partners (which it subsequently explains includes advertisers) to ultimately benefit Facebook users: 'We work with third party partners who help us provide and improve our Products or who use Facebook Business Tools to grow their businesses, *which makes it possible to operate our companies and provide free services to people around the world*' (emphasis added).[686]
- **WeChat's** Terms of Service are also couched in terms of how this benefits its users. It stated that 'WeChat may include advertising or commercial content' and that users agree that '…we may use targeted advertising to try to make advertising more *relevant* and *valuable* to you' (emphasis added).[687] WeChat's Privacy Policy also specifies that WeChat collects personal information to 'personalise WeChat, including by providing personalised advertisements'.[688]

### *Ambiguous disclosures relating to data shared with third-parties*

As with the DPI Final Report's review of social media and search services' terms and policies, the online private messaging terms and policy review similarly found that the disclosure around sharing data with third parties was vague for some online private messaging services.

Generally, it was not clear from the language in online private messaging services' terms and policies who were considered to be third-parties, or what information was shared with them. Given this, users are likely to find it hard to understand which third parties have access to their personal data.

Online private messaging services used a range of terms to describe third parties that may receive or provide user data, including phrases such as 'partner' or 'trusted partner' (see table D.4). These third parties were sometimes referred to in contexts that make it difficult for users to identify exactly who they were agreeing to have their information shared with. For example:

- **WhatsApp**'s Privacy Policy stated that in addition to sharing information with other Facebook companies[689], it works with various third party providers, who are not expressly identified:

  *We work with third party providers to help us operate, provide, improve, understand, customize, support, and market our Services. When we share information with third party providers, we require them to use your information in accordance with our instructions and terms or with express permission from you.*[690]

- **WeChat's** Terms of Service stated that it may share user 'content' (including data, information and media) with third parties which were not identified but described as 'third parties that we work with to help provide, promote, develop and improve WeChat in accordance with the WeChat Privacy Policy.'[691] WeChat's Privacy Policy did provide some information about who these third parties may be and included further detail about when information will be shared, including that 'only where necessary will we share your

---

685 This is also set out in Zoom's Security White Paper dated June 2020, which stated: 'We do not use data we obtain from your use of our services, including your meetings, for any advertising. We do use data we obtain from you when you visit our marketing websites, such as zoom.us and zoom.com.' See Zoom, Security White Paper, June 2020, p. 8.
686 Facebook, Data Policy, accessed 8 July 2020.
687 WeChat, Terms of Service, accessed 8 July 2020.
688 WeChat, Privacy Policy, accessed 8 July 2020, see Addendum for Californian Residents section.
689 WhatsApp, Privacy Policy, accessed 8 July 2020.
690 WhatsApp, Privacy Policy, accessed 8 July 2020.
691 WeChat, Terms of Service, accessed 8 July 2020.

information with selected recipients who have a legal basis and valid jurisdiction to request such data'.[692]

- **Zoom's** Privacy Statement (dated July 2020) stated that it 'may' share personal data with 'Zoom Partners' under certain, non-exhaustive circumstances. Zoom noted that its partners have contractually agreed to comply with appropriate privacy and security obligations.'[693] However 'Zoom Partners' was not defined in the Privacy Statement.
- **Signal's** Terms & Privacy Policy stated that it works with 'Third Party Providers', 'service providers or partners' and 'third parties'. Although it did not provide an exhaustive list of third parties are, the examples listed ('Third Party Providers sending you a verification code and processing your support tickets') coupled with Signal's policy of sharing limited user data (see above) suggested that these third parties were those related to providing Signal's service.[694]

**Table D.4: Sample of online private messaging services' terms referring to third parties that may provide or receive user data (as at July 2020)[695]**

| Platform | Third parties who may receive user data | Third parties who may provide user data |
|---|---|---|
| **Apple iMessage** | 'third parties'<br>'your carrier'<br>'companies who provide services such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys'<br>'our partners and licensees' | 'other persons if that person has shared their content with you using Apple products, sent gift certificates and products, or invited you to participate in Apple services or forums'<br>'datasets such as those that contain images, voices or other data that could be associated with an identifiable person' |
| **Facebook Messenger** | 'our partners'<br>'third-party apps, websites or other services that use, or are integrated with, our Products'<br>'third party partners'<br>'partners who use our analytics services'<br>'advertisers'<br>'measurement partners'<br>'partners offering goods and services in our products'<br>'vendors and service providers'<br>'researchers and academics' | 'partners'<br>'third party data providers'<br>'advertisers, app developers and publishers' |

692 WeChat, Privacy Policy, accessed 17 July 2020.
693 Zoom, Privacy Statement, accessed 8 July 2020.
694 Signal, Terms & Privacy Policy, accessed 9 July 2020.
695 This table provides a sample of the terms used by online private messaging services to describe third parties, and is not intended to provide an exhaustive summary of third parties that may receive or provide user data.

| | | |
|---|---|---|
| **Google Hangouts** | 'our affiliates and other trusted businesses or persons'<br>'our partners — like publishers, advertisers, developers, or rights holders' | 'trusted partners, including marketing partners … and security partners'<br>'advertisers' |
| **Signal** | 'third parties … For example, our Third-Party Providers send a verification code to your phone number when you register for our Services' | Not specified. |
| **Viber** | 'app Providers and Other Third-Parties'<br>'advertising partners'<br>'third party advertising partners, and advertising service providers (such as Google)' | 'social media sites if users of those sites give us access to their profiles'<br>'outside records (e.g. demographic information and additional contact information)'<br>'trusted third parties' |
| **WeChat** | 'service providers'<br>'WeChat Official Accounts and Mini Program operators, other services via which you choose to use WeChat Login for third-party apps'<br>'third party services or features that are made available within WeChat' | 'service providers'<br>'WeChat Official Accounts and Mini Program operators, other services via which you choose to use WeChat Login for third-party apps' |
| **WhatsApp** | 'third party services'<br>'third-party providers' | 'third party services'<br>'third-party providers' |
| **Zoom** | 'third-party partners'<br>'sub-processors or service providers' | 'data enrichment services (only in connection with Marketing Pages)'<br>'email marketing lists (where permitted under applicable law)' |

In some policies, it was also unclear whether user data shared with third parties was sold to those parties, particularly where policies noted that their handling of data may amount to a 'sale' of data under overseas legislation (in particular, the California Consumer Privacy Act, see box D.1). For example:

- **Viber's** Privacy Policy stated that it 'may' process users' data in such a way that would be considered to be a 'sale of personal information' under the California Consumer Privacy Act (CCPA)[696]. It also contained references to 'sharing' of user information with 'third party advertising partners' without stating whether this information was sold.[697]
- **Zoom's** previous Privacy Policy (updated 29 March 2020), repeatedly stated that Zoom does not sell users' data, but elsewhere stated that some of what Zoom did may be considered 'sale' under the definition in the CCPA.[698] This differed from earlier versions of Zoom's Privacy Policy (up until 29 March 2020) that did not place emphasis on not selling users' data, and more clearly articulated that Zoom sends users' data to third parties. Under the policy as at July 2020, the reference to the CCPA definition of 'sale' has been moved to a separate California Privacy Rights Statement.

696 Viber, Privacy Statement, accessed 8 July 2020.
697 Viber, Privacy Statement, accessed 8 July 2020.
698 Zoom, Privacy Policy, accessed 31 March 2020.

### D.2.4 Extent of user information collected

The types of user information collected by online private messaging services and the reasons or purposes provided for its collection varied across the terms and policies reviewed. Generally, most online private messaging services, with the exception of Signal, permitted the collection of a broad range of information from users (including personal information, technical information about a user's device, and location information), and the purposes of the collection were not always clear.

Additionally, as was noted in the review conducted for the DPI Final Report, in some cases the policies reviewed confirmed that information is collected by a platform even when users are not logged-in, or do not have accounts.[699]

An overview of the types of information that may be collected by each online private messaging service according to terms and policies, and the reasons provided for collecting this information, is summarised in table D.5.

**Table D.5: Key types of information collected by online private messaging services according to terms and policies and the reasons provided (based on current privacy policies as at 9 July 2020)**

| Platform | Key information collected | Reasons for collecting information |
|---|---|---|
| **Apple iMessage** | information used to create an Apple ID[700]<br>contact details of friends and family users to share content with using Apple products | 'to fulfil your requests, provide the relevant product or service, or for anti-fraud purposes' |
| **Facebook Messenger** | information and content provided by users<br>device information<br>information obtained from third party partners | to 'provide, personalise and improve our products; provide measurement, analytics and other business services; promote safety, integrity and security; communicate with you; and research and innovate for social good' |
| **Google Hangouts** | information about the apps, browsers and devices used to access Google's services<br>user's activities in Google services (including search terms, videos watched, views and interactions with content and ads, voice and audio information, purchase activity, people with whom the user communicates or shares content, and Chrome browsing history)<br>user's activity on third party sites and apps that use Google services<br>location information | to 'provide our services', 'maintain and improve our services', 'develop new services, 'provide personalized services, including content and ads', 'measure performance', 'communicate with you, 'protect Google, our users, and the public |

699 ACCC, DPI Final Report, 26 July 2019, p. 600. For example, Facebook's Data Policy notes that its third party partners 'provide information about your activities off Facebook—including information about your device, websites you visit, purchases you make, the ads you see and how you use their services—whether or not you have a Facebook account or are logged in to Facebook': Facebook, Data Policy, accessed 25 August 2020.

700 The Apple Identifier for Advertisers (or Apple Advertising ID) is a unique alphanumeric string that is randomly assigned to an Apple device. The ID can track activity on the device, such as user clicks, interactions and installs, which advertisers can use to serve targeted advertising. See P Dhamane, Does this app use the Advertising Identifier (IDFA)?, *Medium*, 24 January 2020, accessed 22 September 2020; Apple, Advertising & Privacy, accessed 22 September 2020.

| | | |
|---|---|---|
| | telephony log information | |
| **Signal** | phone number<br>device information<br>contacts who also use Signal | 'to provide our Services to you and other Signal users' |
| **Viber** | registration and account information<br>social media information (such as when users sign in to Viber through third party social media sites, or potentially through friends or connections of users)<br>a user's activity on Viber<br>information from 'outside records'<br>device and location information | to 'make our service available', 'improve our services', 'provide interesting offerings to you and others', 'process your payments' |
| **WeChat** | personal information<br>location information<br>chat data (stored temporarily on servers)<br>credit card information<br>data collected through cookies and other trackers<br>device data (such as the media stored on user's devices)<br>pseudonymised and aggregated personal information<br>biometric information | 'to maintain your WeChat account'<br>'to provide personalised help and instructions'<br>'to develop new and improve existing services'<br>'to administer the WeChat platform'<br>'to better understand how you access and use WeChat'<br>'for internal operations, including troubleshooting, data analysis, testing, research, security, fraud-detection, and account management' |
| **WhatsApp** | account information (such as mobile phone number and contacts who also use WhatsApp)<br>usage and log information<br>device and connection information<br>status information | 'to help us operate, provide, improve, understand, customize, support, and market our Services' |
| **Zoom** | account user data (such as name and contact details)<br>location information<br>data collected from cookies and other tracking technology on Zoom's marketing websites and other online services | to 'provide Zoom services'<br>to 'suggest choices such as language preferences'<br>'marketing, including facilitating tailoring of advertising you see when you are on other online services' |

### *Collection of information through cookies and tracking technologies*

The terms and policies of online private messaging platforms that permitted the collection of a broad range of user information also extend to permitting the placement of cookies and other tracking technologies. This could enable the collection of extensive information about users' activity, including for the purposes of targeted advertising.

The DPI Final Report's review of terms and policies found that certain digital platforms providing social media and search services, such as Google, Facebook and Twitter, generally did not clearly outline the extent to which users were tracked for online advertising purposes.[701] These platforms instead described cookies and other tracking technologies as being beneficial to users, and emphasised the importance of cookies for product improvement or user convenience.

We made similar observations in relation to online private messaging services. The policies of all online messaging platforms reviewed, with the exception of Signal, emphasised the usefulness of cookies or other tracking technologies (and in some cases discouraged users from disabling or deleting them). For example:[702]

- **Viber's** Ads, Cookies & Tracking Technologies Policy stated:

  *We may use cookies for a variety of purposes and to enhance your online experience, for example, by remembering your log-in status and viewing preferences from a previous use of our Services, for when you later return to the Services.*

  *Please note, however, that without HTTP cookies and HTML5 local storage, you may not be able to take full advantage of all the features of our Services and some parts of the Services may not function properly.'*[703]

- **WhatsApp's** Cookies Policy stated that:

  *We use cookies to understand, secure, operate and provide our Services. For example, we use cookies to provide WhatsApp for web and desktop and other Services that are web-based, improve your experiences, understand how our Services are being used, and customize our Services.*[704]

Furthermore, online private messaging services sometimes described the use of cookies and other tracking technologies as common or standard practice. For example:

- **Apple's** Privacy Policy stated that '*As is true of most internet services, we gather some information automatically and store it in log files*. This information includes Internet Protocol (IP) addresses, browser type and language, Internet service provider (ISP), referring and exit websites and applications, operating system, date/time stamp, and clickstream data' (emphasis added).[705]
- **Viber's** Ads, Cookies & Tracking Technologies Policy stated that '*Like many companies*, we use tracking technologies on our Services' (emphasis added).[706]

---

[701] ACCC, DPI Final Report, 26 July 2019, p. 413.

[702] See also:
Apple, Privacy Policy, accessed 8 July 2020: 'Apple also uses cookies and other technologies to remember personal information when you use our website, online services, and applications. Our goal in these cases is to make your experience with Apple more convenient and personal.'
WeChat, Cookies Policy, accessed 8 July 2020: 'We use cookies to: retain authentication information in order to provide WeChat to you; provide mapping and location-based services (such as 'Shake' and 'People Nearby'), which require your location; retain your language preference; track traffic flow and patterns of travel in connection with WeChat; understand the total number of visitors to WeChat on an ongoing basis and the types of operating systems (e.g. iOS, Android) used; monitor the performance of WeChat and to continually improve it; and customise and enhance your WeChat experience.'
Facebook, Cookies & Other Storage Technologies, accessed 16 July 2020: 'Cookies help us provide, protect and improve the Facebook Products, such as by personalizing content, tailoring and measuring ads, and providing a safer experience.'
Google, Privacy Policy, accessed 9 July 2020: 'You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.'
Zoom, Cookie Policy, accessed 8 July 2020. 'Certain features of Zoom's Products and services depend on cookies. Please be aware that if you choose to block cookies, you may not be able to sign in or use those features, and preferences that are dependent on cookies may be lost. If you choose to delete cookies, settings and preferences controlled by those cookies, including advertising preferences, will be deleted and may need to be recreated.'

[703] Viber, Ads, Cookies & Tracking Technologies Policy, accessed 8 July 2020

[704] WhatsApp, Cookies Policy, accessed 8 July 2020.

[705] Apple, Privacy Policy, accessed 8 July 2020.

[706] Viber, Ads, Cookies & Tracking Technologies Policy, accessed 8 July 2020.

- **Zoom's** Privacy Statement (dated July 2020) stated: '*Like many companies*, we use advertising services that try to tailor online ads to your interests based on information collected via cookies and similar technologies on our Marketing Pages'[707] (emphasis added).

### D.2.5 Extent of user control

#### *User control of data collection and ability to opt out*

Some online private messaging services stated that users could opt-out or withdraw consent for certain data collection or use, but the extent to which users can in practice opt-out of data collection is not always clear from the platforms' policies. For example:

- **WeChat's** Privacy Policy stated that users can withdraw their agreement to the sharing of information with third parties by changing their preferences. The process appears to require unfollowing, deleting or de-authorising every individual third party service, and even after doing so, then also relies on WeChat requesting that the third party delete the information at their end.[708]
- **Zoom's** previous Privacy Policy (dated 29 March 2020) listed a number of ways users could potentially opt out of data collection. For example, users 'may' have the right to withdraw consent for processing personal data, such as requesting to be removed from marketing communications after having signed up for them. It was not clear in what other instances users could withdraw consent.[709] However, Zoom's Privacy Policy (dated July 2020) appeared to only allow users to opt-out of data collection if they reside within the European Economic Area.[710]

Similarly, **Google Hangouts** is governed by Google's Privacy Policy, which Google stated is 'as user friendly and accessible as possible'.[711] From the online private messaging terms and policy review, the ACCC considered that it was not clear on the face of the policy whether users are able to completely opt-out of targeted advertising. In particular, the ACCC found different disclosures about opting-out of, or limiting, use of data for targeted advertising by Google on a number of different webpages. These collectively suggested that even if a user could opt-out of receiving targeted ads, at least some data would still be collected by Google. These disclosures included the following:

- Google's Privacy Policy stated that users can use the 'Privacy Checkup' feature, 'which provides an opportunity to review and adjust important privacy settings'[712] including Google Search History, Google Ad settings, Google Analytics opt-out and Chrome Cookie Settings.
- Two subsequent clicks from the 'Privacy Checkup' reference in Google's Privacy Policy took users to the 'Safeguarding your data' page, which suggested that users may be able to 'limit use of their analytics data' (figure D.12).[713]
- Google's 'Data and personalisation' page allowed 'Ad personalisation' to be turned off.[714] This page also noted that users could download and install the 'Google Analytics Opt-out

---

[707] Zoom, Privacy Statement, accessed 8 July 2020.
[708] See WeChat, Help Center, accessed 9 July 2020: 'After taking one of the steps above, WeChat will inform the third party developer of your action so that they know to delete any additional information that you have previously disclosed to their service'.
[709] Zoom, Privacy Policy, accessed 31 March 2020.
[710] Zoom, Privacy Statement, accessed 25 July 2020.
[711] Google, Submission in response to the CMA's Interim Report on Online Platforms and Digital Advertising Market Study, p 4.
[712] Google, Privacy Policy, accessed 9 July 2020.
[713] Google, Safeguarding your data, accessed 9 July 2020.
[714] Google, Data & personalisation, accessed 10 July 2020.

Browser Add-On' to opt-out of having their data collected on third party websites by Google Analytics (figure D.13).

- However a Google Ads help page explained that 'Once you've turned off personalization, Google will no longer use your info to personalize your ads. Ads can still be targeted with info like your general location or the content of the website you're visiting' (figure D.14).[715]

**Figure D.12: Screenshot of Google's 'Safeguarding your data' web page – accessed 9 July 2020**

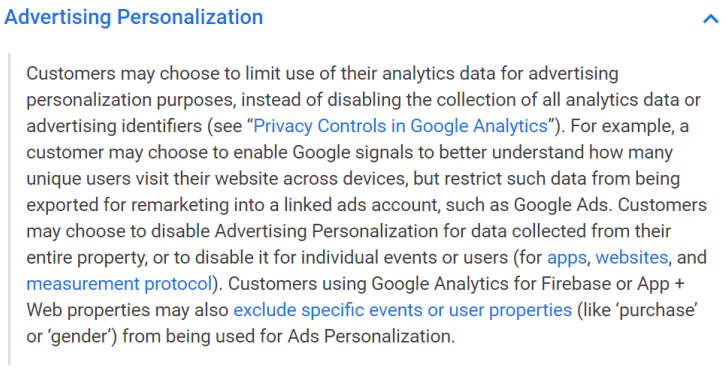



**Figure D.13: Screenshot of Google's 'Data and personalisation' web page – accessed 9 July 2020**

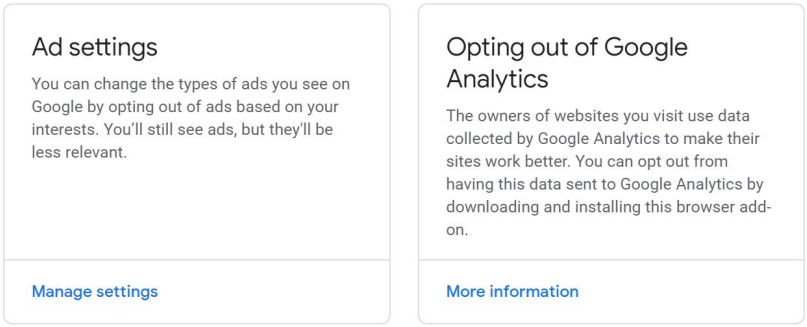
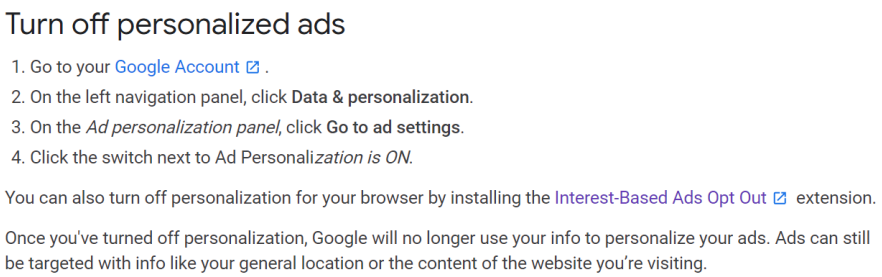



**Figure D.14: Screenshot of Google's 'Ads Help—Control the ads you see' web page—accessed 10 July 2020**




## *Notification of changes to the terms*

Many online private messaging services' terms and policies indicated that users would not be directly notified of changes to the terms, or used language that indicated notification was

[715] Google, Ads Help – Control the ads you see, accessed 10 July 2020.

at the discretion of the service. Furthermore, in some cases, continued use of the service indicated consent to any changes. For example:[716]

- **Google Hangouts** is subject to Google's overarching terms, which stated that users will be given 'reasonable advance notice' of changes that are 'material', though this did not apply in certain circumstances including where the changes related to the launch of a 'new service or feature'.[717]
- **Zoom's** Terms of Service noted that it will 'exercise commercially reasonable business efforts' to notify users of 'material changes', and continued use after ten business days was deemed to be consent.[718]
- **WhatsApp's** Privacy Policy indicated that it would provide notice of amendments 'as appropriate', as well as updating the 'Last Modified' date on the Privacy Policy, and users were instructed to 'review [the] Terms from time to time.'[719] Continued use indicated acceptance of any changes.

The ACCC notes that Facebook recently introduced a 30-day notification period for proposed changes to its terms of service.[720] With the addition of this notification period, **Facebook's** Terms of Service, which applies to Facebook Messenger, now states that:

> *We will notify you (for example, by email or through our Products) at least 30 days before we make changes to these Terms and give you an opportunity to review them before they go into effect, unless changes are required by law. Once any updated Terms are in effect, you will be bound by them if you continue to use our Products.*[721]

### D.2.6 Incorporation of data protection regulation

The ACCC found that the way in which data protection regulation was incorporated into online private messaging platforms' policies varied across platforms, with some applying the same protections to all users and others specifying certain terms or protections only for users in particular jurisdictions.

Some online private messaging services had separate terms and policies for users in different jurisdictions. For example, **WhatsApp** had separate Terms of Service and Privacy Policies for users located in the European Economic Area (EEA) to users located outside of it,[722] due to rights available in the EEA under the European General Data Protection Regulation (GDPR).[723] While the non-EEA Privacy Policy stated that Facebook may use information from WhatsApp (excluding message content) to 'improve your experiences within their services such as […] showing relevant offers and ads,'[724] the EEA Privacy Policy stated that 'Facebook does not use your WhatsApp account information to improve your

---

716 See also:
Signal, Terms & Privacy Policy, accessed 7 September 2020: 'Signal may update the Terms from time to time. When we update our Terms, we will update the 'Last Modified' date associated with the updated Terms. Your continued use of our Services confirms your acceptance of our updated Terms and supersedes any prior Terms. You will comply with all applicable export control and trade sanctions laws'.
WeChat, Terms of Service, accessed 7 September 2020: 'We may make changes to these Terms (and any applicable Additional Terms) over time …so please come back and review these Terms regularly. Where we consider that such changes are reasonably material, we will (where reasonably practicable) notify you (via http://www.wechat.com, direct communication to you, on this page or the relevant page for the relevant additional terms or policy, or other means), prior to such changes becoming effective. By continuing to use WeChat after we make any changes to these Terms, you are agreeing to be bound by the revised Terms.'

717 Google, Terms of Service, accessed 6 May 2020.

718 Zoom, Terms of Service, accessed 28 May 2020.

719 WhatsApp, Privacy Policy, accessed 3 June 2020.

720 For example, the inclusion of a 30 day notification period was not in Facebook's Terms of Use as at 11 February 2019.

721 Facebook, Terms of Use, accessed 8 July 2020.

722 WhatsApp, WhatsApp Legal Info (non-European Region), accessed 9 July 2020; WhatsApp, WhatsApp Legal Info (European Region), accessed 9 July 2020.

723 For a discussion of consent requirements under the GDPR see ACCC, DPI Final Report, 26 July 2019, pp. 465-467.

724 WhatsApp, WhatsApp Legal Info (non-European Region) - Privacy Policy, accessed 9 July 2020.

Facebook product experiences or provide you with more relevant Facebook ad experiences.'[725]

WhatsApp also had a supplementary 'California Privacy Notice' and 'Brazil Privacy Notice' that applied to users residing in California and Brazil respectively.[726] These provided additional information and rights for users subject to the California Consumer Privacy Act (CCPA) and the Brazilian General Data Protection Law (LGPD[727]) (see box D.1), and applied in addition to WhatsApp's general non-EEA Terms of Service and Privacy Policy. For example, the California Privacy Notice stated that the CCPA gives users the right to access the personal information collected about them by WhatsApp in the last 12 months and to request deletion of personal information collected by WhatsApp.[728] This right did not appear in WhatsApp's non-EEA Privacy Policy.

**Box D.1: The California Consumer Privacy Act and Brazilian General Data Protection Law**

In California, the CCPA gives Californian residents certain rights relating to the collection and use of their personal information by certain businesses.[729] Rights under the CCPA include a right to be notified of the types of information a business will collect and what they can do with it (at or before the point of collection), a right to ask businesses to disclose what personal information of yours they already hold, a right to request that a business delete your personal information, and a right to request that your personal information not be sold.[730] Under the CCPA 'sale' is defined broadly as meaning 'selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for *monetary or other valuable consideration'* (emphasis added).[731]

In Brazil, the LGPD imposes various restrictions on the collection, usage, storage and treatment of personal data belonging to anybody located in Brazil.[732] The LGPD requires businesses have a lawful basis under the legislation for processing data.[733] It also provides consumers located in Brazil with various rights which have been likened to those available to EU citizens under the GDPR, such as the right to be informed about the purpose of the processing of their personal data, the right to request their personal data be deleted, and the right to be notified about the sharing of their personal data.[734]

Other online private messaging services had single policies containing different terms applicable to different jurisdictions. For example, **WeChat's** Privacy Policy included a number of separate terms only applicable to users in the European Economic Area and California, including rights relating to user control of data that seem to only apply to users in the European Economic Area. These included the right for users to access, delete and copy their data. For users that are Californian residents subject to the CCPA *'and other applicable*

---

725 WhatsApp, WhatsApp Legal Info (European Region) – Privacy Policy, accessed 9 July 2020.
726 WhatsApp, California Privacy Notice, accessed 9 July 2020; WhatsApp, Brazil Privacy Notice, accessed 9 July 2020.
727 In Portuguese, the Brazilian General Data Protection Law is referred to as the Lei Geral de Proteção de Dados (LGPD).
728 WhatsApp, California Privacy Notice, accessed 10 July 2020.
729 The CCPA applies to all for-profit businesses that do business in California and meet any one of the following criteria: have a gross annual revenue of over $USD25 million; buy, receive or sell the personal information of 50,000 or more California residents, households or devices; or derive 50% or more of their annual revenue from selling California residents' personal information.
730 State of California Office of the Attorney General, California Consumer Privacy Act (CCPA), accessed 22 September 2020.
731 California Legislative Information, California Consumer Privacy Act of 2018, section 1798.140(t)(1), accessed 22 September 2020.
732 National Congress of Brazil, Lei Geral de Proteção de Dados Pessoais - Law No. 13,709/2018 (English Translation), 14 August 2018, accessed 22 September 2020; IGLC, Brazil: Data Protection Laws and Regulations 2020, 7 June 2020, accessed 22 September 2020.
733 IGLC, Brazil: Data Protection Laws and Regulations 2020, 7 June 2020, accessed 22 September 2020; GDPR.eu, What is the LGPD? Brazil's version of the GDPR, accessed 22 September 2020.
734 National Congress of Brazil, Lei Geral de Proteção de Dados Pessoais - Law No. 13,709/2018 (English Translation), 14 August 2018, accessed 22 September 2020; GDPR.eu, What is the LGPD? Brazil's version of the GDPR, accessed 22 September 2020.

*laws'*, an addendum provided a more succinct and clear list of purposes for data collection, including *'providing personalised advertisements'*.[735]

In some cases, the terms placed the onus on the user to know what rights they were entitled to in their jurisdiction. For example, **Zoom's** previous Privacy Policy stated that '*Depending on where you reside*, you *may* be entitled to certain legal rights with respect to your Personal Data (emphasis added)'[736] including allowing users to request access, deletion and a copy of their data.

## D.3 Application of end-to-end encryption to online private messaging services

- **For some online private messaging services which claim to offer end-to-end encryption, end-to-end encryption is only available in certain circumstances, or is subject to certain exceptions.**

The ACCC also examined how end-to-end encryption is offered on a broader range of online private messaging services. Table D.6 below lists a selection of online private messaging services, whether they offer end-to-end encryption and any restrictions on the application of this encryption.

**Table D.6: Selected online private messaging services and end-to-end encryption (as at August 2020)**

| Platform | Default end-to-end encryption? | Opt-in end-to-end encryption? | Restrictions on the application of end-to-end encryption? |
|---|---|---|---|
| **Apple iMessage** | ✓ | × | • End-to-end encryption only applies to iMessages (not SMS), which must be sent between two iOS devices.[737]<br>• Backups of messages stored in iCloud are not protected by end-to-end encryption. |
| **Facebook Messenger** | × | ✓ | • End-to-end encryption applies to 'secret conversations', which can only be accessed in the Messenger app, not in a browser, and must be manually enabled for each chat.[738]<br>• The secret conversation option is unavailable for group chats (only one-on-one).[739] |
| **Google Hangouts** | × | × | • N/A |
| **Google Messages** | ×[740] | × | • N/A |
| **Line** | × | ✓ | • Where enabled, end-to-end encryption only applies to text and location messages, and one-on-one |

[735] WeChat, Privacy Policy, accessed 10 July 2020.
[736] Zoom, Privacy Policy, accessed 29 March 2020.
[737] Apple, iMessage and FaceTime Privacy, accessed 5 August 2020.
[738] Facebook, Secret Conversations, accessed 4 August 2020.
[739] J Peterson, Chat with End-to-End Encryption Using Facebook Messenger's Secret Conversations, *Gadget Hacks,* 6 February 2019, accessed 22 September 2020.
[740] Note that Google is reportedly launching end-to-end encryption for 'Rich Communication Service' (RCS) messages in a forthcoming update. As with iMessage, it will not apply to Google Messages sent as an SMS. This is due to functionality limitations of SMS. See K Bradshaw, Google Messages preparing end-to-end encryption for RCS messages, *9to5Google*, 26 May 2020, accessed 22 September 2020.

| | | | |
|---|---|---|---|
| | | | audio and video calls. It does not apply to images, videos, files or group audio or video calls.[741]<br>• For chats between 2 to 50 users, all users in the chat must have end-to-end encryption enabled. Group chats with more than 50 members cannot be protected by end-to-end encryption.[742] |
| **Signal** | ✓ | × | • N/A |
| **Snapchat** | ✓ | × | • Annual reports refer generally to data on Snapchat being 'end-to-end encrypted',[743] however it has been reported that this applies to snaps (i.e. images and videos) but not messages.[744] |
| **Threema** | ✓ | × | • N/A |
| **Telegram** | × | ✓ | • End-to-end encryption only applies to 'secret chats', which can only be one-on-one and must be started with each recipient.[745] |
| **Viber** | ✓ | × | • Viber only guarantees that end-to-end encryption will work in the latest version of Viber. Therefore, in a group chat, end-to-end encryption may not apply if some group members do not have the latest version of the app.[746]<br>• Chats with bots, Public Accounts and in Viber 'communities' are not end-to-end encrypted.[747]<br>• Backups of messages stored in iCloud or Google Drive are not protected by end-to-end encryption. |
| **WeChat** | × | × | • N/A |
| **WhatsApp** | ✓ | × | • Backups of messages stored in iCloud or Google Drive are not protected by end-to-end encryption.[748] |
| **Zoom** | × | ×[749] | • N/A |

741 LINE, LINE Encryption Report, 13 November 2019, accessed 4 August 2020.
742 LINE, LINE Encryption Report, 13 November 2019, accessed 4 August 2020.
743 Snap Inc, 2019 Annual Report, 4 February 2020; Snap Inc, 2018 Annual Report, 5 February 2019.
744 T Titcomb, Snapchat adds end-to-end encryption to protect users' messages, *The Telegraph*, 9 January 2019, accessed 4 August 2020; Choose to Encrypt, Is Snapchat Privacy-Friendly? [Analysis], 16 October 2019, accessed 22 September 2020.
745 Telegram, Telegram FAQ, accessed 5 August 2020. The ACCC notes that Telegram's FAQ stated that the reason all chats are not 'secret' (and therefore end-to-end encrypted) is to provide users with the option of reliable backups. Telegram's regular chats disable system backups by default and are stored in Telegram's own cloud storage system.
746 Viber, Viber account security and encryption, accessed 4 August 2020.
747 Viber, Viber Privacy Policy, accessed 4 August 2020. However, the ACCC understands that these functionalities of Viber are of a different nature to its use as an online private messaging service.
748 WhatsApp, About Google Drive backups, accessed 28 July 2020; WhatsApp, How to back up to iCloud, accessed 28 July 2020.
749 In June 2020, Zoom reported that it was introducing an 'early beta' of its end-to-end encryption feature in July 2020. When rolled out, end-to-end encryption will be an optional feature available to all users. To access the feature, users will be required to participate in a one-time authentication process that prompts the user for an additional piece of information, such as verifying a phone number via text message. See E S Yuan, End-to-End Encryption Update, *Zoom Blog,* 17 June 2020, accessed 22 September 2020.

## D.4 Potential consumer harms arising from the extensive data practices of platforms

- **The extensive data practices of online private messaging, search and social media platforms increases the risk of harms occurring to consumers. These potential consumer harms, which were identified in the DPI Final Report, include an increased risk of profiling, discrimination and exclusion. These harms are particularly acute for vulnerable consumers such as children. These potential harms continue to be observed.**

The DPI Final Report observed that platforms' data practices, which leverage the information asymmetries, bargaining power imbalances and behavioural biases between platforms and consumers were resulting in the following consumer harms:[750]

(a) reduced consumer trust and data-based innovations

(b) decreased consumer welfare from decreased privacy

(c) risks to consumers from increased profiling

(d) risks to consumers from discrimination and exclusion

(e) particular risks to vulnerable consumers, and

(f) decreased consumer welfare from reduced competition.

The ACCC has observed the potential for these harms to occur across online private messaging, social media and search services and online advertising services. This arises particularly in relation to the extensive tracking practices of the platforms offering these services, as discussed in chapter 4.

### D.4.1 Reduced consumer trust and data-based innovations

Consumer trust is critical to the digital economy and many consumers are increasingly concerned about their privacy and the use of information on platforms.[751] Recent research and reports have also found that consumers continue to be uncomfortable with platforms' data practices as outlined in box 4.4.

As noted in chapter 4, AppCensus observed that platforms such as Facebook and Google, and suppliers of online advertising services received user information from Android apps during the testing period.[752]

Many consumers consider the sharing of their personal information to third parties to be a misuse of their personal information.[753] For example:

- the OAIC's 2020 survey found that approximately 84 per cent of those surveyed view their personal information being used for a purpose other than the purpose for which it was collected to be a misuse[754]
- the Norwegian Consumer Council's *Out of Control* report, which observed the data flows between apps and third parties, similarly found 'that there were many instances of personal data being sent to ad tech companies that appear to use this information for purposes that consumers cannot reasonably expect, such as tracking and profiling'.[755]

---

750 ACCC, DPI Final Report, 26 July 2019, pp. 442–448.
751 ACCC, DPI Final Report, 26 July 2019, p. 382.
752 AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. 33.
753 Roy Morgan, Consumer views and behaviours on digital platforms, November 2018, p. 21.
754 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, p. 37.
755 Norwegian Consumer Council (Forbrukerradet), Out of Control – How consumers are exploited by the online advertising, 14 January 2020, p. 82.

### D.4.2 Decreased consumer welfare from decreased privacy

Decreased privacy and control over consumer data can result in harms including data breaches of personal or financial information, unsolicited targeted advertising, and identity fraud.

In March 2020, the OAIC instituted proceedings against Facebook in relation to the 2018 Cambridge Analytica data breach. The OAIC estimated that 311 127 Australian Facebook users had their personal information (including sensitive information) disclosed to a third party as a result of the data breach.[756] In addition, the OAIC's 2020 survey found that 59 per cent of those surveyed have experienced problems with the handling of their personal information in the past twelve months.[757]

Recent reports from the eSafety Commissioner and the Australian Cyber Security Centre indicate that incidents of fraud and cybersecurity incidents are continuing and resulting in potential harms to consumers. The eSafety Commissioner's June 2020 report into the impact of COVID-19 on consumers' experiences online found that nearly 38 per cent of surveyed adults reported a negative online experience and 5 per cent of reported having money stolen or being subject to fraud.[758] The Australia's Cyber Security Strategy Report also noted that the Australian Cyber Security Centre responded to over 2,200 cyber security incidents between 1 July 2019 and 30 June 2020.[759]

### D.4.3 Risks to consumers from increased profiling

The ACCC considers that platforms' extensive collection of consumer data, in conjunction with the opacity of the information provided to consumers about how their data is used or may be used by platforms, increases the likelihood of consumer harms resulting from increased profiling. Demographic information used by marketers to segment target audiences is increasingly combined with psychographic information that measures individual's attitudes and interests.[760] The ACCC has observed that this information can be used to influence consumer behaviour, leading to potential consumer harm.

For example, payday loans targeting financially vulnerable consumers are increasing in Australia, in part due to the visibility of these offers which are frequently advertised on platforms.[761] Researchers have found that many payday lenders have profiles on social media platforms that blend finance tips and recommend payday loans[762], and that consumers in financial hardship have been targeted by payday lenders' advertising strategies, including on social media.[763] Despite responsible lending obligations, research has found that lenders are offering payday loans to those who can't afford to pay them. In the past three years to 2019, the amount lent via payday loans doubled from $881 million in 2016[764] to approximately $1.7 billion as at the end of 2019.[765] The number of payday loans which originate on platforms have also significantly increased—from approximately 5.6 per cent in 1999 to 85.8 per cent in 2019.[766]

---

[756] *Australian Information Commissioner v Facebook Inc & Anor,* Concise Statement, March 2020, p. 1.
[757] OAIC, Australian Community Attitudes to Privacy Survey, September 2020, p. 20.
[758] eSafety Commissioner, Covid-19 impact on Australian adults' online activities and attitudes, June 2020, p. 16.
[759] Australian Government, Australia's Cyber Security Strategy 2020, p. 10.
[760] ACCC, DPI Final Report, 26 July 2019, p. 445.
[761] Payday loans are high cost, short term loans with equivalent annual interest rates between 100 to 400 per cent. See Stop the Debt Trap Alliance, The Debt Trap – How payday lending is costing Australians, November 2019, p. 6.
[762] Payday Lenders: Trusted Friends Or Debt Traps?, Impact, 15 October 2019, accessed 22 September 2020; V Chen, Online Payday Lenders: Trusted Friends Or Debt Traps?, UNSW Law Journal, 43(2) (2020) p. 688.
[763] V Chen, Online Payday Lenders: Trusted Friends Or Debt Traps?, UNSW Law Journal, 43(2) (2020) p. 675.
[764] S Martin, More than 30,000 payday loans targeting the financially vulnerable taken out each week, *The Guardian*, 12 November 2019, accessed 22 September 2020.
[765] Stop the Debt Trap Alliance, The Debt Trap – How payday lending is costing Australians, November 2019, p. 6.
[766] Stop the Debt Trap Alliance, The Debt Trap – How payday lending is costing Australians, November 2019, p. 4, 10.

Google announced that it would ban payday loans ads from July 2016[767], and that it would ban apps which offer short term loans from its Google Play Store in August 2019. However, it has been reported that advertisers and apps continue to find workarounds.[768]

### D.4.5 Risks to consumers from discrimination and exclusion

The ACCC remains of the view that the extensive consumer data held by platforms and the opacity surrounding how online advertising and advertising services are supplied enables more detailed targeting of consumers.[769] This further increases the likelihood that consumers could be exploited for discriminatory purposes or that vulnerable consumers may be excluded.[770]

While many platforms allow advertisers to choose to target certain consumers that may be relevant to their advertisement, there is a risk that these tools could be used to exclude groups of consumers. There have been alleged instances of these practices occurring on Facebook, leading to settlements with state authorities including the Washington State Attorney-General[771] to ensure that ethnic and religious minorities, immigrants, LGBTQ individuals and other protected groups were not excluded by third party advertisers on Facebook.[772]

However, since those settlements, there have been recent reports that Facebook's ad delivery algorithms can continue to target certain groups based on the content of the advertisement, which could have a potentially discriminatory effect.[773] Researchers are reported to have found that even when advertisers did not specify particular audiences for an advertisement, Facebook algorithmically determined that the audience for job advertisements for cleaners, secretaries, nurses and pre-school teachers were primarily women; while job ads for supermarket cashiers, fast food workers and taxi drivers were mainly delivered to African-Americans.[774]

While Google and Facebook have each announced changes to their advertising policies to prohibit housing, employment and credit advertisers from targeting US based users based on age, gender and postcode, it remains to be seen whether these changes will be effective or whether they will extend to non-US based users.[775]

In addition, despite these measures being introduced, platforms continue to collect vast amounts of consumer data, including highly sensitive user information, and this may increase the risk of such information being used in discriminatory or exclusionary ways. For example, Privacy International found that almost 98 per cent of popular mental health websites contained third party elements (such as third party cookies), with approximately

---

767 A Peterson and J Marte, Google to ban payday loan advertisements, *The Sydney Morning Herald,* 12 May 2016, accessed 22 September 2020.

768 K Wack, Payday lenders are finding ways around Google's ad ban, *American Banker,* 11 October 2017, accessed 22 September 2020; Z Mider and Z Faux, Google Ban Fails to Stamp Out Short-Term Payday Lending Apps, *Bloomberg*, 24 January 2020, accessed 22 September 2020.

769 ACCC, DPI Final Report, 26 July 2019, p. 446.

770 ACCC, DPI Final Report, 26 July 2019, pp. 446–447.

771 ACCC, DPI Final Report, 26 July 2019, p. 447.

772 Washington Attorney General's Department, Media release, AG Ferguson Investigation Leads To Facebook Making Nationwide Changes To Prohibit Discriminatory Advertisements On Its Platform, 24 July 2018, accessed 22 September 2020.

773 J Fong, Facebook showed this ad almost exclusively to women. Is that a problem? *Vox*, 31 July 2020, accessed 22 September 2020.

774 J Fong, Facebook showed this ad almost exclusively to women. Is that a problem? *Vox*, 31 July 2020, accessed 22 September 2020.

775 For example, Google's proposed change is due to be implemented in US and Canada by the end of 2020, and Facebook's proposed change was announced in March 2019, with advertisers required to comply with the requirements by 31 March 2020. See S Spencer, Upcoming update to housing, employment and credit advertising policies, *The Keyword (Google Blog)*, 11 June 2020, accessed 22 September 2020; S Sandberg, Doing more to protect against discrimination in housing, employment and credit advertising, *Facebook Newsroom,* 19 March 2019, accessed 22 September 2020; A Hutchinson, Facebook Sets Deadlines for Advertisers to Comply with New Requirements for Housing, Credit and Employment Ads, Social Media Today, 8 January 2020, accessed 22 September 2020.

76 per cent of web pages containing trackers used for advertising and marketing purposes.[776] Privacy International found that Google, Facebook and Amazon trackers were present on many mental health websites, with approximately 70 per cent containing trackers owned by Google DoubleClick.[777]

### D.4.6 Particular risks to vulnerable consumers

The ACCC notes that the vast amount of data collected by platforms may include data which identifies or infers an individual's vulnerabilities and the ACCC is concerned about the impact of problematic data practices on children and vulnerable consumers, who are particularly susceptible to the risks associated with data collection practices.[778]

Children are increasingly engaging in online activities and using platforms for a range of purposes, including education, communication and entertainment. In doing so children may use apps which can collect and transmit their data to third parties. For example, AppCensus[779] observed that 'Kids apps' transmitted data to platforms such as Facebook and Google, and other businesses such as suppliers of advertising services, during the testing period.[780] AppCensus also observed that 'Kids apps' transmitted data during the testing period, with over 45 per cent of 'Kids apps' transmitting the Android Advertising ID[781] (a type of identifier which is primarily used for advertising purposes and can be reset by users).[782] Other data types that AppCensus observed 'Kids apps' to transmit during the testing period include the Android ID (which can only be reset with a factory reset of the mobile device)[783], which was transmitted by over 45 per cent of 'Kids apps'. [784]

While many platforms restrict children under 13 from using their services, the data collection practices of platforms (such as those outlined above) may have special harms for children, who are unlikely to understand the consequences of their online activities on their privacy and the potential inferences from their data that could impact their future.[785] Additionally, as discussed in chapter 4, social media platforms have been subject to the settlements and investigations regarding their alleged collection of children's data despite these age restrictions.

The ACCC remains of the view that certain groups of consumers may not have the technical, critical and social skills to engage in online activities in a safe way.[786] For example, recent research from the eSafety Commissioner found that older Australians and those with a disability reported the lowest levels of digital confidence and have the greatest perceptions of risk online.[787] In addition, recent research found that certain groups are more likely to have a negative experience online. The eSafety Commissioner found that Aboriginal and Torres Strait Islander peoples and Australians who identify as LGBTQI and were more likely

---

776 Privacy International, Your mental health for sale - How websites about depression share data with advertisers and leak depression test results, September 2019, p. 3.
777 Privacy International, Your mental health for sale - How websites about depression share data with advertisers and leak depression test results, September 2019, p. 4.
778 ACCC, DPI Final Report, 26 July 2019, p. 447.
779 AppCensus analysed the top 1,000 Android apps in Australia from June–July 2020. Based on ranking and active users, the top 1000 most popular Android apps consist of top apps on the Google Play Store across all categories and at least 100 top apps in both the Fitness and Health categories ('Health apps') and in the Education, Games and Animation and Comics categories that are targeted to children aged 13 and under ('Kids apps').
780 AppCensus, 1,000 Mobile Apps in Australia: Appendix C: Kids Apps, 24 September 2020, pp. C-2–C-3.
781 AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, pp. ii–iii; AppCensus, 1000 Mobile Apps in Australia: Appendix C: Kids Apps, 24 September 2020, p. C-1. AppCensus observed that 47 'Kids apps' transmitted the Android Advertising ID.
782 For further information, see box 4.5 at chapter 4.
783 AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. iii.
784 AppCensus, 1,000 Mobile Apps in Australia: A Report for the ACCC, 24 September 2020, p. ii; AppCensus, 1000 Mobile Apps in Australia: Appendix C: Kids Apps, 24 September 2020, p. C-1. AppCensus observed that 46 'Kids apps' transmitted the Android ID.
785 Consumer Policy Research Centre, A Day in the Life of Data: Removing the opacity surrounding the data collection, sharing and use environment in Australia, May 2019, p. 39.
786 ACCC, DPI Final Report, 26 July 2019, p. 448.
787 eSafety Commissioner, Building Australian adults' confidence and resilience online, September 2020, p. 3.

to have had a negative experience online[788], with nearly 6 in 10 respondents stating that the experience had an adverse impact such as mental or emotional stress.[789] The research also found that social media platforms and online private messaging services were among the most common channels for negative online experiences.[790]

### D.4.7 Decreased consumer welfare from reduced competition

Consumers also continue to experience decreased consumer welfare from reduced competition.[791] While the OAIC's 2020 survey found that 84 per cent of individuals surveyed consider the privacy of their information to be extremely or very important when choosing a digital service[792], information asymmetries and bargaining power imbalances may prevent consumers from accessing products and services that best meets their data and privacy preferences. In addition, these information asymmetries and bargaining power imbalances are likely to have reduced the degree of competition between platforms in relation to the quality of privacy protections.[793] As noted in the DPI Final Report, Australian consumers may experience reduced choice and reduced quality of services in relation to the privacy dimension compared to those in overseas jurisdictions with stronger privacy protections.[794]

---

788 eSafety Commissioner, Building Australian adults' confidence and resilience online, September 2020, p. 3, 6. The eSafety Commissioner found that Aboriginal and Torres Strait Islanders recorded the top response for 16 of the 17 negative online experiences identified in the survey and people identifying as LGBTQI recorded the second highest response for 12 of the 17 experiences.

789 eSafety Commissioner, Adults' negative online experiences, August 2020, p. 10.

790 eSafety Commissioner, Adults' negative online experiences, August 2020, pp. 9–10.

791 ACCC, DPI Final Report, 26 July 2019, p. 448.

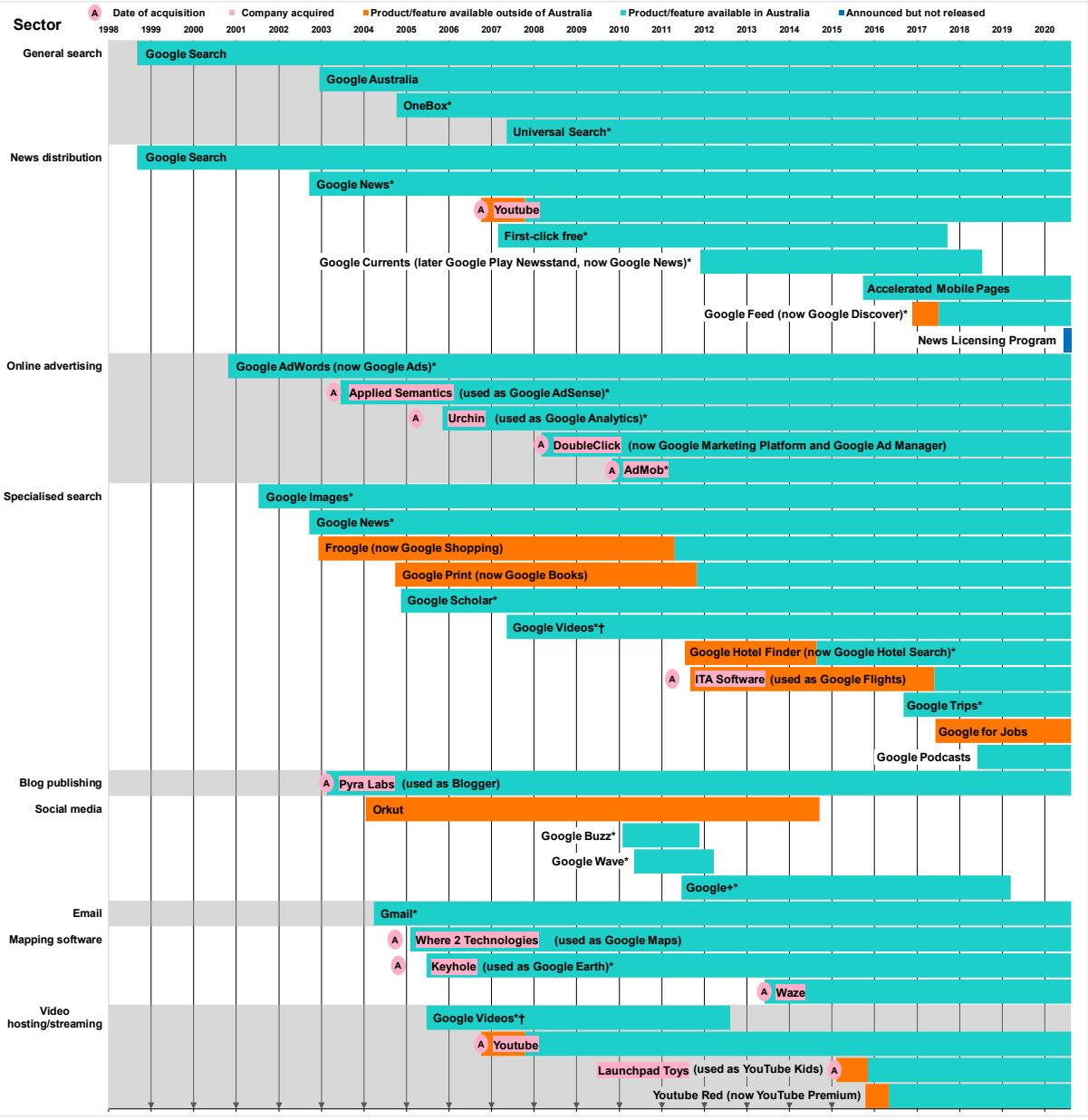
792 OAIC, Australian Community Attitudes to Privacy Survey, September 2020, p. 18.

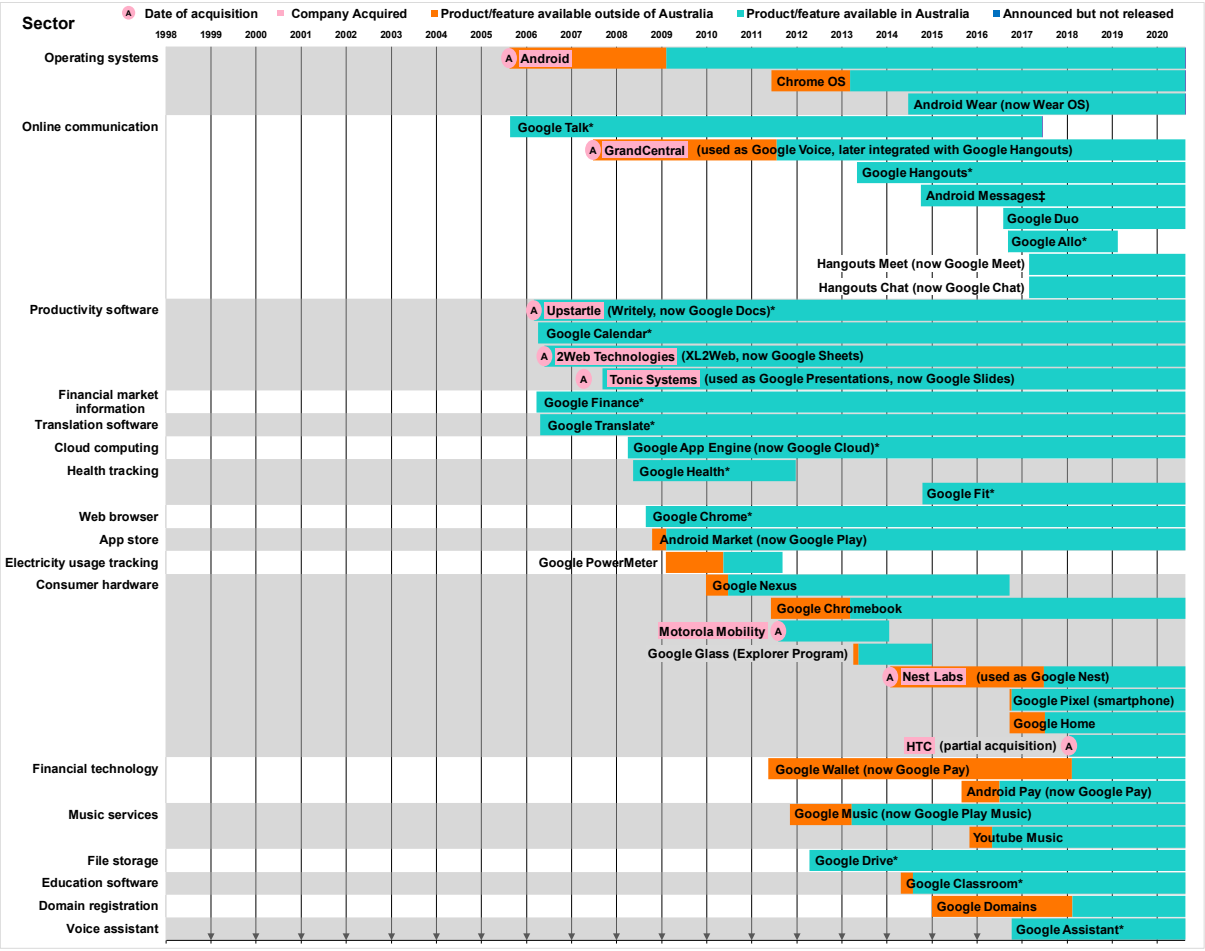
793 ACCC, DPI Final Report, 26 July 2019, p. 448.

794 ACCC, DPI Final Report, 26 July 2019, p. 448.

# Appendix E: Timeline of Google's expansion into new sectors

The below timeline includes notable products/features/acquisitions that demonstrate Google's expansion into a range of products, services and sectors. It is not an exhaustive list of Google's products and services, features of those products and services and acquisitions. The dates shown are best estimates based on publicly available sources.






* The dates in these charts are based on Google Blog posts, media reporting and reports published by international regulators. The products/features/acquisitions with an asterisk were not reported to be released in a specific country or region, therefore it is assumed that the release on that date was global, including Australia.

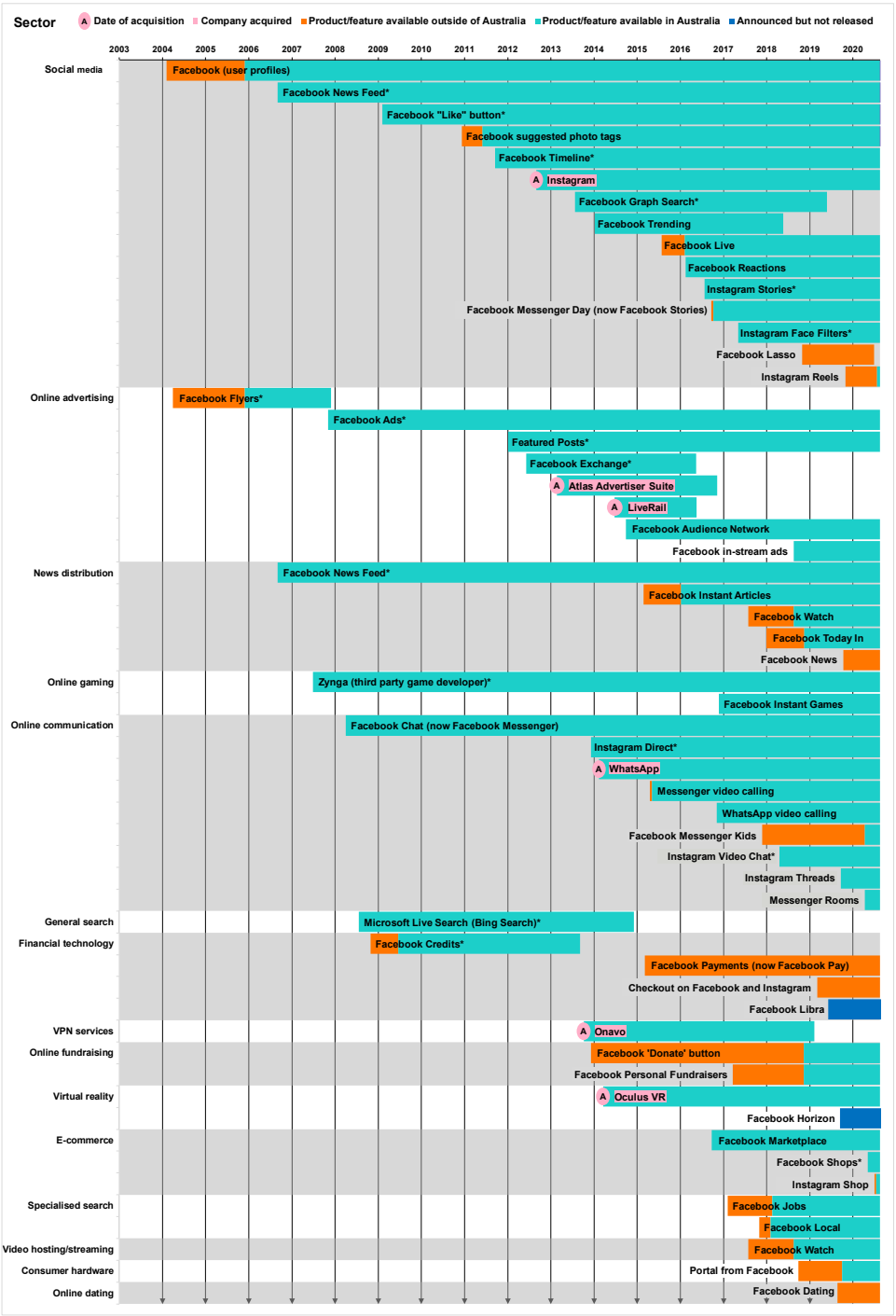
† In June 2005, Google Videos enabled video hosting. In May 2007, search functionality was enabled for videos across the internet in addition to videos on Google Videos and YouTube. In August 2012 Google Videos discontinued its video hosting functionality and became solely a specialised search engine for videos.

‡ Android Messages, through its 'Chat' feature, provides the ability for users to send and receive messages using the Internet rather than mobile networks. See further discussion in chapter 1.

Source: ACCC analysis.

# Appendix F: Timeline of Facebook's expansion into new sectors

The timeline below includes notable products/features/acquisitions that demonstrate Facebook's expansion into a range of products, services and sectors. It is not an exhaustive list of Facebook's products and services, features of those products and services and acquisitions. The dates shown are best estimates based on publicly available sources.




* The dates in these charts are based on Facebook Blog posts, media reporting and reports published by international regulators. The products/features/acquisitions with an asterisk were not reported to be released in a specific country or region, therefore it is assumed that the release on that date was global, including Australia.

Source: ACCC analysis.

# Appendix G: International regulatory proposals and developments

The Direction's terms of reference require the ACCC to consider developments in markets for the supply of platform services outside of Australia. There has been a broad international trend of governments and regulators increasingly focusing on the role and practices of digital platforms. At the same time, platforms have themselves announced a range of self-regulatory measures seeking to address identified issues.

The global nature of services offered by large platforms has seen similar competition and consumer protection issues emerge across international jurisdictions, as discussed in chapter 7. However, in response to these common issues, overseas jurisdictions have taken both similar and different approaches including regulatory proposals and enforcement action. Common themes in these responses are discussed below, and are also outlined in table G.1 and table G.2.

**Table G.1** outlines a number of regulatory developments relating to online private messaging, social media and search services *implemented* in overseas jurisdictions since July 2019.

**Table G.2** outlines a number of regulatory proposals relating to online private messaging, social media and search services that have been *proposed* in overseas jurisdictions since July 2019, but have not yet been implemented or completed.

The ACCC notes that the developments outlined below do not relate exclusively to platforms providing online private messaging, social media and search services, and may extend to other platforms and businesses.

## G.1 Gatekeeper role and the need for greater fairness in platform-to-business relationships

Across jurisdictions, governments and regulatory agencies have paid particular attention to the ability of large platforms with market power to act as 'gatekeepers'.

The EC's proposed Digital Services Act package, presented as part of the European Data Strategy in February 2020, seeks to modernise the regulatory framework for digital services and reduce fragmentation across Member States. It proposes ex ante regulatory measures to address the market imbalances where a few large online platforms act as gatekeepers and are considered to set the 'rules of the game' for their users and their competitors. It also includes rules concerning the role and obligations of online intermediaries in the EU, and a governance system to enforce such rules.[795]

This proposal builds on *the Regulation on promoting fairness and transparency for business users of online intermediation services* ('platform-to-business' regulation), which places obligations on large platforms to create a fair and transparent business environment. This regulation came into force in June 2019 and obligations commenced from 12 July 2020.

Governments across the world have also recognised the need for greater transparency and fairness in the dealings between large platforms and business users with similar ex ante 'platform-to-business' regulations being proposed or adopted in Asia. In Japan, the *Bill for Improving Transparency and Fairness of Digital Platforms* was passed in May 2020, and will be implemented into law within a year.[796] The bill proposed obligations on large platform operators to improve transparency and fairness in dealings with Japanese business

---

[795] European Commission, Commission launches consultation to seek views on Digital Services Act package, Press Release, 2 June 2020; European Commission, Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers, accessed 22 September 2020.

[796] K Toda, Japan: Latest Developments on the Regualtion of Digital Platformers from a Competition Law Perspective, TMI Associates, 8 July 2020, accessed 22 September 2020.

partners, including submitting annual reports to the Minister of Economy, Trade and Industry, who can issue corrective recommendations and orders for unfair treatment.[797]

In South Korea, proposed legislation seeks to prevent market leading online platforms from monopolising the market and abusing their superior position, including by establishing a legal basis to intervene in setting commission rates and allocating costs for promotional activities of small and medium sized enterprises vulnerable to unfair contract terms. The proposed legislation may also require merging firms to report the deal if there is a potential threat to competition (regardless of size).[798]

In the United Kingdom, both the Furman Report and the CMA's final report into Online Platforms and Digital Advertising acknowledged the crucial 'gatekeeper' function that some large platforms have in the digital economy, mediating relationships between consumers and businesses in a variety of markets.[799] To protect consumers and competition where platforms have market power from this gatekeeper position, the CMA recommended a pro-competitive regulatory regime to oversee the activities of these platforms.[800] This would include an enforceable code of conduct to govern the behaviour of platforms that hold a position of market power or 'strategic market status' (likely to be those with gatekeeper positions). The code would seek to help protect competition from the negative effects that can arise from market power, rather than seeking to address the underlying causes of market power.[801] It is proposed to take the form of high-level principles and each platform with 'strategic market status' would have its own tailored code.[802]

## G.2 Need for increased scrutiny of acquisitions by large digital platforms and other antitrust reforms

Overseas jurisdictions are taking new approaches to antitrust reforms concerning platforms across a range of common competition issues. While different approaches have been advocated, there is commonality in some areas such as the importance of competition authorities placing more scrutiny on acquisitions by digital platforms.

Several jurisdictions are adopting changes to merger control that seek to increase scrutiny on the acquisitions of large digital platforms. For example:

- In Japan, companies are now recommended to consult with the Japan Fair Trade Commission (JFTC) on deals valued at more than 40 billion yen, and consideration of mergers will take into account factors including data accumulation, network effects and whether a platform is acquiring a start-up.[803]
- In France, a bill introduced by the Senate proposes to subject all acquisitions by global platforms to a formal merger review, and to examine the impact of acquisitions. This bill also places new obligations on tech companies such as Google, Apple, and Facebook with 'systemic' market power, including ex ante sectoral regulation to guarantee consumer freedom of choice and mobility.[804]

---

797 Ministry of Economy, Trade and Industry, Cabinet Decision on the Bill for the Act on Improvement of Transparency and Fairness in Trading on Specified Digital Platforms, Press Release, 18 February 2020.

798 K Jae-Heun, KFTC drafts policy to prevent platform monopolies' The Korea Times, 29 June 2020, accessed 22 September 2020.

799 Competition and Markets Authority, Online platforms and digital advertising – Market study final report, 1 July 2020, p. 16. Digital Competition Expert Panel, Unlocking digital competition, March 2019, p. 41.

800 Competition and Markets Authority, Online platforms and digital advertising – Market study final report' 1 July 2020, p. 324.

801 Competition and Markets Authority, Online platforms and digital advertising – Market study final report, 1 July 2020, p. 22.

802 Competition and Markets Authority, Online platforms and digital advertising – Market study final report, 1 July 2020, p. 23.

803 Japan Fair Trade Commission, Amendments to Guidelines to Application of the Antimonopoly Act concerning Review of Business Combination and to Policies concerning Procedures of Review of Business Combination (English Translation), 17 December 2019.

804 MLex, Digital giants should notify all acquisitions to French watchdog, says Senate law proposal, 22 January 2020, accessed 22 September 2020.

- Germany and Austria both introduced new transaction value thresholds into their merger control regimes, which came into force in 2017.[805] These changes were introduced in order to address concerns that purely turnover-based criteria sometimes failed to cover important mergers, especially in the digital economy where very high purchase prices may be paid for companies, which have achieved little or hardly any turnover.
- In the United Kingdom, the Digital Markets Taskforce led by the CMA, established in March 2020 to advise the UK Government, is considering (among other things) whether to introduce a separate merger control regime for acquisitions by firms with 'strategic market status'. This separate regime would have its own jurisdictional and substantive tests owing to the increased risks of consumer harm. The CMA currently considers that firms with strategic market status may be required to notify all transactions to the CMA (subject to limited exemptions) and a more cautious standard of proof may be applied to reviewing their acquisitions, potentially with a separate assessment of non-competition concerns.[806] The CMA is also updating its Merger Assessment Guidelines to reflect developments in its approach to digital mergers.[807]
- In Australia, the ACCC recommended that large platforms agree to a voluntary merger notification protocol to give the ACCC advance notice of proposed transactions to address the issue of strategic acquisitions contributing to a platform's market power.[808] The ACCC is working towards a protocol, which is subject to negotiation between the ACCC and large digital platforms. The ACCC also recommended amendments to the *Competition and Consumer Act 2010* (section 50(3)) to incorporate additional merger factors including the likelihood that the acquisition would result in the removal from the market of a potential competitor.

## G.3 Need for better understanding and scrutiny of digital platform markets

Governments and relevant agencies in many overseas jurisdictions have undertaken or are currently conducting reviews into various digital markets, to develop a better understanding of the market dynamics and proactively identify any potential issues that could give rise to competition concerns or consumer harms.[809] In some cases, these reviews have found similar issues and identified similar remedies to address these issues in the relevant market. Some of these reviews are discussed below.

---

805 C Burholt, A Traugott, F Carlin and J Hobson, New Value-based Filing Thresholds in European Merger Control Regimes – Implications for Healthcare and Life Sciences Companies, *Global Compliance News*, 1 November 2017, accessed 22 September 2020.

806 Competition and Markets Authority, Call for Information – Digital Markets Taskforce, 1 July 2020, pp. 20-21.

807 The Furman Report recommended that digital companies with strategic market status be required to notify the CMA of their intended acquisitions, and that the CMA prioritise scrutiny of mergers in digital markets. The Report also recommended changes to merger law that would enable the CMA to better account for the scale and likelihood of impacts on competition as a result of the acquisition, in light of the practice of larger platforms acquiring small, innovative platforms before they become a serious competitor. See Digital Competition Expert Panel, Unlocking digital competition, March 2019, pp. 12-13; Competition and Markets Authority, Online platforms and digital advertising – Market study final report, 1 July 2020, pp. 436-437.

808 ACCC, DPI Final Report, 26 July 2019, p. 30.

809 For example, in November 2019, the Swedish Competition Authority commenced a sector inquiry into digital platforms, across various markets to understand platforms' influence on market structure and competition, and identify potential regulatory reforms. See P Torbol et al, 'Swedish Sector Inquiry into Digital Platforms', K&L Gate, 8 November 2019, accessed 22 September 2020.

## Reviews and market studies of digital platform markets

Many of these studies and reviews have looked or are looking at aspects of online advertising, including studies in the United Kingdom[810], Germany, Spain[811], Mexico[812] and Japan[813]. For example, in Germany, the Bundeskartellamt is examining the market structure and technical developments of online advertising, and whether, as some market players claim, there is a closed systems of a few large providers exist and what significance these systems have, if any.[814]

In July 2020, the CMA published its Final Report of its market study into online platforms and digital advertising. The CMA's Chief Executive Andrea Coscelli summarised the study, noting:

> *Through our examination of this market, we have discovered how major online platforms like Google and Facebook operate and how they use digital advertising to fuel their business models. What we have found is concerning—if the market power of these firms goes unchecked, people and businesses will lose out. People will carry on handing over more of their personal data than necessary, a lack of competition could mean higher prices for goods and services bought online and we could all miss out on the benefits of the next innovative digital platform.*[815]

As set out above, the CMA recommended a new pro-competition regulatory regime to govern the behaviour of major platforms funded by digital advertising, like Google and Facebook, with an enforceable code of conduct.

In Japan, the JFTC carried out a detailed, large-scale survey into the state of trade practices on online retail platforms and app stores to identify whether there are any concerns under Japanese competition law. The survey and inquiry focused on digital advertising with an interim report published in October 2019.[816] A number of findings were reached by the JFTC and further fact-finding inquiries will be carried out by the JFTC to inform them on whether platform operators are acting in a way that imposed unfair disadvantages on other businesses or are acting in an exclusionary manner.

In Australia, the ACCC is also conducting an 18-month inquiry into the markets for the supply of digital advertising technology services and digital advertising agency services.[817]

Several reviews and investigations are also underway in the United States, looking at the role of online platforms and issues of market power. These are being led by the Department of Justice, state Attorney Generals, the United States House Subcommittee on the Judiciary Subcommittee on Antitrust, Commercial and Administrative Law and the United States House Subcommittee on the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights.

The Department of Justice commenced a review in July 2019 into whether and how market-leading online platforms have achieved market power and are engaging in practices that have reduced competition, stifled innovation, or otherwise harmed consumers.[818]

There are also a number of joint investigations reportedly underway by United States state Attorney Generals. These include a joint antitrust investigation by the Department of Justice

---

810 Competition and Markets Authority, Online platforms and digital advertising – Market study final report, 1 July 2020.
811 Comision Nacional de los Mercados y la Competencia (CNMC), Online advertising, 2019.
812 Comision Federal de Competencia Economica, 'COFECE investigates possible relative monopolistic practices in the market for digital advertisement services and related services', Press Release, 24 August 2020.
813 Japan Fair Trade Commission, Interim Report Regarding Digital Advertising, Press Release, 28 April 2020.
814 Bundeskartellamt, Bundeskartellamt launches sector inquiry into market conditions in online advertising sector, Press Release, 1 February 2018.
815 Competition and Markets Authority, New regime needed to take on tech giants, Press Release, 1 July 2020.
816 Japan Fair Trade Commission, Report regarding trade practices on digital platforms (English Translation), 31 October 2019.
817 ACCC, Digital advertising services inquiry, 10 March 2020, accessed 22 September 2020.
818 United States Department of Justice, Justice Department Reviewing the Practices of Market-Leading Online Platforms, Press Release, 23 July 2019.

and a coalition of state Attorney Generals into Apple's App Store[819], a joint investigation led by Washington and California into Amazon's website,[820] a joint investigation led by New York into Facebook[821] and a joint investigation led by Texas into Google's business practices.[822]

The US Subcommittee on Antitrust, Commercial and Administrative Law has been undertaking an ongoing investigation into online platforms and market power. As part of this investigation, the CEO's of Facebook, Google, Amazon and Apple appeared at a hearing before the US Subcommittee in July 2020.[823]

The US Subcommittee on Antitrust, Competition Policy and Consumer Rights has also held a hearing to examine Google's online advertising business model and its potential impact on market competition, as part of its investigation into the digital advertising market.[824]

## G.4 Platforms calling for regulation in some areas and some adopt self-regulatory measures

In the midst of government inquiries and proposed new legislation, many digital platforms are themselves calling for new regulation or are taking self-regulatory actions.

For example, in an op-ed for the Financial Times in January 2020, Google and Alphabet CEO, Sundar Pichai suggested regulation of AI should be nuanced and balance mitigation of 'potential harms' with space for 'social opportunities'. He also called for international alignment to make global standards work, and agreement on core values.[825]

Some platforms are also setting their own standards around AI, for example Microsoft has adopted a set of company-wide rules for enacting responsible AI[826] and Facebook is reported to be studying Facebook and Instagram for racial bias and looking at whether its AI trained algorithms adversely affect some racial groups.[827]

Several platforms and tech companies are also adopting changes in relation to data portability. Whilst the potential introduction of data portability is being contemplated in some jurisdictions, companies have been involved in 'The Data Transfer Project'[828] that seeks to create an open-source, service-to-service data portability so that individuals across the web can easily move their data between online service providers whenever they want. The Project contributors believe portability and interoperability are central to innovation, and making it easier for individuals to choose among services facilitates competition and consumer choice.[829] It would allow users to move their online data between platforms without the need to download or uploaded data. The Project was founded by Facebook, Google, Twitter, and Microsoft in 2018 (Apple joined in 2019).[830] The Project appears to be

---

819 L Nylen, Apple's easy ride from U.S. authorities may be over, *Politico*, 24 June 2020.

820 K Weise and D McCabe, Amazon said to be under scrutiny in 2 States for abuse of power, *The New York Times*, 12 June 2020, accessed 22 September 2020.

821 NY Attorney General, AG James Investigating Facebook for Possible Antitrust Violations, Press Release, 6 September 2019.

822 Attorney General of Texas, Attorney General Paxton Leads 50 Attorneys General in Google Multistate Bipartisan Antitrust Investigation, Press Release, 9 September 2019.

823 In July 2020, the subcommittee held a hearing examining the dominance of Amazon, Apple, Facebook and Google, which was attended by the CEO's of these companies, House Committee on the Judiciary, Hearings: Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook and Google, 29 July 2020, accessed 22 September 2020.

824 D Perera, Google faces panel of US senators sceptical of claims about robust market for digital display, *MLex*, 16 September 2020, accessed 22 September 2020.

825 S Pichai, Why Google thinks we need to regulate AI, *Financial Times*, 20 January 2020, accessed 22 September 2020.

826 Microsoft, Operationalising responsible AI, accessed 22 September 2020.

827 N Statt, Facebook will study whether its algorithms are racially biased, *The Verge*, 21 July 2020, accessed 22 September 2020.

828 C Shank, Microsoft, Facebook, Google and Twitter Introduce the Data Transfer Project: An Open Source Initiative for Consumer Data Portability, *Microsoft EU Policy Blog*, 20 July 2018, accessed 22 September 2020.

829 Data Transfer Project, About us, accessed 22 September 2020.

830 J Constine, Facebook, Google and more unite to let you transfer data between apps, *Tech Crunch*, 20 July 2018, accessed 22 September 2020.

in progress, with Facebook rolling out a tool to allow users to transfer photos and videos to Google Photos[831] as well as cloud storage services Dropbox and Koofr.[832]

Facebook has also published a white paper on data portability and privacy calling for clear rules about portability, and posing questions about what and whose data should be portable, how to protect privacy while enabling portability and who is responsible if data is misused or improperly protected.[833] The white paper followed calls from Facebook CEO Mark Zuckerberg, in an op-ed for the Washington Post, for a globally harmonised framework for data protection and privacy.[834] In August 2020, Facebook also submitted official comments to the United States FTC calling for the FTC to examine portability in practice, and introduce dedicated federal portability legislation so that companies have clear rules.[835]

In relation to copyright and content moderation, many platforms have taken to publishing their own transparency reports. These are intended to provide users with more oversight about how platforms' enforce their policies such as Community Guidelines and Standards, including their approach to content moderation, as well as how they respond to government or legal requests. Platforms that currently publish some form of public transparency report include Google[836], Facebook[837], Twitter[838], Snap[839], Apple[840] and Microsoft.[841]

While these actions may go some way to addressing potential consumer harms, a fragmented approach may be ineffective and could create other risks. Furthermore, where platforms adopt self-regulatory measures, there may be inconsistent impacts depending on the action undertaken as this is ultimately at the discretion of the platforms.[842]

---

831 Facebook rolled out this feature between December 2019 and June 2020. See Facebook, Driving innovation in data portability with a new photo transfer tool, Facebook Newsroom, 2 December 2019, accessed 22 September 2020.

832 N Bose, Facebook partners with two more companies ahead of FTC hearing on data portability, *Reuters*, 3 September 2020, accessed 22 September 2020.

833 E Egan, Charting a Way Forward: Data Portability and Privacy, September 2019.

834 M Zuckerberg, The internet needs new rules. Let's start in these four areas, *The Washington Post*, 31 March 2019, accessed 22 September 2020.

835 Facebook, Facebook Files Official Comments on Data Portability with Federal Trade Commission, Facebook Newsroom, 20 August 2020, accessed 22 September 2020.

836 Google, Google Transparency Report, accessed 22 September 2020.

837 Facebook, Facebook Transparency Report, accessed 22 September 2020.

838 Twitter, Twitter Transparency report, accessed 22 September 2020.

839 Snap Inc., Transparency Report, 27 May 2020, accessed 22 September 2020.

840 Apple, Transparency Report, accessed 22 September 2020.

841 Microsoft, Microsoft Privacy Report, accessed 22 September 2020.

842 H Murphy, Facebook joins Silicon Valley's rush to appear responsible, *Financial Times*, 26 December 2019, accessed 22 September 2020.

**Table G.1: Overseas regulatory developments relating to platforms supplying online private messaging, social media and/or search services since July 2019.**

| Jurisdiction | Proposal | Stage of proposal | Overview of proposal |
|---|---|---|---|
| **Competition and fair dealing** | | | |
| European Union | **Regulation on promoting fairness and transparency for business users of online intermediation services**[843] | Came into force June 2019. Obligations commenced from 12 July 2020 | 'Platform-to-business' regulation that places obligations on 'online intermediation services' in relation to their dealings with businesses using the platform including in regards to terms and conditions, ranking of services, informing businesses of any differentiated treatment, informing businesses of their access to data and dispute resolution options. |
| Japan | **Improving Transparency and Fairness of Digital Platforms**[844] | Passed Parliament—27 May 2020 and will be implemented within a year of its promulgation[845] | 'Platform-to-business' regulation that places obligations on large platform operators to improve transparency and fairness in dealings with Japanese business partners, including submitting annual reports to the Minister of Economy, Trade and Industry, who can issue corrective recommendations and orders for unfair treatment. |
| Japan | **Amendments to Guidelines to Application of the Antimonopoly Act Concerning Review of Business Combination**[846] | Implemented—17 December 2019 | Companies are recommended to consult with the JFTC on deals more than 40 billion yen and consideration of mergers will take into account factors such as data accumulation, network effects, switching costs, and specific consideration for platforms acquiring a start-up. A company may attract scrutiny if it has a 'superior bargaining position' in relation to its competitors.[847] |

843 Regulation (EU) 2019/1150 of the European Parliament and of the Council, 20 June 2019, accessed 22 September 2020.
844 T Dokei, H Nakajima and T Onki, Bill for Improving Transparency and Fairness of Digital Platforms, White & Case, 7 February 2020, accessed 22 September 2020.
845 K Toda, Japan: Latest Developments on the Regualtion of Digital Platformers from a Competition Law Perspective, TMI Associates, 8 July 2020, accessed 22 September 2020
846 Japan Fair Trade Commission, Amendments to Guidelines to Application of the Antimonopoly Act concerning Review of Business Combination and to Policies concerning Procedures of Review of Business Combination (English Translation), 17 December 2019.
847 T Dokei, A M. Mitchell and H Nakajima, Digital platforms will soon face more regulatory scrutiny in Japan, White & Case, 13 September 2019, accessed 22 September 2020.

| Jurisdiction | Proposal | Stage of proposal | Overview of proposal |
|---|---|---|---|
| **Consumer protection, including content moderation** | | | |
| European Union | **'New Deal for Consumers' legislative package**<br><br>**Directive (EU) 2019/2161 on better enforcement and modernisation of Union consumer protection rules**[848] | Adopted—27 November 2019[849]<br><br>Date of effect—7 January 2020 | A package of legislative reforms aimed at strengthening enforcement of EU consumer law in light of growing risk of EU-wide infringements and modernising EU consumer protection rules in light of market developments. The directive amends the following existing EU consumer laws:<br>• Council Directive 93/13EEC on unfair terms in consumer contracts<br>• Directive 2011/83/EU on consumer rights<br>• Directive 2005/29/EC on unfair business-to-consumer commercial practices<br>• Directive 98/6/EC on consumer protection in the indication of the prices of products offered to consumers |
| Japan | **Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.** [850] | Enacted and published—17 December 2019 | The Guidelines[851] intend to provide clarity and predictability for the situations where conduct would be problematic in business-to-consumer transactions under the abuse of superior bargaining power regulation, specifically for transactions where consumers provide information (e.g. personal information) to platforms.[852] |
| Singapore | **The Protection from Online Falsehoods and Manipulation Act (POFMA)**[853] | Came into effect – 2 October 2019[854] | The new legislation is aimed at protecting society from fake news that harms public interest. It gives Ministers the power to decide whether something is a falsehood and, if it is in the public interest to do so, order a 'competent authority' |

848 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, accessed 22 September 2020.

849 European Commission, Review of EU Consumer Law – New Deal for Consumers, accessed 22 September 2020.

850 Japan Fair Trade Commission, Release of the "Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.", Press Release, 17 December 2019.

851 The Guidelines are published under the Antimonopoly Act on the Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.

852 T Dokei, H Nakajima and T Onoki, New Guidelines re: Application of ASBP to Transactions between Digital Platforms and Consumers, White & Case, 15 January 2020, accessed 22 September 2020.

853 Protection from Online Falsehoods and Manipulation Act 2019 (POFMA), accessed 22 September 2020.

854 T See Kit, Law to curb deliberate online falsehoods takes effects, Channel News Asia, 2 October 2019, accessed 22 September 2020.

| Jurisdiction | Proposal | Stage of proposal | Overview of proposal |
|---|---|---|---|
| | | | to take action. This includes issuing corrections to be run next to the false content or take-down orders in extreme cases. |
| **Data protection** | | | |
| United States (California) | **California Consumer Privacy Act**[855] | Came into effect – 1 January 2020<br><br>Regulations package came into effect – 14 August 2020[856] | Grants Californian consumers data privacy rights and control over their personal information, including the right to know, the right to delete, and the right to opt-out of the sale of personal information that businesses collect, as well as additional protections for minors.<br><br>It imposes a set of data protection obligations on any company that operates in California and either has at least $25 million in annual gross revenue, gathers data on more than 50,000 users, or derives 50 per cent or more of its annual revenue from user data. |
| Brazil | **General Data Protection Law**<br><br>**(Lei Geral de Protecao de Dados, LGPD)** [857] | Came into effect – 15 August 2020 | Grants a number of rights to data subjects in Brazil, including rights to confirm existence of processing, access data, correct inaccurate or incomplete data, anonymise or delete data, information about how data is used, and revocation of consent. |
| Japan | **Revision of the Act on the Protection of Personal Information**[858] | Passed in June 2020.<br><br>The main provisions will come into force within two years from the date of their promulgation. | Requires companies to obtain consent from users when handing over personal data, such as internet browsing history, to third parties, and when it is clear that the data can be traced to individuals by third parties. It also calls for the pseudonymisation of data, in which names and other personal information are replaced with markers. |

855 California Consumer Privacy Act (CCPA), accessed 22 September 2020.
856 Xavier Becerra Attorney General, CCPA Regulations, accessed 22 September 2020.
857 Cookie Law, Lei Geral de Protecao de Dados (LGPD), 12 March 2020, accessed 22 September 2020.
858 The Japan Times, Japan's government adopts bill to tighten rules on personal data, *The Japan Times*, 11 March 2020, accessed 22 September 2020.

| Jurisdiction | Proposal | Stage of proposal | Overview of proposal |
|---|---|---|---|
| **Other regulatory developments** | | | |
| European Union | **Directive on Copyright in the Digital Single Market**[859] | Member states have two years to pass appropriate legislation – until 7 June 2021 | Measures aimed at creating a fairer market place for online content, especially for press publications, online platforms and remuneration of authors and performers. Platforms, such as YouTube, could be held accountable if users upload copyright protected movies and music and will need to police copyrighted material. They will need to obtain licenses for copyrighted works from rights holders in order to host their content. |
| France | **Ratification of EU Directive on Copyright** [860] | Came into force – 24 October 2019 | The French legislation effectively requires a platform (such as Google or Facebook) using all or part of a press article to compensate the relevant news publisher. The compensation is to be negotiated taking into account the costs incurred by the publisher. |

[859] European Commission, Copyright, accessed 22 September 2020.
[860] WIPO, France: Law No. 2019-775 of July 24, 2019, on the Creation of Neighbouring Rights for the Benefit of Press Agencies and Publishers, 24 October 2019, accessed 22 September 2020

**Table G.2: Overseas regulatory proposals relating to platforms supplying online private messaging, social media and/or search services since July 2019.**

| Proposal | Stage of proposal | Overview of proposal |
|---|---|---|
| **European Union** | | |
| **Digital Services Act**[861] | Public consultation: 2 June 2020—8 September 2020 | As part of the European Single Market framework, the Digital Services Act package is intended to modernise the current legal framework for digital services by proposing clear rules framing the responsibilities of digital services to address the risks faced by their users and to protect their rights; and ex ante rules covering large online platforms acting as gatekeepers to promote competition. |
| **New competition tool**[862] | Public consultation on an inception impact assessment from 2 June to 8 September 2020. | A possible new competition tool to enable the EC to address gaps in the current competition rules and to intervene against structural competition problems, such as tipping markets, across various markets in a timely and effective manner. The tool is without prejudice to existing sector-specific regulation and existing competition tools; and is complementary to the Digital Services Act package. |
| **e-Privacy Regulation**[863] | 22 November 2019—the European Council rejected the latest draft | The ePrivacy Regulation (ePR), proposed in 2017, is intended to update the 2002 ePrivacy Directive and cover privacy of electronic communication data issues. The ePR is intended to work alongside the GDPR, and specify how the general data protection framework outlined in the GDPR will be applied. |

861 European Commission, Consultation on the Digital Services Act package, accessed 22 September 2020.
862 European Commission, Antitrust: Commission consults stakeholders on a possible new competition tool, Press Release, 2 June 2020.
863 C Baskerville, Still no consensus on ePrivacy, *Global Data Review*, 5 June 2020.

| Proposal | Stage of proposal | Overview of proposal |
|---|---|---|
| **Amendments to the Act against Restraints of Competition**[864]<br><br>**[Germany]** | Draft bill published—24 January 2020[865]<br><br>Cabinet approved—9 September 2020[866] | A proposed 10th amendment to German competition law, focused on changes to establish a 'digital regulatory framework', including the introduction of 'access to competition-relevant data' as an additional factor for assessing the market position of a company, extending theories of abusive conduct to refusal to grant access to data that is 'objectively necessary', self-preferencing behaviour and preventing data portability. The bill also proposes changes to implement EU Directive 2019/1[867] (European Competition Network (ECN) + Directive), revisions to the German merger control regime (reversal of burden of proof), changes to the antitrust enforcement proceedings, and clarifications to the damages claims provisions. |
| **Draft bill guaranteeing the consumer's free choice in cyberspace**[868]<br><br>**[France]** | Bill passed Senate – 19 February 2020[869]<br><br>Further amendments passed Senate – 8 July 2020[870] | A Senate draft law that would create new obligations on tech companies such as Google, Apple, Facebook and others with 'systemic' market power, includes ex ante sectoral regulation to guarantee consumer freedom of choice and mobility, and modernisation of competition law to examine impact of acquisitions. It would subject all acquisitions by global platforms to a formal merger review. |
| **United States** | | |
| **Amendments to Section 230, Communications Decency Act 1996** | 17 June 2020 – Department of Justice released reform proposals | On 17 June 2020, the Department of Justice released a set of reform proposals to update Section 230 after a 10-month review, which arose during the broader review of market leading online platforms and practices.[871] |

[864] F Hinderer and M Masling, Draft Amendments to German Competition Law Published, *JDSupra*, 3 February 2020, accessed 22 September 2020.
[865] Concurrences, The German Ministry for Economic Affairs and Energy publishes the draft bill on the 10th Amendment to the German act Against Restraints of Competition, 24 January 2020, accessed 22 September 2020.
[866] R Colitt, K Matussek and S Sed, Germany Moves to Crack Down on Big Tech with Anti-Trust Bill, Bloomberg, 9 September 2020, accessed 22 September 2020.
[867] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, accessed 22 September 2020.
[868] MLex, Digital giants should notify all acquisitions to French watchdog, says Senate law proposal, 22 January 2020, accessed 22 September 2020.
[869] A Yaiche, French plans for Big Tech merger notifications divide government and Senate, *MLex*, 20 February 2020, accessed 22 September 2020.
[870] A Yaiche, A French law to make all platform deals face scrutiny could help EU regulator, de Silva says, *MLex*, 9 July 2020, accessed 22 September 2020.
[871] US Department of Justice, Justice Department Issues Recommendations for Section 230 Reform, 17 June 2020.

| Proposal | Stage of proposal | Overview of proposal |
|---|---|---|
| | | On 28 May 2020, the President of the United States issued an Executive Order on Preventing Online Censorship that seeks to reduce the platform liability protections under Section 230, and allow the FTC to create a tool for users to report bias online. [872] |
| **Anticompetitive Exclusionary Conduct Prevention Act (S.3426)** [873] | Introduced in Senate – 10 March 2020 | The proposed legislation would increase the burden of proof on monopolists to prove they are not suppressing competition, and discourage courts from granting immunity from antitrust enforcement. |
| **Data Protection Act (S.3300)** [874] | Introduced in Senate – 13 February 2020 | To establish a Federal data protection agency, and for other purposes, to regulate the processing of personal data. |
| **Preventing Real Online Threats Endangering Children Today (PROTECT Kids Act) (H.R.5573)** [875] | Introduced in House of Representatives – 9 January 2020 | To amend the *Children's Online Privacy Protection Act 1998* (COPPA) and increase the prohibition age of collection of children's data from 13 to 16. It also proposes to ban collection of sensitive information such as precise geolocation and biometric information, and install a feature for parent's to delete their child's information.[876] The bill mirrors many of the protections offered under a similar Senate measure (S. 748). |
| **Consumer Online Privacy Rights Act (COPRA) (S.2968)** [877] | Introduced in Senate – 3 December 2019 | This bill places requirements on entities that process or transfer a consumer's data, including requirements to make their privacy policy publicly available and provide an individual with access to their personal data; delete or correct, upon request, information in an individual's data; export, upon request, an individual's data in a human-readable and machine-readable format; and establish data security practices to protect the confidentiality and accessibility of consumer data. |
| **Augmenting Compatibility and Competition by Enabling Service Switching Act** | Introduced in Senate – 22 October 2019 | A bill to promote competition and reduce consumer-switching costs in the provision of online communications services. It would apply to 'large communications platforms' |

872 White House, Executive Order on Preventing Online Censorship, Executive Order, 28 May 2020.
873 S.3426—Anticompetitive Exclusionary Conduct Prevention Act of 2020, accessed 22 September 2020.
874 S.3300—Data Protection Act of 2020 accessed 22 September 2020.
875 H.R.5573—PROTECT Kids Act, accessed 22 September 2020.
876 M Kelly, 'Eraser button' for children's data gains support in the House, *The Verge*, 9 January 2020, accessed 22 September 2020.
877 S.2968—Consumer Online Privacy Rights Act, accessed 22 September 2020.

| Proposal | Stage of proposal | Overview of proposal |
|---|---|---|
| **(ACCESS Act) (S.2658)** [878] | | with 100 million monthly users that generate income from collecting, processing, or sharing user data. |
| **Mind Your Own Business Act (S.2637)** [879] | Introduced in Senate – 17 October 2019 | To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes. The bill empowers the FTC to fine tech companies that violate user privacy and would allow the FTC to establish minimum privacy and cybersecurity standards for tech platforms and give it authority to issue fines of up to 4 percent of a company's annual revenue for first-time offences (similar to provisions in the GDPR). |
| **Other jurisdictions** | | |
| **Proposed law to prevent possible power abuse by online platform operators**[880] **[South Korea]** | June 2020 | Proposed new legislation to prevent market leading online platforms from monopolising the market and abusing their superior position, including establishing a legal basis to intervene in setting commission rates and allocating costs for promotional activities of small-and medium-sized enterprises, vulnerable to unfair contract terms. The proposed legislation will also affect merger and acquisition conditions, and may require merging firms to report the deal if the FTC considers it may threaten competition regardless of size. |
| **Draft amendment to Section 79 of the IT Act**[881] **[India]** | Public consultation on draft amendments – February 2020 | The regulations are intended to curb the misuse of social media and stop the spreading of fake news. The proposed amendment would require internet companies to take down content deemed inappropriate by authorities within 72 hours of the origin of that content and to disable that user's access within 24 hours. |

878 S.2658—Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019, accessed 22 September 2020.
879 Mind Your Own Business Act of 2019, accessed 22 September 2020
880 K Jae-Heun, KFTC drafts policy to prevent platform monopolies, *The Korea Times*, 29 June 2020, accessed 22 September 2020.
881 M Bahree, India's New Rules to govern social media raise fears of more censorship, *Forbes*, 22 January 2019, accessed 22 September 2020.