



ACCC Digital Platforms Services Inquiry

**September 2022 Report on updating competition and consumer
law for digital platform services**

Google's supplementary submission to the ACCC

3 August 2022

Introduction and Summary

In April 2022, we submitted our detailed response (**Response**) to the ACCC's Discussion Paper for Interim Report No.5: Updating competition and consumer law for digital platform services (**Discussion Paper**), outlining our position on the broad-ranging issues and potential measures canvassed by the ACCC. We advocated for any new regulatory framework for digital platforms to adhere to the following six principles:

- Principle 1: Promoting competition and innovation, and enhancing the welfare of consumers, should be the ultimate objectives for this type of regulatory framework. A regulatory framework that shields companies from robust competition would ultimately operate at consumers' expense.
- Principle 2: Preventing competitive harm and permitting evidence-based justifications for conduct under scrutiny should be embedded in the overarching framework.
- Principle 3: The rules on conduct should be necessary and proportionate to the seriousness of anticipated harm and the likelihood of it occurring.
- Principle 4: Suitable procedural protections and review mechanisms should be incorporated to ensure the integrity of a new regulatory framework. Full merits review by a Court should be available for decisions that have legal consequences.
- Principle 5: Any changes to the rules should follow evidence and consultation; there should be clear conditions, not unfettered discretion, to change rules or introduce additional rules.
- Principle 6: The rules should avoid creating overlapping obligations that are inconsistent with other regulatory frameworks.

Since Google's Response to the Discussion Paper, the ACCC has published more than 80 submissions from stakeholders¹ and summaries of the competition and consumer roundtables held by the ACCC on 1 and 7 June 2022, respectively.² Stakeholders' submissions and comments at the roundtables illustrate the breadth of different views on the adequacy of existing laws, the need for and objectives of additional regulation, the framework and tools that could or should be adopted, the scope and content of any new

¹ ACCC, ['Digital platform services inquiry 2020-2025 | September 2022 interim report'](#).

² ACCC, ['Summary of stakeholder roundtable on competition measures'](#) and ['Summary of stakeholder roundtable on consumer protection measures'](#), 7 July 2022.

rules, and the platforms that should be subject to them. There appears to be a lack of consensus on virtually all aspects of possible additional regulation of digital platforms.^{3,4}

In this supplementary submission, Google responds to some of the issues raised by stakeholders that were not covered in our Response, with a view to correcting misunderstanding and highlighting relevant new developments, regarding:

- the status of international developments, particularly in relation to competition law, and implications for Australian reform;
- app stores;
- choice screens and choice architecture;
- dark patterns;
- scams; and
- fake reviews.

We feel it is important to address these issues in order to avoid:

- incorrect speculation or allegations about Google's conduct or products;
- ill-founded assumptions about the state of international developments; and
- consequently, proposals for reform that are based on incorrect claims, which creates a greater risk of unintended consequences or undesirable outcomes for consumer welfare and competition.

We do not agree with some of the statements made in stakeholder submissions and at the competition and consumer roundtables, but we have not sought to respond to each of

³ For example, while some submissions argue that regulation of digital platforms is necessary, other submissions argue that existing laws are sufficient or that any new regulation must be justified by rigorous economic analysis (see, for example, submissions from the [Antitrust Law Section of the American Bar Association](#), [Asia Internet Coalition](#), [Business Council of Australia](#), [Computer & Communications Industry Association](#), [Digi](#), [Global Antitrust Institute](#), [George Mason University](#), [Law Council of Australia](#) and [The App Association](#)).

⁴ This lack of consensus was also noted by the ACCC in its '[Summary of stakeholder roundtable on competition measures](#)', for example:

- at p 2: 'In relation to the dominance in search and web browsers, stakeholders had conflicting views over potential remedies.';
- at p 2: 'Stakeholders held a variety of views on regulatory regimes to address data advantages, and the circumstances in which it should apply.';
- at p 3: 'Most stakeholders broadly agreed that regulation of digital platforms is necessary. However, some stakeholders argued that existing laws are sufficient or that it would be beneficial to wait and learn from international counterparts.'; and
- at p 3: 'Some stakeholders noted that while there is consensus on the issues that should be regulated, there is no international consensus on the best approach to regulation.'

them here. Instead, we have focused on issues which appear to us to be most material, and that we have not otherwise meaningfully addressed with the ACCC.

We trust that the ACCC will continue to test the robustness of stakeholders' claims. We stand ready to assist the ACCC as it prepares its Interim Report and conducts future phases of the Digital Platform Services Inquiry, working towards its Final Report in March 2025.

I. THE STATUS OF INTERNATIONAL DEVELOPMENTS IN COMPETITION LAW & IMPLICATIONS FOR AUSTRALIAN REFORM

We recognise that digital platforms' popularity has given rise to debate about how well competition law works in digital markets. New rules have been legislated in the EU (with the *Digital Markets Act (DMA)*), Germany and Korea. There have also been proposals in the UK and the US. Several stakeholders have suggested that Australia needs to act urgently to implement platform regulation or risk 'falling off the pace' as other jurisdictions develop their own rules.

There is, however, some confusion about these new proposals, their status, and how they operate. To assist the ACCC, we'd like to make four high-level points about international platform regulation.

First, there is no international consensus on the need for, objectives or content of, new competition rules.

While the EU's DMA has passed, its behavioural rules do not enter into force until sometime in late 2023 or early 2024. The position in the UK and the US is less certain. The UK Government has decided not to introduce its new regime for digital platforms during the present Parliamentary term. In the US, various bills are under legislative review (including the *American Innovation & Choice Online Act*, the *Open App Markets Act*, and the *Digital Advertising Trading Transparency and Competition Act*). But it is too soon to know which bills, if any, will pass, and, if so, in what form. In addition, each has taken a different design and implementation approach.

Despite the impression given by some stakeholders, there is no clear international consensus on the need for new competition regulation for digital platforms; the objectives of such regulation; and the specific content of new rules.

Second, a common theme across (almost all) the new regimes is the importance of defences and justifications.

While there is no consensus internationally on the need for new competition rules, one common theme that emerges from the new regimes that have been proposed is the importance of justifications and defences:

- In the UK, the CMA has emphasised that firms should be able to justify their conduct, even if it may seem to fall within one of the prohibited categories of

behaviour. Under the proposals, conduct would be exempted from sanction if it 'is necessary, or objectively justified, based on the efficiency, innovation, or other competition benefits it brings.'⁵ Likewise, the CMA considers that interventions should be ordered only when there is a risk of an adverse effect on competition.

- In the US, legislation pending in the House and the Senate raise fundamental concerns about cybersecurity, user privacy, content moderation, and the quality of technology products Americans currently enjoy. But the bills at least do contain defences based on overall competitive effects. Specifically, the House legislation permits conduct that is narrowly tailored to 'increase consumer welfare' (or that prevents a violation of law or protects user privacy).⁶ The Senate legislation goes a step further, requiring plaintiffs to affirmatively show 'material harm' to competition on the 'covered platform',⁷ as well as allowing for defences where conduct helps 'maintain or enhance the core functionality of the covered platform', (or prevents a violation of law or protects user privacy).⁸
- In Germany, firms can defend their conduct by demonstrating objective justifications. The German rules, in addition, are not self-executing – in that they do not apply immediately, but only after the FCO has undertaken an investigation and identified a problem in a reasoned decision.

The EU's DMA, by contrast, does not expressly allow for such defences. It does not include an express provision allowing companies to justify conduct, for example, based on user security, system integrity, quality, functionality, or privacy. Articles 8 and 9 include some exceptions based on public morality, public health, and public safety, but it remains unclear how situations involving these critical issues will be decided.

Several of the DMA's behavioural rules are far-reaching and novel, banning conduct that until now has been considered to be procompetitive, such as keeping assets to oneself and not sharing them with horizontal rivals. It would therefore have been sensible to include an express safeguard in the DMA to protect against unintended harmful consequences for citizens and businesses.

In the global debate on potential ex ante rules for digital platforms, many stakeholders have expressed concerns about the lack of safeguards in the DMA:

⁵ CMA Digital Markets Taskforce, '[Appendix C of the Advice of the Digital Markets Taskforce](#)', 8 December 2020, para 35-36.

⁶ *American Innovation and Choice Online Act*, H.R. 3816, Sec. 2(c).

⁷ *American Innovation and Choice Online Act*, S. 2992, Sec. 2(a),(d).

⁸ *American Innovation and Choice Online Act*, S. 2992, Sec. 2(d).

- Experts consistently call for allowing ‘an explicit and well-framed defence’, to prevent the unintentional outlawing of beneficial conduct and depriving Europeans of the benefits that such conduct brings.⁹
- Advocate-General G. Pitruzzella has explained that ‘too much rigidity could hinder efficiency and introduce a disproportionate limitation on the freedom to conduct a business’.¹⁰
- The German Monopolies Commission ‘considers that there are weighty reasons to supplement the DMA to include an efficiency defence on a case-by-case basis’; it recommended allowing firms to defend their conduct by showing it ‘promotes technical development or economic progress’.¹¹
- In the same vein, a stakeholder responding to the Discussion Paper explained that the UK’s flexible approach to regulation ‘may be preferable to the more rigid approach pursued by the EU with the DMA’.¹²
- Professor Richard Whish has described the DMA as having been shaped by ‘embryonic’ abuse of dominance cases. For Whish, the DMA’s rules are based on theories of harm that are not yet conclusively anticompetitive.¹³ This is particularly dangerous if there is no scope to justify deviation from these rules.

In summary, while we do not think that the case for digital platform regulation in Australia has been made, we firmly believe that if any regime were introduced, then the ability to justify and defend conduct based on consumer and business benefits should be embedded in the framework.

⁹ See Cabral, L, Haucap, J, Parker, G, Petropoulos, G, Valletti, T, and Van Alstyne, M, European Commission, ‘[The EU Digital Markets Act: A Report from a Panel of Economic Experts](#)’, 2021, 9 (‘one of the main challenges in the implementation of the DMA is how to separate the positive efficiency and welfare gains that platforms generate [...] from negative anti-competitive and welfare-reducing platform behaviour [...] Pro-competitive remedies should not undermine the efficiency gains of platforms’); Centre on Regulation in Europe, ‘[The European proposal for a Digital Markets Act: A first assessment](#)’, January 2021, 22 (‘given that many practices in the digital economy have multiple positive and negative effects on contestability and fairness (as well as on welfare and innovation) and the (still) many unknowns in competitive dynamics of digital technologies and markets, it is appropriate to provide for an explicit and well framed defence that could be brought by the gatekeepers.’); Crofts, L and Hirst, N, ‘[Comment: EU’s ‘mechanical’ approach to Big Tech regulation in the spotlight](#)’, MLex, February 2021 (‘Blunt rules will make it harder for Big Tech players to innovate, and may degrade consumers’ enjoyments of their services’); Chrétien, J and Isaac, H, ‘[Digital Markets Act: A Revolution or a Legal Contradiction?](#)’, Renaissance Numérique, April 2021 (‘the proposed DMA introduces a sort of presumption of competitive guilt’).

¹⁰ Crofts, L and Hirst, N, ‘[EU gatekeeper regulation raises questions of ‘proportionality,’ member of top court says](#)’, MLex, March 2021.

¹¹ Monopolies Commission, ‘[Recommendations for an effective and efficient Digital Markets Act](#)’, 5 October 2021, para 131-138 for rationale.

¹² DailyMail Australia, ‘[Response to the Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services](#)’, 30 March 2022, 3.

¹³ Aranze, J, ‘[DMA obligations influenced by unresolved tech cases, Whish says](#)’, Global Competition Review, 13 July 2022.

Third, international developments do not justify bypassing the steps required in Australia to introduce new rules.

Some stakeholders have suggested the fact that other jurisdictions are introducing new regimes means that Australia needs to act urgently to implement ex ante rules for large digital platforms, or risk 'falling off the pace'. One stakeholder added that the ACCC should develop a mandatory code for digital platforms under the *Competition and Consumer Act 2010* (Cth) (**CCA**), and bypass the usual steps, including preparing a regulatory impact statement and a cost / benefit analysis, on the basis of the ACCC's existing digital platform findings.

We disagree. It is not appropriate to truncate the usual processes in Australia for developing codes or other regulatory frameworks, including proper scrutiny of costs and benefits,¹⁴ because of developments in other countries or on the basis of previous findings made by the ACCC in broad inquiries into a range of digital platforms issues. This is particularly so given (i) the haste under which the DMA was adopted, (ii) the risks inherent in the DMA because, in particular, of its lack of express safeguards, and (iii) the acknowledged high-degree of innovation and dynamism in digital markets.¹⁵

Rather, we continue to believe that a proper cost / benefit analysis is an essential precursor before considering whether to adopt any new regime in Australia. We are not alone in thinking so. This imperative was echoed in submissions by a range of stakeholders, including the Law Council of Australia, the Business Council of Australia, Atlassian, DIGI, Amazon Australia, Meta, the Australian Investment Council, the Computer & Communications Industry Association, the Consumer Policy Research Centre, the Antitrust Law Section of the American Bar Association and the Global Antitrust Institute of George Mason University.

Accordingly, we encourage the ACCC and Government to undertake further consultation on concrete proposals to allow for careful consideration of the interaction of individual rules with each other and with Australia's existing laws, as well as any unintended consequences from the proposed rules. As noted by the Business Council of Australia in its response to the Discussion Paper:

¹⁴ Australian Government Department of the Prime Minister & Cabinet, Office of Best Practice Regulation, '[Guidance Note: Cost-Benefit Analysis](#)', March 2020.

¹⁵ For example, Google Search and Maps are being impacted by a growing preference for social media and videos as the first stop on younger users' path to discovery (see Perez, S, '[Google exec suggests Instagram and TikTok are eating into Google's core products, Search and Maps](#)', TechCrunch, 13 July 2022. Benedict Evans reported that Amazon's advertising revenue increased from just over \$4bn at the end of 2017 to \$14bn by 2019. At the end of 2021, Amazon reported \$31bn of advertising revenue). See Evans, B, '[TV, merchant media and the unbundling of advertising](#)', Benedict Evans, 18 March 2022. Similarly, the Digital 2022 Global Overview Report reported that TikTok was the most-downloaded mobile app in 2021. Bytedance reported that TikTok's advertising reach increased by 60 million users in the past 90 days, taking worldwide advertising reach to roughly 885 million users by the start of 2022. See We are Social and Hootsuite, '[Digital 2022: Another Year of Bumper Growth](#)', 26 Jan 2022. On 1 April 2022, Nine announced it had launched an exclusive partnership with ad-tech/martech platform AdGreetz to introduce new 'Dynamic Ads' technology. See Nine, '[Nine launches cutting edge advertising platform on 9Now](#)', 1 April 2022.

'Poorly crafted regulation will ... make Australia less competitive and less attractive as a destination for international capital. This is not only through the direct costs of bad regulation, but also by disincentivising existing businesses from modernising their business models - either through new explicit regulatory barriers, or from the signal sector poor specific regulation sends about government's attitude towards what the Discussion Paper calls 'digital' activities. This would be a very poor outcome: Australia's future prosperity relies on businesses modernising and taking up new technologies and ways of doing business. Without this, we will be left behind.'¹⁶

Fourth, Australia can learn from international experience.

Several stakeholders have suggested that Australia should take the opportunity to learn from international experience.¹⁷ We agree. The DMA is a novel and untested piece of legislation. The impact of its provisions on consumer welfare, innovation, efficiency and competition will take time to be known. Similarly, Australian policy makers could gain valuable insights from observing the outcomes of digital platform regulation in the UK (or US), if and when that occurs, noting the different design and implementation approaches currently being explored in those jurisdictions.

We reiterate our position that any new framework should seek to promote Australian consumers' welfare, while promoting and protecting robust competition, economic efficiency and innovation. If the ACCC is considering recommending rules that have the objectives of protecting or promoting the welfare of producers, this should be made clear and subject to consultation, given that it would be a significant departure from the objectives of the CCA.¹⁸

* * *

In conclusion, we do not think the fact that some international regimes are considering introducing platform regulation means that it is a foregone conclusion that Australia should do the same or shortcuts should be taken. Instead, we encourage the ACCC and Australian Government to conduct a fulsome cost / benefit analysis in considering the need for new rules, and seek to learn from other regimes, to avoid unintended consequences for Australian citizens and businesses.

¹⁶ Business Council of Australia, '[Digital Platforms Services Inquiry - Interim Report: Submission on the Discussion Paper for Interim Report No. 5](#)', April 2022, 3.

¹⁷ See, for example, submissions in response to the Discussion Paper from the [Law Council of Australia](#), [Amazon Australia](#) and [Gumtree](#).

¹⁸ The submission in response to the Discussion Paper by the Global Antitrust Institute, Antonin Scalia Law School of George Mason University discusses the risks of rules that 'rein in the competitive striving and performance improvements of large digital platforms so that smaller rivals will not fall too far behind' and 'focus on the interests of competitors, without adequate consideration of ultimate effects on consumers' (at 6). We agree that '[t]he antithesis of competition would be a stifling regulatory regime that restrains innovators in how they can use their innovations to benefit and thereby win customers, and whose incentives to innovate are impaired by requirements to share the use of their innovations with rivals' (at 5). See Antonin Scalia Law School, George Mason University, '[Comment on the ACCC Digital Platform Services Inquiry's Discussion Paper for Interim Report No. 5: Updating Competition and Consumer Law for Digital Platforms Services](#)', 2022.

For completeness, this is also the case in respect of any proposed consumer measures specific to large digital platforms. Like the DMA, the *EU Digital Services Act (DSA)*, is novel and untested, and its impact will not be known for several years. The DSA's official text is yet to be made available. Its obligations will not come into effect before at least mid-2023 (for very large online platforms and very large online search engines), and before 2024 (for other intermediaries and platforms).

Similarly, the UK Government had been considering further consumer protection laws in the form of the *Online Safety Bill*. There is, however, significant uncertainty regarding the future contents of the bill. We expect the UK Government to reconsider the bill later in the year. It is uncertain whether the Government will support the bill in its current form, or whether significant changes will be made.

We reiterate our position that proposals to strengthen Australia's consumer protection regime should be directed to addressing any gaps in the current regime, consistent with other domestic laws and reform proposals, and apply economy-wide.

II. APP STORES

Some stakeholders have raised concerns regarding app stores. Most concerns are focused on Apple, though some raise issues with our app store, Google Play, too. Complaints are raised, in particular, at the fact we charge a service fee to distribute apps on Google Play and that we use Google Play Billing as the means to collect the fee.

We wanted to correct some of the misconceptions around Google Play. We do not propose to address each and every claim made during the ACCC's consultation. Rather, we want to provide a very short background to how Google Play works and its billing system and payments policy. We also want to be clear about the efforts we make to ensure transparency and fairness on the platform.

Background and development of Google Play

Android is an open mobile platform. Anyone can build devices using the Android operating system for free under an open-source licence. Promoting an open Internet that is accessible to all is fundamental to our company ethos.¹⁹

In line with this open approach, Android was designed to create a community of third-party developers creating apps for use on Android devices. Unlike on some other platforms, app developers on Android can choose to distribute their apps on any of the competing app stores available on Android devices (for example, Samsung's Galaxy Store,²⁰ or Amazon's

¹⁹ Google Official Blog, '[The meaning of open](#)', 21 December 2009. See also [Google's Response](#) to the Discussion Paper, Q.1.

²⁰ Samsung, '[Galaxy Store](#)'.

Appstore²¹). Google Play is just one of these app stores, albeit it is the most popular with Android users and developers.

Unlike some other platforms, Android also allows consumers to download apps directly from websites (known as 'sideloading').²² Developers can also gain distribution on Android by negotiating preload deals with OEMs and distributing their services on the web.

Google Play also competes for app distribution with many other platforms outside of the Android ecosystem. In particular, Android and Google Play face intense competition from iOS and Apple's exclusive App Store (as the only distribution channel for apps on iOS). Google Play and the App Store compete head-to-head for developers and users on price as well as innovation and quality.

Google therefore has a strong incentive to generate value for app developers so that they choose to distribute their apps on Google Play and invest in their Android apps, ensuring that Google Play and the broader Android platform can compete effectively with Apple's iOS and other platforms.

Google Play creates value by providing app developers a platform through which to distribute their apps to users. Google Play also provides security, development, optimisation, and billing services across devices, which enable developers to reach billions of users globally. That value includes:

- **Developer tools, guidance and support:** Developers can run experiments, beta tests, optimise store listings, analyse performance, and more. These services facilitate development, launch, and growth of apps and create important cost savings for developers. Google regularly updates Google Play and introduces new features that help developers get their apps discovered, improve their content, and monetise their apps. Our dedicated blog also provides access to hundreds of insights for developers.²³
- **Security:** Consumers trust Android and Google Play because of their security features. For example, Google Play Protect scans over 100 billion apps per day for malware, data breaches, and fraud. A lack of trust would discourage users from downloading apps to their devices or entering into online transactions.

²¹ Amazon, '[Amazon Appstore App For Android](#)'.

²² Without protections, sideloading does carry security risks. Unlike apps downloaded through Play, sideloaded apps do not go through the review and approval processes that app stores have in place. Our sideloading process is easy to use but presents appropriate warnings to consumers of the security risks involved, to ensure their choice is fully-informed. If a user chooses to permit an app (such as a browser) to sideload apps, they can authorise this 'once and for all' via the settings app. In Android 12, the warning message itself directs the user to the relevant settings page (and back again) so that users can grant the permission in a single flow.

²³ Android, '[Android Developers Blog](#)', 21 October 2021.

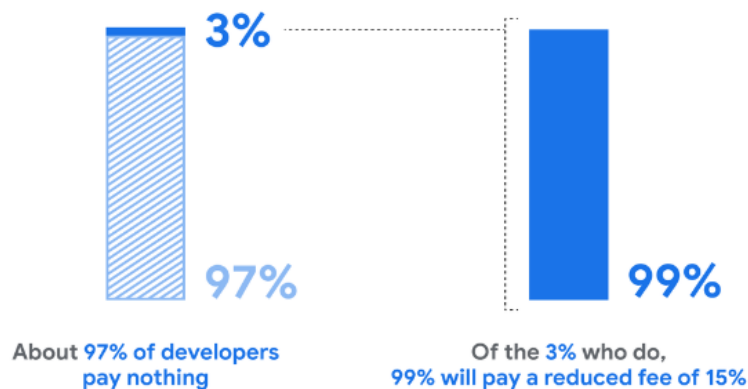
- **Technical infrastructure:** Developers can host and distribute apps globally and seamlessly. Google also provides backend infrastructure to enable developers to update their apps on all devices globally.
- **Reporting:** Google provides developers with extensive reporting on their apps, and continually invests to make metrics and visualisations more helpful. These reports help developers understand, for example, the lifecycle of their apps, from how they are discovered in Google Play, to how users engage with them and what users pay for.
- **Global User Base:** Google Play provides a place for developers to distribute their apps and games globally, available in over 190 countries and to more than 2.5 billion users with personalised recommendations and easy discovery of high-quality apps.
- **Features promoting user activity and engagement on the Google Play platform,** including givebacks like Google Play Points, Google Play Pass, promotions, pre-registration, LiveOps, personalised recommendations, and subscription services.
- **New Android platforms:** Google has worked to add new form factors such as Chromebook, Auto, and TV, to help developers increase their reach in new ways.
- **Billing system:** Google Play offers a safe and trusted payment experience that delivers substantial benefits for users and developers. Google Play's billing system is not simply a payment processing system, but rather an integrated, comprehensive payments platform. On top of providing over 200 forms of payment (including credit cards and PayPal), it manages the check-out flow and after-sales services such as refunds, subscription management, parental controls and budgeting.

Google Play charges developers a service fee as remuneration for its services

Google Play's service fee is the principal means by which Google is compensated for the value it provides to developers through Google Play. Just as it costs money to develop, launch, and market an app for developers, it costs money to develop, launch, market and maintain a high-quality app store.

Only 3% of developers offering apps on Google Play are subject to a service fee, and 99% of those developers are eligible for a service fee of 15% or less. Developers are subject to the Google Play service fee only if they choose to generate revenue from the sale of their apps, or from in-app purchases of digital content in apps downloaded through Google Play. If the developer chooses to distribute its app for free, distribute its app outside of Google Play, or monetise its app in any other way (e.g. through advertising, or outside Google Play, such as selling digital content through the developer's website that can then be accessed in the app), the developer is not subject to any service fee and pays only a one-time charge of USD 25 to register a Google Play Developer Account. Service fees also do not apply to the purchase of physical goods or services (including for example ride-hailing or food

delivery services) or to other transactions (e.g. certain charitable donations) where Google does not wish to impose a service fee as a matter of policy.



By structuring service fees as a percentage of developers' revenues, Google Play lowers entry barriers that app developers would face from an upfront charge. Developers do not have to raise capital to cover service fees before they launch. Developers pay service fees only after they succeed in earning revenues subject to service fees. This enables developers to take risks in launching their apps and to use their limited resources on creating innovative and better apps for their users.

Google Play's revenue-based fee structure also ensures that all developers, including those subject to a service fee, are able to be successful on the platform. Smaller developers are not disproportionately impacted by paying a greater proportion of their revenue in service fees. Developers that derive substantial in-app purchase revenue through Google Play, in turn, pay a proportionate sum towards the upkeep of the platform.

Based on partner feedback and in response to competition to attract developers from Apple and other app distribution channels, Google Play's pricing model has evolved over time to help all developers on our platform succeed. For the small minority of developers that do charge for their apps or in-app content, the Google Play service fee rates are highly competitive. Google Play's service fee rates are comparable to other rival digital stores, including the Samsung Galaxy Store, Amazon Appstore, Microsoft Xbox, Sony PlayStation, Nintendo Switch and Apple App Store. And even though Google Play has become more secure and benefitted from continuous technological improvement, Google Play's service fees have only ever decreased since Google Play was first introduced, to compete with other app distributors.

Our service fee rate reductions have also occurred in the context of significant growth in the number of downloads and the revenue generated by developers distributing their apps on Google Play. Public data indicates that, globally:

- 111.3 billion apps were downloaded on Google Play in 2021, an increase of 2.6% on the previous year.²⁴
- Developers' revenues on Google Play increased by 24% from 2020 to 2021.²⁵
- Total consumer spend on Google Play increased by 23.5% from 2020 to 2021.²⁶

In short, Google Play's service fees reflect the value of the services we provide and we work hard to ensure that Google Play is an attractive distribution platform for developers.

Google Play's Payments Policy

Google Play's Payments Policy requires purchases of digital content associated with apps distributed through Google Play to go through Google Play's billing system.²⁷ Google Play's billing system provides a secure, trusted payments system for users and developers.

The requirement to use Google Play's billing system also allows Google to efficiently collect Google Play's legitimate service fee, without incurring additional costs to monitor and enforce recovery of service fees, or imposing additional administrative burden on developers. Allowing alternative billing systems to be used within Google Play would reduce this efficiency. It may also result in developers who are otherwise required to pay the service fee avoid it, while still having access to, and benefit from, all the services and tools Google Play provides.

Google Play's billing system does *not* prevent users from paying using their chosen method. Google Play provides a choice of over 200 forms of payment, including credit and debit cards, PayPal, direct carrier billing, and gift cards.

We understand that some stakeholders have raised concerns that app developers offering digital content are prevented from directly communicating with their users about purchasing channels other than Google Play's billing system. This is not correct. Under Google Play's Payments Policy, developers *are* able to inform their users outside the app of other ways to pay for digital content. Our Payments Policy also makes it clear that developers can continue to use contact information obtained in-app to communicate with users out-of-app, including about subscription offers or lower-cost offerings on a rival app store or the developer's website.²⁸

²⁴ Sensor Tower, '[Global Consumer Spending in Mobile Apps Reached \\$133 Billion in 2021, Up Nearly 20% from 2020](#)', December 2021.

²⁵ Business of Apps, '[App Revenue Data \(2022\)](#)', 30 June 2022.

²⁶ Sensor Tower, '[Global Consumer Spending in Mobile Apps Reached \\$133 Billion in 2021, Up Nearly 20% from 2020](#)', December 2021.

²⁷ Google Play Console Help, '[Payments - Play Console Help](#)'.

²⁸ Google Play Console Help, '[Understanding Google Play's Payments policy - Play Console Help](#)'.

Google recognises, however, that a discussion has emerged around billing choice within app stores. In this context, Google is exploring alternative approaches to billing for Google Play, which meet Google's safety and security requirements and enable the collection of a service fee. One of those approaches is our billing pilot, starting with Spotify, slated to launch later this year.²⁹ This program will allow users to have the ability to use and benefit from Google Play's billing system if they choose, while providing developers with the option of offering users an alternative billing system for in-app purchases.

Google Play's billing system

Google Play's billing system benefits users and developers. Android users expect that when they pay for apps, subscriptions, or in-app content, their payments are safe. Google Play's billing system is an efficient means of meeting users' expectations of a trusted, safe, secure, and consistent payment system. For example, it:

- Offers a consistent interface and user experience, and enables users to enter and store their payment details only once.
- Offers a safe and secure environment for storing user payment data.
- Enables users to manage and track their purchases and subscriptions, and apply control and security features, like budget controls, payment controls (requiring re-authentication prior to every purchase) and parental controls.
- Allows users to effectively review payments, including recurring charges, and gives them clear upfront information about the terms of payments on subscription plans.
- Performs fraud checks, validates the developer and the user's identities, and confirms that payments have been accurately delivered.
- Provides a streamlined refund process whereby users can obtain refunds without having to access individual apps and developers' processes.
- Provides a choice of over 200 forms of payment, as described above.

On the developer side, Google Play's billing system provides developers with a secure and reliable process for collecting payments for their apps and in-app content, and for managing refunds and customer complaints. This is particularly valuable for the many app developers that do not have these capabilities in-house.

Several third-party billing systems do not offer the above benefits or provide all of the services we provide as an app store. This can expose users to considerable risks. Bad actors can lure users into subscription purchases with high fees, unclear terms about

²⁹ Android Developers Blog, ['Exploring User Choice Billing With First Innovation Partner Spotify'](#), 23 March 2022.

auto-renewal, and make them difficult (or impossible) to cancel.³⁰ This then undermines the willingness of users to trust apps on Google Play, which impacts all developers in the ecosystem. It also undermines user trust in the Android ecosystem and weakens its competitiveness against Apple's iOS ecosystem.

Google has a transparent and fair app store review process

Separately, some stakeholders have expressed concerns that app store reviews and enforcement processes are difficult to understand and arbitrary.

Google Play operates a robust and fair app review process to create a safe environment for users and developers. Developers who wish to distribute their apps through Google Play, agree to adhere to Google Play's policies (i.e. the Developer Distribution Agreement, and Developer Program Policies). This includes policies against restricted content, impersonation and infringing intellectual property rights, privacy, deception and device abuse.³¹

Google Play's app review criteria are designed to be clear and easy for business users to understand. The Developer Program Policies are publicly available online, written in plain language (not 'legalese'), and displayed in a tile-based format on Google's support pages.

Upcoming updates to Google Play's policies are published online³² and developers are given notice before new policies are introduced or existing policies are updated with new requirements.³³

Where Google finds an app is in breach of the Developer Distribution Agreement or Developer Program Policies, we act in accordance with the enforcement process outlined on our Developer Policy Centre page.³⁴ We believe we provide a fair, flexible and proportionate intervention and appeal process for non-compliant apps, as described in Annex Q.13 of our Response to the Discussion Paper.

Our robust app store process helps us to protect consumers from malicious, harmful, and exploitative content on Google Play. The ACCC has recognised these harms, and found

³⁰ For example, the US Federal Trade Commission has filed a lawsuit against Match because the non-transparent and cumbersome cancellation process makes it very difficult for users to cancel their subscriptions, See [FTC vs. Match Group, Inc.](#), Case No. 3:19-cv-02281 (N.D. Tex.), 25 September 2019.

³¹ Google Play, '[Developer Policy Center](#)'.

³² Google Play, '[Developer Policy Center](#)'.

³³ Google Play gives advance notice of upcoming changes to Play's policies (typically 30 days', or longer if significant technical changes are required to comply), except for changes that are required to take immediate effect (e.g. required by law). For examples of upcoming policy changes, see: Play Console Help, '[Updates to Google Play Policies](#)', 2022.

³⁴ Google Play, '[Developer Policy Center](#)'; Google Play Console Help, '[Enforcement process](#)'.

that 'Apple and Google should take further measures to prevent and remove apps that harm consumers'.³⁵ It is to protect consumers that we have developed:

- Extensive policies directed at preventing harmful apps and content³⁶ and robust app review processes to detect harmful apps, as described above;³⁷
- Troubleshooting tools to allow Google Play users to report or flag harmful apps;³⁸ and
- Controls to protect consumers on Google Play, such as Google Play Protect that runs safety checks on installed apps.³⁹

At the same time, the ACCC and stakeholders have criticised Google and Apple's app review processes for delaying or rejecting apps.⁴⁰ In assessing such claims, it's important for the ACCC to consider the trade-offs in terms of user harm in introducing rules that prevent Google from acting swiftly to remove harmful apps or thoroughly reviewing apps to detect harmful apps.

In conclusion, app store interventions require careful design and assessing justifications.

As the ACCC will appreciate, the issues around app stores and their billing systems are complex. Any regulatory measures that impact app stores should be based on a full understanding of the facts and the evidence, and testing justifications against the evidence. The alleged benefits of regulatory changes need to be balanced against costs and risks, in terms of chilling innovation, risks to security, and harm to consumers if we are, for example, unable to thoroughly review apps or act quickly to remove harmful apps from our store. The benefits of regulatory changes, when implemented to address the concerns of a few large developers, should also be balanced against the costs and risks to the majority of app developers who benefit from the current processes in place.

We trust the ACCC will consider the information provided in this paper and will undertake a thorough examination of the evidence available on app stores as part of the process of designing any proposed regulatory measures.

³⁵ [Discussion Paper](#), 51.

³⁶ We are constantly updating these policies to address new and emerging harmful business practices. As noted above, Google Play gives advance notice of upcoming changes to Play's policies.

³⁷ Google Play, '[How Google Play Works](#)'.

³⁸ See Google Play Help, '[How to report an app on the Google Play Store](#)'; and Play Console Help, '[Report inappropriate apps](#)'.

³⁹ Krish Vitaldevara, Google Security Blog, '[How we fought bad apps and developers in 2020](#)', 21 April 2021.

⁴⁰ [Discussion Paper](#), 55.

III. CHOICE ARCHITECTURE AND CHOICE SCREENS

The Discussion Paper references the ACCC's previous recommendation to implement 'a mandatory choice screen - which would provide users with the ability to choose which search app will be used as the default for searches conducted on their mobile devices - initially only for Android mobile devices'.⁴¹ The ACCC suggested this measure would be able to 'facilitate greater consumer choice and help reduce barriers to entry in the supply of search services...addressing default biases and customer inertia.'⁴² Various stakeholders have commented on the need for choice screens, and the appropriate design of choice screens.

Further to our submission of 7 May 2021, which discussed the benefits of default and preinstallation arrangements and responded to proposals to mandate a choice screen on Android devices, we'd like to take this opportunity to provide our views on choice architecture, i.e. '[t]he design of user interfaces that influence consumer choices',⁴³ and the role of choice screens, to address some inaccuracies or misunderstandings.

We believe that well-thought through choice architecture can address the ACCC's stated concerns about consumer inertia.⁴⁴ This is different to mandating a choice screen on Android only, which would not address these concerns. The following pro-consumer principles inform our thinking.

First, too many choices can have downsides for users.

Promoting active choice entails certain costs. These costs can result in a less seamless user experience, and actually *reduce* users' ability to make active choices, as is well established in academic literature. In particular:

- **Choice tools can add friction to the user experience.** Surfacing choices when the user is in the middle of a task interrupts their journey through a platform's user interface. For example, the ACCC has recognised that 'consumers can benefit from having browsers pre-installed and search engines pre-set as defaults on their mobile devices.'⁴⁵ These benefits would be lost if each and every instance of preinstallation or defaults required users to go through an enhanced choice solution.

Moreover, pre-selected choices can enhance consumer utility by picking the best option for the majority of users in circumstances where they may not be able to (or

⁴¹ [Discussion Paper](#), 86.

⁴² ACCC, '[Digital platform services inquiry - September 2021 interim report](#)', 17.

⁴³ Discussion Paper, 1. The full definition of choice architecture is: 'The design of user interfaces that influence consumer choices by appealing to certain psychological or behavioural biases.'

⁴⁴ ACCC, '[Digital platform services inquiry - September 2021 interim report](#)', 7.

⁴⁵ [Discussion Paper](#), 46.

do not want to go to the effort of) selecting the best option for themselves, either due to lack of information or cognitive biases.

- **Forcing users to make too many choices can result in ‘decision fatigue’.** Cookies are a useful example to illustrate decision fatigue. Under current arrangements, users must accept or reject cookie pop-ups on every website they visit, meaning they are often prompted with the same choice multiple times within the space of a few minutes.⁴⁶ Over time, this encourages users simply to dismiss cookie prompts instead of meaningfully engaging with them, particularly since the pop-up appears at a time when the user is focused on a separate task (visiting a website and consuming content), rather than engaging with the issue of their personal data.
- **Choice overload can undermine user decisions.** Too many options in a given choice can lead to choice overload. Users become less engaged and frustrated, and ultimately carry out less activity.⁴⁷ This is a well-known effect known as the ‘paradox of choice’; as recognised by a 2019 article, ‘potential negative outcomes of choice overload identified by researchers include frustration, dissatisfaction, post-choice regret, post-choice dissatisfaction, ambivalence about choice outcomes, choice deferral, and less motivation to choose.’⁴⁸

To illustrate, Netflix offers over 6,500 titles to users in the UK.⁴⁹ Part of Netflix’s proposition is its ability to present its choice architecture in a way that maximises relevant choices for users, and does not lead to choice overload (while maintaining the ability of users to search and browse across a wide stock of titles). According to one Netflix product designer, ‘[t]he virtue is that users want the power and control of the product. But along with that power and control comes that... frustration that can soak up precious watch time: “I’m browsing too long and I’d rather actually be watching right now.”’⁵⁰

Choice regulation therefore requires careful balancing. It should seek to recognise and preserve the benefits of preinstallation and defaults; facilitate active user decisions; and

⁴⁶ Information Commissioner Elizabeth Denham has commented: ‘I often hear people say they are tired of having to engage with so many cookie pop-ups. That fatigue is leading to people giving more personal data than they would like.’ See ICO, ‘[ICO to call on G7 countries to tackle cookie pop-ups challenge](#)’, 7 September 2021.

⁴⁷ See generally Antti Oulasvirta et al., ‘[When more is less: the paradox of choice in search engine use](#)’, 2009; Böhme, R and Korff, S, ‘[Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation](#)’, 2015; Iyengar, S and Lepper, M, ‘[When Choice is Demotivating: Can One Desire Too Much of a Good Thing?](#)’, June 2000.

⁴⁸ Burns, L, Koenig, H and Tung, T, ‘[Choice Overload and Online Approach Behavior](#)’, International Journal of E-Business Research, Vol. 15, Issue 4, October–December 2019, 57 and the research studies cited therein.

⁴⁹ See Statista, ‘[Number of Titles Available on Netflix, Amazon Prime Video, NowTV and Disney+ in the United Kingdom](#)’, March 2022.

⁵⁰ See Laurent, S, ‘[Netflix vs. decision fatigue: How to solve the paradox of choice](#)’, 14 May 2021.

avoid *undermining* user choice by inadvertently creating decision fatigue or choice overload.

Second, effectiveness of choice – the ability for users to make active and informed choices – does not turn on outcomes.

Assessing the success of a choice measure should not turn on the result, i.e., what users ultimately choose, but whether the choice being presented to users effectively supports their ability to make informed choices. The ultimate goal of a choice tool should be to provide users with the ability to make choices, not to skew users' choices towards less popular options.

In other words, choice interventions – like competition law as a whole – are not intended to pick winners. And they cannot, therefore, be judged based on which service achieves the best results from a choice tool. Rather, the relevant question is whether the choice being presented to users effectively supports their ability to make active and informed choices.

This has two implications when considering potential choice tool interventions:

- A choice tool should not steer users towards options they would not otherwise select. High quality or popular options should not, for example, be artificially hidden or demoted in the choice tool.
- The success of a choice tool – if properly designed and implemented – should not be judged by users' selection of a particular option. An apparently low proportion of users selecting alternatives does not mean that the choice tool itself is deficient. Rather, it may reflect the popularity of the product. For example, Google Search is popular due to its high quality, as evidenced in our Response to the Discussion Paper.⁵¹ The ACCC has also concluded that Google 'continually improve[s] the relevance of its search results.'⁵²

Third, choice interventions should not be applied discriminatorily. Questions about choice architecture and design should apply to platforms in equal measure, particularly to ensure that there aren't distortions in competition among various devices.

Following a careful assessment, if it's decided that a measure to increase choice would be beneficial to users, there is no reason why such a measure should not apply to all platforms.

Any proposals to impose choice screens should take into account the following:

- First, to the extent that regulatory interventions to increase choice are adopted to 'address[...] default biases and customer inertia',⁵³ there is no reason they should

⁵¹ See Annex Q.1.2 of [Google's Response](#) to the Discussion Paper.

⁵² [Discussion Paper](#), 41.

⁵³ ACCC, '[Digital platform services inquiry – September 2021 interim report](#)', 7.

apply only to Android devices. The ACCC has suggested that it should have the power to mandate the implementation of a search engine choice screen in relation to Android mobile devices,⁵⁴ as well as ‘other devices (e.g. desktop devices) and operating systems (e.g. non-Android mobile devices)’, subject to further consideration and user testing.⁵⁵ Although we do not agree that interfering with the market to mandate choice screens is warranted, any mandating of choice screens should apply universally across Android, Apple, and Windows devices.

- Second, it would distort competition to implement regulation that burdens some platforms, but not others. Questions about choice architecture and design apply to all platforms in equal measure. Requiring certain platforms to implement choice screens and not others will not enhance competition amongst those platforms based on merits.
- Third, measures with the stated purpose of increasing user choice should not be discriminatorily applied to platforms that already provide more choice to users than other platforms. In this regard, we note that the ACCC has contrasted the ‘open source and licensable’ Android operating system with the ‘closed source and non-licensable’ Apple iOS,⁵⁶ over which Apple ‘maintains complete control’, while also finding that Apple devices comprise over 50% of the mobile devices supplied in Australia.⁵⁷

IV. DARK PATTERNS

The ACCC is also considering the need for potential measures to address ‘dark patterns’. Potential measures canvassed by the ACCC include:

- an unfair trading practices prohibition; and
- specific rules requiring digital platforms to ensure their user interfaces and choice architecture are designed fairly without taking advantage of behavioural biases to undermine consumer choice or nudging consumers towards a certain outcome that benefits the platform.⁵⁸

Many stakeholders addressed dark patterns in their submissions or at the consumer roundtable. A majority agreed that there is no common understanding of what constitutes a dark pattern, that dark patterns are not unique to digital platforms, and that some examples of dark pattern practices given by the ACCC in its Discussion Paper are

⁵⁴ ACCC, [‘Digital platform services inquiry - September 2021 interim report’](#), 10.

⁵⁵ ACCC, [‘Digital platform services inquiry - September 2021 interim report’](#), 17.

⁵⁶ ACCC, [‘Digital platform services inquiry - September 2021 interim report’](#), 20.

⁵⁷ ACCC, [‘Digital platform services inquiry - September 2021 interim report’](#), 109.

⁵⁸ [Discussion Paper](#), 97.

commonly employed by traditional businesses online and offline. There was a range of views on whether existing laws are sufficient to address harmful dark patterns,⁵⁹ and whether a general, economy-wide prohibition on unfair trading practices would sufficiently deal with any existing gap.

We'd like to provide our views on these issues, and correct some misunderstandings about alleged 'dark patterns' on Chrome.

Dark patterns are economy-wide issues and require further examination.

The EC has recently completed an in-depth study of dark patterns, and published its findings in its 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation - Final Report' (**EC Report on Dark Patterns**).⁶⁰ The EC Report on Dark Patterns was based on mystery shopping exercises and experiments in Europe. Nonetheless, it suggests that dark patterns are not only (nor predominantly) employed by large digital platforms,⁶¹ that there are different views on the types of practices that could be regarded as dark patterns,⁶² and that dark patterns could be addressed by existing laws.⁶³ The report suggests that measures to deal with dark patterns should 'go beyond regulatory interventions and involve businesses and the designer community directly, for example by developing guidelines and practical examples, which allow [businesses] to determine ex ante whether the practices that they are considering may be unfair.'⁶⁴

A local report, by the Consumer Policy Research Centre (**CPRC**), based on a survey of 2,000 Australians, exploring the prevalence and impact of dark patterns in Australia, also confirms that dark patterns are not limited to or concentrated on large platforms.⁶⁵ According to the CPRC, participants identified businesses from almost every sector as using dark patterns on their websites and apps.⁶⁶ The top five were clothing and

⁵⁹ For example, [The Law Council of Australia](#) and the [Developers Alliance](#) considered the existing laws in the Australian Consumer Law are sufficient to address the ACCC's dark patterns concerns.

⁶⁰ Lupiáñez-Villanueva et al., Directorate-General for Justice and Consumers (European Commission), '[Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation](#)', April 2022.

⁶¹ [EC Report on Dark Patterns](#), 6. The report finds that dark patterns are prevalent and increasingly used by traders of all sizes, not only large platforms. According to the EC's mystery shopping exercise, 97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern.

⁶² [EC Report on Dark Patterns](#), Tables 2-4.

⁶³ [EC Report on Dark Patterns](#), Table 11.

⁶⁴ [EC Report on Dark Patterns](#), 7.

⁶⁵ CPRC, '[Duped By Design, Manipulative online design: Dark Patterns in Australia](#)', June 2022.

⁶⁶ CPRC, '[Duped By Design, Manipulative online design: Dark Patterns in Australia](#)', June 2022, 8.

accessories, online marketplaces, tech products and services, social media and department stores.⁶⁷

The studies cited above support our views that:

- Further exploration of dark patterns in Australia is needed to better understand their characteristics and the extent to which they are causing harm to consumers.
- Having identified harmful dark patterns, it is necessary to consider whether those practices can be addressed by existing laws, such as the prohibitions on misleading or deceptive conduct, unconscionable conduct and unfair contract terms.
- To the extent there is a gap in existing laws, these issues are best addressed as economy-wide issues.
- Any new rules should avoid creating overlapping obligations that are inconsistent with other regulatory frameworks, including Australia's existing consumer laws, the proposed prohibition on unfair trading practices, and upcoming reforms in relation to unfair contract terms and online privacy.

Google Chrome does not use 'dark patterns'.

Some stakeholders have raised concerns that Google employs 'dark patterns' to supposedly discourage users from installing and retaining 'extensions' in Chrome that change the default search engine on desktop. It has also been suggested that this is a form of self-preferencing, which is said to stifle competition from alternative search engines.

This is not correct, for the reasons below.

First, the process for installing extensions in Chrome supports, rather than subverts, user choice. It involves only two notifications to users:

- **Permissions notification:** When users first click a button to install a Chrome extension, a pop-up asks them if they want to add the extension and lists the extension's permissions. This notification ensures users understand how extensions will use their data (among other things). It gives users the chance to review an extension's permissions carefully, rather than simply 'clicking through'. The same notifications apply consistently to all Google and third-party extensions (both search and non-search). For example, the same notification would appear if a user sought to install the 'Google Arts & Culture' extension.
- **Confirmation dialogue:** A further pop-up notification – 'to change back' to a user's default search setting – appears once only after installation. This is not specific to changing back to Google Search; the confirmation dialogue appears whenever an extension has changed a user's search settings from what the user has identified as

⁶⁷ Google was not among the top 10 businesses that consumers identified as using dark patterns. See CPRC, '[Duped By Design, Manipulative online design: Dark Patterns in Australia](#)', June 2022, 8.

their default in Chrome's settings. For example, if a user had DuckDuckGo as their default search engine on Chrome and downloaded an extension that forcibly changed the user's search settings, the confirmation notification would come up asking if the user wanted to change back to DuckDuckGo search. The confirmation dialogue gives users an easy 'undo' option, particularly if they 'clicked through' inadvertently. It is not a 'dark pattern' to ask users if they want to change back to their default search provider, rather than to 'keep' the new extension. Both pop-ups (permission and switch back) focus on what will change if users exercise the choice presented to them: changing to the new search service, changing back to their existing search service.

The messages above are each displayed once only. They do not appear when users interact with features on the search page itself, such as entering queries in the search bar. Nor do these messages appear when a user has changed the default search engine via the ordinary means (e.g. by configuring the settings menu in Chrome - discussed below).

Second, the confirmation prompts are proportionate to potential consumer harms. Extensions may create particular privacy risks that need to be managed. For example, 'host permissions' enable developers to read and change users' data on the websites they visit, including tracking users' activity online.⁶⁸

Third, there is nothing exceptional about the use or design of Google's prompts:

- Extensions themselves can show automatic 'switch back' prompts after they have been uninstalled. Neither these prompts, nor Google's prompts, are 'dark patterns' simply because they present an 'undo' option.
- Chrome's approach to installing extensions is, in fact, more permissive than the approaches taken by other major browsers.

Fourth, on desktop, users can set a search engine as the default in the Chrome settings menu, where other search engines can be picked from a list (the relevant menu is reached with three clicks in Chrome).⁶⁹ In this process, users are not asked to confirm their choice nor any other questions: Chrome simply uses the chosen search engine as the default. This is because – unlike installing an extension – changing the default search service via the settings menu does not give third parties additional permissions over the user's activity. It is also clear in this case that the user is actually intending to change their settings (rather than it being an incidental change resulting from the download of an unrelated extension).

⁶⁸ Certain extension providers have been found to 'package', within a single extension, both (i) a feature that users are likely to want and which is prominently advertised (e.g. a privacy shield or a particular wallpaper), and (ii) permission for the extension provider to take control of the user's search settings, which is not prominently explained to users in advance and might in hindsight be perceived as 'hidden' by users. This 'packaging' may be advantageous for extension providers because search settings can be readily monetised. However, it can confuse or frustrate users who might not want the provider to change their search configuration and might have refused permission if they had been aware of this part of the 'package' in advance.

⁶⁹ Google Chrome Help, '[Set your default search engine](#)'.

V. SCAMS

In submissions and at the consumer roundtable, most stakeholders that addressed the topic of scams acknowledged that scams are perpetrated by bad actors using many methods not limited to the largest digital platforms. The ACCC's report 'Targeting Scams: Report of the ACCC on scams activity 2021' confirms that telephone and text message scams continue to account for the vast majority of reported scams.⁷⁰

Google agrees with many stakeholders that it is appropriate to consider the issue of scams holistically. In our experience, scammers and other motivated bad actors are nimble and not easily deterred — addressing scams on one platform will simply shift the problem to another platform or forum. Scammers are also quick to adapt to trends in enforcement and it is challenging to stay one step ahead of them.

We strive to protect consumers from scams and malicious, harmful and exploitative content and apps on our products. We work around the clock to protect our users in Australia and around the world from bad actors, with teams dedicated to fighting abuse. We do this through comprehensive policies and enforcement of those policies. We described our efforts to combat scams on Search, our ads products and Play in our Response to the Discussion Paper. Demonstrating the extent and scale of our efforts:

- In respect of **ads**:⁷¹
 - In 2021, we removed over 3.4 billion bad ads, restricted over 5.7 billion other ads and suspended over 5.6 million advertiser accounts.
 - We also blocked or restricted ads from serving on 1.7 billion publisher pages, and took broader site-level enforcement action on approximately 63,000 publisher sites.
 - Over 657,000 ad creatives were blocked from Australian advertisers for violating our misrepresentation ads policies (misleading, clickbait, unacceptable business practices, etc).⁷²
- In respect of **Play**:⁷³
 - We continue to enhance our machine learning systems and review processes, and in 2021 we blocked 1.2 million policy violating apps from being published on Google Play, preventing billions of harmful installations.

⁷⁰ ACCC, '[Targeting Scams: Report of the ACCC on scams activity 2021](#)', July 2022, 7.

⁷¹ Google, '[2021 Ads Safety Report](#)' 4 May 2022.

⁷² Google's [Annual Transparency Report](#) under the *Australian Code of Practice on Misinformation and Disinformation*, May 2022.

⁷³ Google, '[How we fought bad apps and developers in 2021](#)', 27 April 2022.

- We also continued in our efforts to combat malicious and spammy developers, banning 190,000 bad accounts in 2021.
- In addition, we have closed around 500,000 developer accounts that are inactive or abandoned.
- In addition, Google Play Protect continues to scan billions of installed apps each day across billions of devices to keep people safe from malware and unwanted software.
- Our data shows that 99% of apps with abusive or malicious content are rejected before anyone can install them.

Our policies are designed to protect users and often are broader than the minimum legal requirements, and we are continuously looking for ways to improve our efforts to detect and combat bad actors. To take just one area for example, in June 2022, we voluntarily updated our advertising policies for financial products and services to expand our verification program for financial services advertisers to Australia. We are working closely with the Australian Securities and Investment Commission (**ASIC**) to implement our updated policy.⁷⁴

Since we launched this policy in the UK, we've seen a pronounced decline in reports of ads promoting financial scams.⁷⁵ The success of this program in the UK has demonstrated that this is a meaningful and effective solution to safeguarding people online, and gave us confidence to expand verification to additional countries.

As part of the newly introduced verification process, financial services advertisers in Australia will need to demonstrate that they are authorised by ASIC and complete Google's advertiser verification program in order to promote their products and services.⁷⁶ Advertisers have been able to apply for verification since the end of June, and the policy will go into effect on 30 August 2022. Advertisers that have not completed the new verification process by this date will no longer be allowed to promote financial services on Google's platforms.

Putting the continued evolution and enforcement of our policies to one side, if the Government were minded to increase investment and impact in this area, there appear to be opportunities for enhanced scam protection through:

⁷⁴ Google, '[Australian Financial Services Advertisers Verification](#)', 9 June 2022.

⁷⁵ It has been reported that UK bank TSB has had no account holder scammed as a result of advertisements on Google Search since Google introduced this policy in the UK, and that online investment fraud has shifted to other platforms. See The Times, '[Facebook and Instagram blamed for surge in scams](#)', 1 July 2022.

⁷⁶ We note that a stakeholder suggested that Google implement its UK approach in Australia via an industry co-designed Code of Practice, or that the ACCC impose a duty on digital platforms to prevent advertisement for financial scam products, including through an ASIC verification process. Google's voluntarily implemented initiative renders such measures unnecessary.

- **Greater education of consumers about scams**, so they can take the necessary degree of caution when using platform services.

For example, in the UK, Google (and other tech companies, including Facebook, Instagram, Twitter, Amazon, Microsoft and TikTok) have supported Take Five to Stop Fraud, an anti-fraud campaign run by UK Finance.⁷⁷ The tech companies collectively donated a significant amount of advertising to the campaign to help publicise the Take Five to Stop Fraud advice to consumers and enable it to reach a significant proportion of the online population with its important messages.

- **Improved collaboration between industry sectors and the public sector.**

Stop Scams UK - collaboration between banking, telecommunications and technology sectors

Google is one of 17 members of Stop Scams UK (**SSUK**), a not-for-profit, industry-led collaboration between responsible businesses from across the banking, technology and telecoms sectors who have come together to help prevent the harm and loss caused by scams in the UK.⁷⁸ We have started engaging with SSUK in relation to its research into improved intelligence sharing across its members. SSUK's work is in its early stages but currently focuses on establishing:

- what forms of intelligence sharing could be most useful in stopping scams;
- whether that information exists in usable, shareable forms;
- how that information could be shared, looking at both immediate quick wins as well as long-term solutions; and
- regulatory and legal considerations.

We understand SSUK hopes this work will lead not just to the development of data sharing pilots but also the production of guidance, advice, governance and process design, emphasising practical real-world solutions. We support this goal.

UK Online Fraud Steering Group - a public-private partnership

We see governments increasingly working with the private sector to combat cyberthreats (e.g. the Australian Cyber Security Centre works with the private sector on enterprise level cyber attacks). Information sharing partnerships are an increasingly popular initiative enabling governments and firms to share cyber threat and vulnerability information to improve overall situation awareness.

- In the UK, such public-private collaborative initiatives have proved successful. The Online Fraud Steering Group, co-chaired by the National Economic Crime Centre,⁷⁹

⁷⁷ UK Finance, '[Tech companies join banking industry to tackle fraud](#)', 15 September 2021.

⁷⁸ SSUK, '[Membership](#)' (as at 3 August 2022).

⁷⁹ The creation of the NECC in February 2019 was widely welcomed as a way of dealing with what was seen as a 'fragmented approach' to tackling serious economic crime in the UK. The organisation brought together staff

UK Finance and techUK, brings together the technology, banking and finance sectors, government and law enforcement, to work collectively to tackle online/cyber enabled-fraud in the UK.⁸⁰

Google is motivated to protect its users from harm and, as demonstrated by these examples, we go to considerable lengths to combat scams. Any additional measures in relation to scams should be considerate of the breadth of work we already do. Further, to be effective, such measures would need to operate economy-wide, given the nature of scams.

VI. FAKE REVIEWS

The ACCC's small business questionnaire⁸¹ asked stakeholders, among other things:

- whether their business was affected by fake negative reviews and, if so, on which platform (from a specified list);
- whether they were able to 'fix' the fake review; and
- whether certain specified measures, or other measures, would improve their ability to 'fix' fake reviews.

We have raised some concerns with the ACCC about its survey methodology, including the self-selecting audience and leading nature of the questions. We do not consider a sample size of 61 responses (with some responses incomplete) to be statistically significant nor representative. Of the 61 small businesses that responded to the survey, more than half raised concerns with fake reviews, including on the specified platforms, Google, Facebook / Instagram and Amazon, and other platforms like Yellow Pages, booking.com and productreview.com.au.⁸²

To the extent stakeholders indicated they were affected by fake negative reviews on Google, we assume that this relates to **Local Reviews**—a type of user-generated content that Google users can submit to be displayed alongside results for businesses, places, and points of interest on a number of Google properties. Local Reviews help users to make better, more-informed decisions and to share their experiences with other users.

from the National Crime Agency, the Serious Fraud Office, the Financial Conduct Authority, Her Majesty's Revenue & Customs, the City of London Police, the Crown Prosecution Service and the Home Office to coordinate national responses to economic crime.

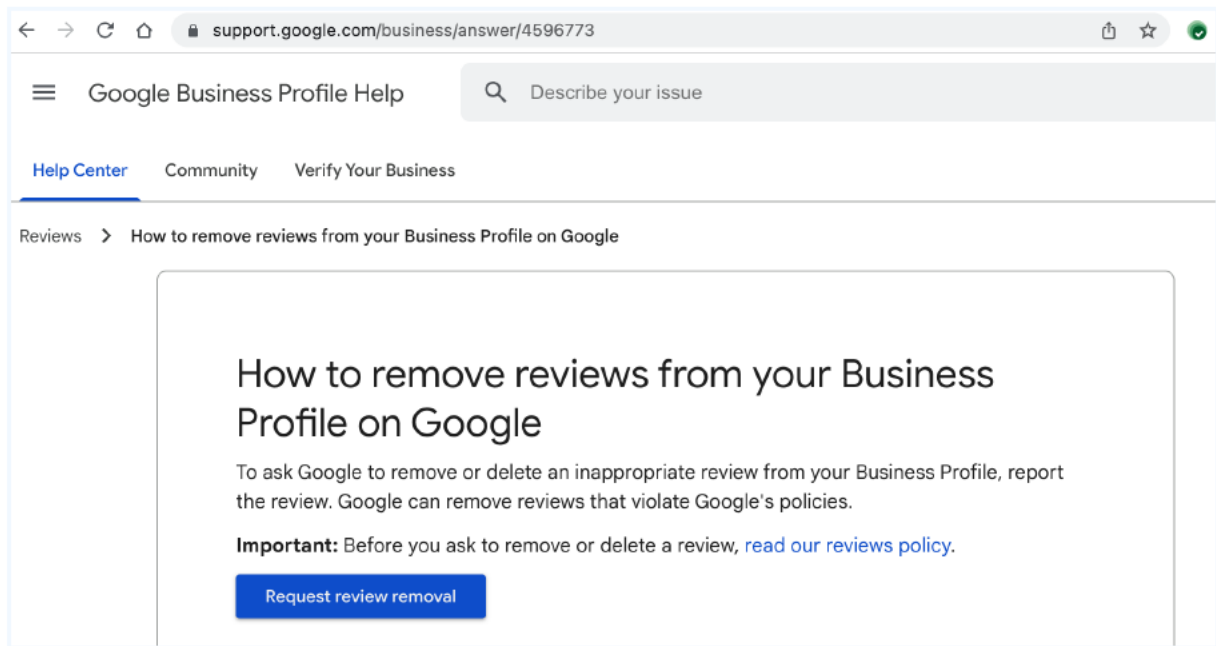
⁸⁰ For further details regarding the Online Fraud Steering Group, see National Crime Agency, '[National Economic Crime Centre](#)'. See also TechUK, '[Online Fraud Steering Group: collaborative efforts to disrupt fraudsters](#)', 1 October 2021.

⁸¹ The survey was available on the [ACCC's Consultation Hub](#) from 29 March 2022 to 29 April 2022.

⁸² ACCC, '[DPSI September 2022 report - Small business questionnaire responses](#)', 10 June 2022.

We invest significant resources in tackling fake Local Reviews.⁸³ We recognise the impact fake negative Local Reviews can have, particularly on small businesses. We are also mindful of fake positive reviews, which may be harmful to consumers, and may also be harmful to competitor businesses. Reviews are tricky, and something we are mindful of managing the integrity of, both fake negative and fake positive reviews.

If a business owner is concerned that a Local Review is fake, they can bring it to Google's attention, including for legal reasons via g.co/legal or otherwise via their account associated with their business profile:⁸⁴



Businesses who submit a removal request using this process can check whether the relevant review was determined to be in breach of Google's policies, and Google now offers the ability to appeal its initial determination:

⁸³ See our blog post for more details: Google The Keyword, '[How reviews on Google Maps work](#)', 2 February 2022.

⁸⁴ Google Business Profile Help, '[How to remove reviews from your Business Profile on Google](#)'.



Manage your reviews

Use this tool to report reviews for removal and check the status of reviews you've already escalated. Reviews that violate the Google review policies can be removed from Business Profiles on Google.

33%

Check the status of reported reviews

These reviews are shown in the order they were posted. Removed reviews aren't displayed.

Review	Rating	Link to review	Decision	Reviewer name
No review text.	5/5 stars	View in Maps 	Report reviewed - no policy violation	

What would you like to do with your reviews?

Appeal eligible reviews

On Google Maps, millions of reviews are posted every day from people around the world.⁸⁵ Google has a rigorous process for assessing the complaints it receives via its reporting mechanisms. We think it is important to remember, however, that fake Local Reviews present some unique challenges, as it is, in many cases, not possible to conclusively ascertain whether a negative review is genuine or fake. It is important that any proposed recommendations take into account the considerable efforts already made to keep abuse, including fake reviews, off our platforms, and the real life complexities involved in doing so. It is also important to consider the perspective of individuals who use reviews to obtain information (both good and bad) about businesses. A requirement (or even an incentive) to remove all reviews about which a business complains would be a bad outcome for consumers.

⁸⁵ See our blog post for more details: Google The Keyword, '[How reviews on Google Maps work](#)', 2 February 2022.