Coalition for APP FAIRNESS

31 March 2022

ACCC, Digital Platform Services Inquiry

Response of the Coalition for App Fairness to the Discussion Paper for Interim Report No.5

I. Introduction

The Australian Competition and Consumer Commission ("ACCC") is undertaking a five-year inquiry into markets for the supply of digital platform services.[1] As part of this inquiry, on 28 February 2022, the ACCC published a discussion paper ("ACCC Discussion Paper") outlining options for addressing harms to competition, consumers and business users in a range of areas dominated by large digital platforms, including social media, search, app marketplaces, general online retail marketplaces and ad tech.[2] At the same time, it launched a consultation, seeking the views of consumers, businesses and other stakeholders on options for legislative reform to address concerns related to the dominance of digital platforms.

The Coalition for App Fairness ("CAF") welcomes the opportunity to submit its observations to the questions raised by the ACCC in the Discussion Paper for the Interim Report No. 5 of the Digital Platform Services Inquiry. CAF is an independent non-profit organization, comprising more than sixty members of all sizes, founded to advocate for freedom of choice and fair competition across the app ecosystem.[3] CAF's vision is to ensure a level playing field for businesses relying on platforms like the Apple App Store to reach consumers and a consistent standard of conduct across the app ecosystem. In this context, CAF has published ten "App Store Principles", enshrining a series of rights that should be afforded to every app developer, regardless of their size or the nature of their business.[4]

CAF agrees with the ACCC's "growing concerns that enforcement under existing competition and consumer protection legislation, […] which by its nature takes a long time and is directed towards very specific issues, is insufficient to address the breadth of concerns arising in relation to rapidly changing digital platform services."[5] CAF, therefore, fully supports the ACCC's decision to assess whether the current legislative framework is sufficient to deal with the conduct of digital platforms

1 Australian Competition and Consumers Commission ("ACCC"), "Digital platform services inquiry 2020-2025", available at https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025.

2 ACCC, "Feedback sought on potential new rules for large digital platforms", 28 February 2022, available at https://www.accc.gov.au/media-release/feedback-sought-on-potential-new-rules-for-large-digital-platforms.

3 See https://appfairness.org.

4 See https://appfairness.org/our-vision/.

5 ACCC, "Digital Platform Services Inquiry: Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services" ("ACCC Discussion Paper"), February 2022, available at https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry.pdf, page 4.

acting as gatekeepers between businesses and consumers. CAF believes that it is not. We thus urge regulators across the world to take decisive action to harness the power of digital gatekeepers, in order to unlock competition and increase choice for consumers.

In this submission, CAF will provide its observations in response to the questions posed by the ACCC that are most relevant for its members' activities. In doing so, CAF's response will focus on the app economy, whereby Apple and Google – having an effective duopoly over mobile ecosystems, and controlling the iOS and Android operating systems and the App Store and Play Store, respectively – are able to dictate the rules of the game, harming app developers and their users. CAF's submission will mostly focus on Apple, but CAF's observations equally apply to Google to the extent that its practices (increasingly) resemble those of Apple.

II. Response to question 1 of the ACCC consultation

The ACCC asks stakeholders to identify the competition and consumer harms, as well as the key benefits, that arise from digital platform services in Australia.

In the app economy, Apple and Google have significant market power in their respective mobile ecosystems: they control the supply of the two main mobile operating systems (iOS and Android, respectively), as well as mobile app distribution (through their operation of the App Store and the Play Store).[6] Competition within and between Apple's and Google's mobile ecosystems is limited.[7] Consequently, Apple and Google "occupy key positions for businesses seeking to reach Australian consumers, and accordingly could be seen to act as 'gatekeepers'."[8] As the ACCC rightly states, "this gatekeeper status enables platforms to control businesses' access to end consumers, and effectively confers on them rule-making authority."[9]

While app marketplaces allow consumers to have access in a centralized manner to a variety of apps, the way Apple and Google operate their app stores – not least because of the gatekeeper role they have on mobile app distribution – has led to significant competition and consumer harms. CAF generally agrees with the findings of the ACCC set out in Chapter 5 of the Discussion Paper with regards to harms to competition and consumers arising from digital platform services, as well as the findings of the ACCC's interim report on app marketplaces.[10]

6 Id., page 16.

7 This has been concluded by the UK Competition and Markets Authority ("CMA") in its Interim Report on the mobile ecosystems market study: CMA, "Mobile ecosystems market study interim report", 14 December 2021, available at https://www.gov.uk/government/publications/mobile-ecosystems-market-study-interim-report.

8 ACCC Discussion Paper, page 23.

9 Ibid.

10 See ACCC, "Digital platform services inquiry, Interim report No. 2 – App marketplaces", March 2021, available at https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202021%20interim%20report.pdf.

The harms arising from Apple's and Google's conducts in relation to their app stores (and operating systems) are well-documented, both by competition authorities in Australia and around the world and by researchers and think tanks. Thus, in this submission, CAF will not go into detail in explaining such harms, instead providing an overview. **Section A** refers to harms arising from the imposition of unfair and abusive terms on app developers. **Section B** touches upon the harms arising from the collection and use of commercially sensitive information. **Section C** refers to the harms arising from the erratic app review process. **Section D** addresses the harms resulting from Apple's and Google's self-preferencing practices, and finally, **Section E** refers to harms arising from the limitations placed on access to technology and functionalities.

A. Harms arising from the imposition of unfair and abusive terms on app developers

The gatekeeper role Apple and Google have over app distribution allows them to "unilaterally set, amend, interpret and enforce the terms and conditions that app developers must follow to reach consumers."[11] App developers have no other choice but to accept Apple's and Google's terms, no matter how unfair or harmful they may be – or else they will lose access to their mobile user base. In this Section, we refer to the harms arising from (i) the mandatory use of Apple's proprietary in-app payment system, In-App Purchase ("IAP"), and (ii) the anti-steering rules Apple imposes on app developers whose apps offer "digital" goods or services. As stated above, while CAF focuses on Apple, the following observations would also apply to Google, to the extent that its practices are similar to those of Apple.[12]

1. The mandatory use of IAP

For app developers whose apps are deemed to offer "digital" goods or services (Apple being the sole arbiter of deciding when this is the case),[13] Apple has tied access to the App Store to the use of IAP. The obligation to exclusively use IAP results in a variety of harms to competition and consumers.

11 ACCC Discussion Paper, page 24.

12 While Google had historically been more lenient about the use of its proprietary in-app payment system, Google Play's billing system ("GPB"), in September 2020, Google announced that all developers selling digital goods or services in their apps will be required to exclusively use GPB by 30 September 2021. Google later announced that app developers could apply for an extension in the deadline for compliance with the GPB obligation until 31 March 2022. See Sameer Samat, "Listening to Developer Feedback to Improve Google Play", 28 September 2020, available at https://android-developers.googleblog.com/2020/09/listening-to-developer-feedback-to.html; Purnima Kochikar, "Allowing developers to apply for more time to comply with Play Payments Policy", *Android Developers Blog*, 16 July 2021, available at https://android-developers.googleblog.com/2021/07/apply-more-time-play-payments-policy.html. In India, the latest compliance date has been extended to 31 October 2022.

13 Apple has discretion in deciding whether an app enables the purchase of "digital" goods or services and should thus use IAP or whether it enables the purchase of "physical" goods or services and thus should not use IAP. The distinction it draws is not always objective or logically founded, and it is difficult to understand why it considers some services as being consumed "within the app" while similar services are considered to be consumed "outside of the app". Note that within the category of apps deemed to offer "digital" goods or services, Apple has made over the years various exceptions to the obligation to use IAP (some of which were applied *ad hoc*, without being included in the App Store Review Guidelines).

App developers cannot choose the payment processor of their choice. App developers whose apps sell "digital" goods or services are prohibited from choosing an alternative service provider to process in-app payments, having to use the "one-size-fits-all" IAP. Users are ultimately the losers, as app developers cannot offer flexible payment options and features valued by users (e.g., carrier billing, subscriptions with different billing cycles, targeted discounts, ability to pay in instalments). In addition, the obligation to use IAP limits competition among and innovation from payment service providers, which would otherwise have a strong incentive to innovate in payment solutions specifically designed for in-app payments.[14]

App developers are disintermediated from their users. When IAP is used, Apple confiscates the customer relationship and forcibly interposes itself between the app developer and its users.[15] The app developer cannot provide customer support on crucial billing issues such as cancellations and refunds, which must be handled by Apple. This artificial separation between the provision of the service (which is the app developer's responsibility) and the provision of customer care services (which are handled by Apple) leads to unnecessary frictions in customer service processes (e.g., the handling of cancellations of subscriptions or refund requests). Not only are users harmed (as they are confronted with a chaotic, inefficient and sub-par customer service), but also app developers' reputation is harmed, as consumers inevitably associate the poor user experience they receive with the developer's brand.[16]

In addition, through the use of IAP, Apple obtains access to commercially sensitive information about subscribers of third-party app developers (e.g., the user's full name, email, age, IP address, location, as well as credit card details and billing information), which it does not share with the app developer providing the service.[17] Consequently, app developers are deprived from valuable user data, which they could use to improve their services, personalize their offering and protect their users (e.g., from fraud) – while Apple collects unparalleled market intelligence.[18]

IAP raises the costs of app developers offering "digital" goods or services. For transactions made through IAP, app developers have to pay an (up to) 30% commission on the transaction value. The ACCC found that it is "highly likely" that such a commission is "inflated by [Apple's] market

14 On the harmful effects of the mandatory use of IAP on innovation see also Coalition for App Fairness ("CAF"), "How Apple's App Store practices are killing innovation", available at https://appfairness.org/wp-content/uploads/2021/05/caf-stifling-innovation.pdf, page 3.

15 For a detailed discussion on how Apple disintermediates app developers from their users when IAP is used, as well as the harmful effects of this, see CAF, "Apple's In-App Purchase ("IAP") as a disintermediation tool", available at https://appfairness.org/wp-content/uploads/2021/05/CAF-IAP-as-DisintermediationTool.pdf.

16 See Id., pages 3-5.

17 Apple only shares limited information with app developers: when a transaction is made through IAP, the app developer receives a real-time notification that a purchase has been made for a specific product offered by the app developer. While the notification provides information about the purchased product, it does not contain information that would enable the app developer to identify the user with certainty, or information such as the amount paid or the currency used. See Id., page 2.

18 See Id., page 3.

power."[19] In fact, the (up to) 30% commission does not reflect the value of the app store; it is a supra-competitive commission that can only be imposed by Apple because of the market power it has over app distribution. In this regard, Judge Gonzalez Rogers noted that Apple set its commission at 30% in an arbitrary manner, without regard to operational costs, benefits for users or developers.[20] The commission has no relationship to the costs of running the App Store or the value offered to app developers, but was a historic gamble that simply allowed Apple to reap supra-competitive margins.[21]

Apple's own apps do not incur such charges – nor do app developers whose apps are deemed to offer "physical" goods or services which are not subject to the IAP obligation. The commission is therefore structured in an unfair and discriminatory manner.[22] This commission eats into the margins of app developers and raises the costs for Apple's rival apps, thus distorting downstream competition. In the long term, this can have significant effects on consumer welfare, either because downstream markets are foreclosed or because app developers have a reduced ability and incentive to invest in their apps or develop new, innovative apps, having handed a significant part of their (potential) income to Apple.[23]

IAP raises switching costs and contributes to consumer lock-in. The mandatory use of IAP increases switching costs, making it harder for users to switch to an Android device. Apple does not allow app developers to require users to link their account with their Apple ID, meaning that users who have purchased a subscription through IAP are not able to access their purchased content after switching to an Android device (instead having to repurchase or re-subscribe). Even if users can access purchased content, they cannot manage (e.g., cancel) pre-existing subscriptions after switching to a device with a different operating system. Therefore, users have to cancel their subscriptions before switching, which may be problematic for consumers as they may have multiple subscriptions with different billing cycles.

In fact, Apple has long perceived the mandatory use of IAP as a way to lock customers in its ecosystem: internal emails uncovered in the context of the Apple eBook litigation in the United States confirm that, in 2010, when Apple executives became aware of an Amazon Kindle ad on TV

19 ACCC Discussion Paper, page 42.

20 *Epic Games, Inc. v. Apple Inc.*, Rule 52 Order after trial on the merits, available at https://cand.uscourts.gov/wp-content/uploads/cases-of-interest/epic-games-v-apple/Epic-v.-Apple-20-cv-05640-YGR-Dkt-812-Order.pdf, page 144.

21 See Id., pages 35, 92, 98 and 114.

22 On this point, see also Adi Robertson, "Tim Cook faces harsh questions about the App Store from judge in Fortnite trial", *The Verge*, 21 May 2021, available at https://www.theverge.com/2021/5/21/22448023/epic-apple-fortnite-antitrust-lawsuit-judge-tim-cook-app-store-questions.

23 For a broader discussion how the IAP commission may stifle innovation see CAF, "How Apple's App Store practices are killing innovation", available at https://appfairness.org/wp-content/uploads/2021/05/caf-stifling-innovation.pdf, page 2.

showing that it was easy for users to switch from iPhone to Android, Steve Jobs suggested that "[t]he first step might be to say they [Amazon] must use our payment system for everything."[24]

2. The anti-steering rules

Apple prevents app developers whose apps offer "digital" goods or services from directly communicating with their users about purchasing channels other than IAP.[25] The anti-steering rules aim at reinforcing the obligation to use IAP and safeguarding the related commission. The scope of Apple's anti-steering rules has changed over time: at first, it was ever-expanding, but recently it has been narrowed down, most likely due to the growing regulatory pressure Apple has been subject to. Their interpretation by Apple has also often been unpredictable.

The anti-steering rules harm app developers, which live in fear that Apple may suddenly change the wording or interpret them in a novel manner and reject an update of their app or remove it from the App Store. They also harm users, as they limit their ability to make informed choices between the various purchasing channels, missing out on (often cheaper) out-of-app alternatives.

B. Harms arising from the collection and use of commercially sensitive information

Because of its position as the operator of the App Store (the only app distribution channel available on iOS) and as the provider of the iOS operating system, Apple has access to a variety of commercially sensitive information. In fact, Apple has contractually built a framework whereby, on the basis of the Apple Developer Program License Agreement (which all app developers must sign in order to distribute their apps through the App Store) and the MFi program (which companies that want their hardware accessories to connect electronically to Apple devices must sign – and which may also be app developers), Apple can obtain and use sensitive information collected from app developers.[26]

In addition, Apple obtains sensitive commercial data from all apps obliged to use IAP, such as their customer lists, the purchasing activity of individual users and the success of subscriptions. Apple gains market intelligence, which it can use to scan the horizon and identify app categories with revenue growth opportunities. Apple can then swiftly develop its own apps and enter the services market, competing with app developers whose data played an instrumental role in Apple's ability to do so. While Apple may claim that its app development team does not have access to data collected from other lines of business, former Apple executive Philip Shoemaker has explained that

24 Email exchange forming part of the public record in the Apple eBook litigation in the United States.

25 See App Store Review Guidelines, available at https://developer.apple.com/app-store/review/guidelines/#payments, Article 3.1.1.

26 See in this regard, ACCC Discussion Paper, page 41.

Apple executives would frequently use insights based on App Store data to inform product development.[27]

The fear of Apple using commercially sensitive information about third-party apps, services and/or products for its own purposes, reduces the incentives of app developers to innovate, since they know that if they are successful, Apple may appropriate their innovation and then target them through exclusionary practices.

C. Harms arising from Apple's erratic app review process

In order for an app (and each subsequent update of the app) to be available on the App Store, it must first be approved by Apple during the app review process. The app review process (during which Apple assesses compliance of the app or update with its unilaterally imposed App Store Review Guidelines),[28] affords Apple unique power over app developers wishing to reach mobile users. While a review process may generally be useful in ensuring the quality and security of apps, what is problematic is that Apple has unfettered discretion in interpreting and applying its rules and carrying out the app review process. As Apple's App Store Review Guidelines put it:

> "We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it."[29]

Apple is the judge, jury and executioner, meaning that it has the leeway to apply its rules in an arbitrary and capricious manner. App developers cannot know in advance how Apple will interpret the rules each time, having to operate their business in uncertainty. At the same time, Apple often only provides cryptic feedback to app developers about the reasons for the rejection of their apps or updates, leaving them wondering what they need do to for their apps to be compliant with Apple's rules.

CAF's members have had their fair share of trouble because of the capricious and inconsistently applied rules. For example, as CAF explained in one of its papers,[30] Apple suddenly changed its approach towards screen time and parental control apps, removing or restricting leading apps from the App Store, once it announced the launch of "Screen Time", a feature that would help people limit the time they and their children spend on the iPhone. This unilateral action exposed millions of children and undermined millions of parents. Similar issues were faced by FlickType, which

27 Reed Albergotti, "How Apple uses its App Store to copy the best ideas", *The Washington Post*, 5 September 2019, available at https://www.washingtonpost.com/technology/2019/09/05/how-apple-uses-its-app-store-copy-best-ideas/.

28 See https://developer.apple.com/app-store/review/guidelines/.

29 App Store Review Guidelines, "Introduction", available at https://developer.apple.com/app-store/review/guidelines/.

30 CAF, "How Apple's App Store practices are stifling innovation", available at https://appfairness.org/wp-content/uploads/2021/05/caf-stifling-innovation.pdf, pages 4-5.

saw an update of its app being rejected, even though previous versions of the app were approved by Apple, and so were other apps offering a similar service. Basecamp has also had a turbulent experience with the app review process following the launch of the HEY email app.[31]

Former Apple executives have acknowledged that Apple applies its rules in an arbitrary and inconsistent manner, as explained in the report of the U.S. House Judiciary Antitrust Subcommittee:

> "Mr. Shoemaker responded that Apple "was not being honest" when it claims it treats every developer the same. Mr. Shoemaker has also written that the App Store rules were often "arbitrary" and "arguable," and that "Apple has struggled with using the App Store as a weapon against competitors.""[32]

As the ACCC rightly points out in its Discussion Paper, the arbitrary application of rules without adequate explanation causes considerable uncertainty, costs and delays for app developers. Ultimately, it is consumers who suffer, as app developers are delayed in rolling out new features that improve the quality and security of their services or are even discouraged from innovating in the first place.[33]

Worse, app developers that disagree with Apple's decisions have no effective redress. What they can do is to file an appeal before the App Review Board. Even in this case, however, it is Apple employees (typically more experienced reviewers) that will decide on the final outcome and, as will be explained further below, the appeal process in itself also lacks transparency.[34]

D. Harm arising from Apple's self-preferencing practices

Apple is vertically integrated, meaning that it does not only control the iOS operating system and the App Store, but it also competes downstream with app developers that make their apps available through the App Store. As the ACCC correctly points out, "[v]ertical integration may create conflicts of interest where a vertically integrated firm is acting to advantage the interests of its other

31 See David Pierce, "A new email startup says Apple's shaking it down for a cut of its subscriptions", *Protocol*, 16 June 2020, available at https://www.protocol.com/hey-email-app-store-rejection

32 Majority Staff Report and Recommendations, Investigation of Competition in Digital Markets, 2020, available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf, page 371.

33 See ACCC Discussion Paper, pages 54-55. See also CAF, "How Apple's App Store practices are stifling innovation", available at https://appfairness.org/wp-content/uploads/2021/05/caf-stifling-innovation.pdf, page 5.

34 See App Store Review Guidelines, "After You Submit", available at https://developer.apple.com/app-store/review/guidelines/#after-you-submit: "Rejections: Our goal is to apply these guidelines fairly and consistently, but nobody's perfect. If your app has been rejected and you have questions or would like to provide additional information, please use App Store Connect to communicate directly with the App Review team. This may help get your app on the store, and it can help us improve the App Review process or identify a need for clarity in our policies. If you still disagree with the outcome, or would like to suggest a change to the guideline itself, please submit an appeal."; See also https://developer.apple.com/app-store/review/.

businesses over those of its customers."[35] Apple can therefore engage in anti-competitive self-preferencing to favour its own apps over rival third-party apps, preventing competition on the merits and harming third-party app developers which are reliant on the App Store to reach their user base.

For example, as the ACCC identified, Apple can "provide greater discoverability to [its] own apps in [its] app [marketplace], implement and enforce favourable pre-installation and default settings, and withhold or limit third-party access to device functionality."[36] Among the app developers that have felt the impact of Apple's self-preferencing practices are those offering digital well-being and parental control apps. For instance, Apple restricts parental control app developers from accessing the full suite of controls available within its operating system and app marketplace, hindering parents' efforts to monitor and protect their children and risking children's wellbeing.[37]

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

Overall, such conduct undermines the ability of app developers to compete, innovate and solve issues of concern to consumers.

E. Harms arising from Apple's restrictions on access to technology and functionalities

As the Discussion Paper points out, "[t]he ACCC is also aware of concerns from app developers regarding Apple delaying or denying access to certain functionality for third-party apps."[39] The ACCC refers to the limited access granted by Apple to the ultra-wideband short-range proximity tracking and data transfer technology present in iPhones, which may reduce future innovation and limit the future products made available to consumers.[40] By delaying or restricting third-party access to useful hardware or software features, such as APIs or chips (like the near-field

35 ACCC Discussion Paper, page 29.

36 Id., page 40.

37 Apple has also made other deliberate choices harming app developers offering parental control apps, while protecting its own ecosystem. For example, Apple allows children over 13 years of age to remove parental controls without parental notice or intervention. In addition, in 2020 with the launch of iOS 14, Apple introduced a Private MAC functionality that blinded school filtering and home parental control tools, affecting the safety of millions of children globally.

38 See Reed Albergotti, "Apple Says Recent Changes to Operating System Improve User Privacy, But Some Lawmakers See Them As An Effort To Edge Out Its Rivals", *The Washington Post*, 26 November 2019, available at https://www.washingtonpost.com/technology/2019/11/26/apple-emphasizes-user-privacy-lawmakers-see-it-an-effort-edge-out-its-rivals/.

39 ACCC Discussion Paper, page 42.

40 Ibid.

communication ("NFC") chip or the ultra-wideband ("UWB") chip), Apple can give itself a competitive advantage over rivals, harming competition and restricting consumer choice.

Another example is how Apple limits access to features within its Mobile Device Management ("MDM") technology, a technology which allows the remote control and configuration of devices. For example, with MDM, an app developer can push to a device settings which apply content filters, determine what features and apps can be accessed and limit access to networks and VPNs. On the Apple platform, the full suite of MDM features is available through a configuration called "Supervision". Apple does not allow consumer app developers to access Supervision. As a result, consumer app developers are not able to access measures such as (i) ensuring that the end user cannot remove or subvert the MDM settings, (ii) restricting end users from accessing risky messaging services such as iMessage and explicit iTunes content or (iii) restricting end users from accessing risky device features such as the camera or screen capture. This undermines the ability of consumer app developers to compete and innovate, harming children as a result.

III. Response to question 2 of the ACCC consultation

The ACCC seeks views on whether competition laws are sufficient to address harms arising from digital platform services or whether regulatory reform is required to effectively deal with such harms. CAF strongly believes that competition law is insufficient to address the harmful conduct of digital platforms with a gatekeeping role, such as Apple and Google which, through the operation of the App Store and the Play Store, respectively, control app distribution on iOS and Android devices.

Over the last years there has been growing global consensus that competition law alone is not sufficient to deal with the competitive harms arising in digital markets. As the ACCC correctly identifies, "despite [the] enforcement efforts [against digital gatekeepers] in Australia and overseas, there has not been a noticeable change in market dynamics and similar [anti-competitive] conduct continues to emerge across these and related digital platform markets."[41]

The shortcomings of competition law enforcement are well-reported: First, competition law investigations and court proceedings take time and are retrospective in effect (i.e., they address competition and consumer harms that have already occurred).[42] Because of the very nature of fast-paced digital markets, which are prone to tipping and are characterized by winner-takes-all dynamics, by the time an investigation is concluded, the harm caused by the anti-competitive conduct of a large digital platform may already be irreversible. Second, competition law can only remedy conduct that falls within the specific scope of the law. This means that harmful conduct may remain unpunished if the requirements set out in competition laws are not satisfied, and this risk is exacerbated by the fact that many of the competitive harms arising in dynamic digital

41 Id., page 61.

42 See Id., page 63.

markets may be novel and not fall within the traditional remit of competition rules.[43] Third, the remedies available under the existing competition framework may be insufficient to "address the underlying cause of the problems in relation to digital platform services, […] particularly where harm is caused by a lack of competition, or where a market has already tipped in favour of one platform, and where there is a likelihood of harm to competition in many related markets."[44] Finally, "it is difficult to impose one-off penalties of a scale necessary to deter very large global digital platforms from engaging in similar conduct in the future and encourage a change in behaviour."[45] Indeed, competition law remedies are narrow and fines do not always have a deterrent effect, as digital gatekeepers have significant financial resources.

CAF, therefore, agrees with the ACCC's discussion in section 6.2.1 of the Discussion Paper and considers that regulatory reform, as pursued for example in the European Union ("EU") with the Digital Markets Act ("DMA"), is required to ensure that business users of gatekeeping digital platforms, including app developers which rely on the App Store and the Play Store to reach end users, as well as consumers are not harmed by the gatekeepers' anti-competitive conducts.

IV. Response to question 3 of the ACCC consultation

The ACCC is considering whether law reform should be staged to address specific harms sequentially as they are identified and assessed, or it should comprise a broader framework that would address multiple potential harms across different digital platform services.

While there is merit in each approach (and different approaches have been followed in various jurisdictions), CAF believes that the adoption of a broader regulatory framework would be preferable, because many of the issues and harms faced by business users of digital platforms as well as consumers are systemic in nature. It is, therefore, preferable to put in place a comprehensive regulatory framework dealing with the conduct of platforms that have become indispensable gateways between businesses and consumers. In this regard, CAF agrees with the ACCC that "given the wide range of competition and consumer issues in relation to digital platform services, a broader framework may ensure the full range of concerns, as well as future changes in relation to these dynamic services, can be addressed. In particular, a broader framework could potentially address systemic issues which can manifest in various ways across digital platforms' ecosystems."[46]

CAF notes, however, that the adoption of a broader framework does not prevent from the outset the adoption of tailored rules: it would be possible to allow for the tailoring of the regulatory framework to a specific digital platform, to the extent necessary and appropriate, to ensure that interventions are targeted and flexible.

43 Ibid.

44 Id., page 64.

45 Ibid.

46 Id., page 74.

V. Response to question 4 of the ACCC consultation

The ACCC's fourth question inquires into the benefits, risks, costs and other considerations (such as proportionality, flexibility, adaptability, certainty, procedural fairness, and potential impact on incentives for investment and innovation) that are relevant to the application of the various regulatory tools considered by the ACCC to address competition and consumer harms arising from digital platform services in Australia. In this Part, CAF will provide its comments on the tools that could be used to address the concerns of its members.

CAF would like to make two preliminary remarks. First, CAF notes that a factor that should be considered in deciding on the regulatory approach to follow is the speed in which the relevant regulatory tool(s) can be adopted and be operational. Given the significant harms to businesses and consumers that have already been caused by the conduct of digital gatekeepers, it is imperative that any regulatory intervention is timely.

Second, CAF notes that, regardless of the approach to be ultimately followed, particular weight should be given to enforcement. If gatekeepers are able to escape the rules, then the harms arising from their conduct will only persist. The example of Apple and its non-compliance with the order of the Netherlands Authority for Consumers and Markets ("ACM") is representative of this concern. Apple first tried to delay the implementation of the ACM's order, and after exhausting every legal mechanism available to it, it chose to not change its practices, instead preferring to pay a €5 million weekly fine for non-compliance.[47] The ACCC, therefore, should pay particular attention to the issue of enforcement: any approach chosen should be accompanied by an effective implementation and enforcement regime, which will encompass strong sanctions, effective in constraining the gatekeepers' harmful conduct. In this regard, it is of utmost importance that the enforcer be granted sufficient (human and financial) resources to monitor, implement and enforce the rules.

A. Prohibitions and obligations contained in legislation

One of the possible regulatory approaches considered by the ACCC in the Discussion Paper is the adoption of prohibitions and obligations contained in legislation. That is the approach of the EU, which is in the process of adopting the DMA, an *ex ante* regulatory regime for digital platforms acting as gatekeepers which will ensure the fairness and contestability of digital markets in which such gatekeepers are present.

The main advantage of this approach is that the rules will be clear: once the law is in place, the platforms falling under its scope will have to comply with a predefined list of dos and don'ts. The relevant legislative instrument could contain obligations and prohibitions that would apply to all

47 See, e.g., Natasha Lomas, "Apple hit with sixth antitrust fine over Dutch dating apps payments", *TechCrunch*, 28 February 2022, available at https://techcrunch.com/2022/02/28/apple-sixth-acm-fine/; Foo Yun Chee, "EXCLUSIVE Apple has not fully complied with order to open up App Store -Dutch watchdog", *Reuters*, 25 March 2022, available at https://www reuters.com/technology/exclusive-apple-has-not-fully-complied-with-order-open-up-app-store-acm-2022-03-25/.

digital platforms falling under its scope and/or could include obligations that would apply to certain sub-categories of digital platforms (e.g., app stores), or even prescribe different rules to different business models. As to the ACCC's concern about whether a legislative instrument would be "sufficiently flexible to remain relevant and effective in response to changes in digital platforms' business models or operations, and the broader innovations in digital services,"[48] it should be noted that, to the extent new practices or business models are not captured by the adopted legislation, nothing would prevent the adoption of additional rules or the combination of an *ex ante* regulatory instrument with another regulatory approach that would be more future-proof (e.g., giving the power to the regulator to adapt the rules to new developments).

CAF believes that the legislative instrument should contain at least the following obligations and prohibitions that are necessary to address the competition and consumer harms arising from the practices of Apple and Google as operators of their respective app stores and providers of the iOS and Android operating systems. These obligations and prohibitions reflect CAF's "App Store Principles", which aim to ensure that app developers can compete in a fair environment:[49]

- ***Obligation to allow the use of alternative app distribution channels.*** App developers should be free to decide how to distribute their apps to users, be it through any app store they prefer and/or through direct downloads from their websites. This obligation would entail that Apple should allow third-party app stores to its devices. In this regard, it should be noted that Apple is expected to oppose such an obligation by invoking the "security" defence – as it has already done time and again.[50] As CAF has, however, already explained in one of its papers,[51] Apple's security claims are largely overblown. The security and integrity of an iPhone device can be ensured even if the App Store is not the exclusive app distribution channel, as device security comes from security measures (e.g., encryption of data, firewall, antivirus) and sandboxing (which restricts apps from accessing content on other apps or the system) which are not dependent on the app distribution method – instead, they are built into the hardware or the operating system. If such features are not deemed to be sufficient, an additional security layer (e.g., human review) could be used – this also regardless of the app distribution method.

48 ACCC Discussion Paper, page 75.

49 See https://appfairness.org/our-vision/.

50 See, for example, Building a Trusted Ecosystem for Millions of Apps – a threat analysis of sideloading, Apple, October 2021, available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf; See also Chance Miller, "Craig Federighi vehemently speaks out against iPhone sideloading in Web Summit keynote: 'Sideloading is a cybercriminal's best friend'", *9to5Mac*, 3 November 2021, available at https://9to5mac.com/2021/11/03/craig-federighi-keynote-side-loading-speech/.

51 See CAF, "Should iOS users be allowed to download apps through direct downloads or third-party app stores?", available at https://appfairness.org/wp-content/uploads/2021/12/iOS_Users_and_Third_Party_App-Stores.pdf. See also "Reality check: Debunking Apple's false security claims", available at https://appfairness.org/wp-content/uploads/2021/07/Apples-False-Security-Claims-1.pdf.

- ***Prohibition of mandating the use of ancillary services (e.g., in-app payment systems) offered by Apple or Google.*** Apple and Google should not be allowed to impose the mandatory use of IAP and GPB on (certain categories of) app developers. All app developers should be free to choose the ancillary services they wish to offer to their users. This will address the harms suffered by app developers subject to the mandatory use of IAP and GPB and will lead to greater consumer choice and greater competition among ancillary service providers.

- ***Obligation to allow app developers to communicate directly with their users for legitimate business purposes.*** As explained above, the restrictions placed on app developers' communications with their users prevent them from informing users about (perhaps cheaper) out-of-app purchasing possibilities. This is detrimental for consumers. It would thus be a clear consumer benefit if app developers could engage freely in in-app and out-of-app communications with their users.

- ***Obligation to provide timely access to the same interoperability interfaces and technical information made available to Apple's and Google's own apps.*** For example, legislation could require Apple and Google to give third-party apps comparable and timely access to device hardware or operating system features (e.g., the NFC or UWB chip) as the digital platform's own first-party apps.

- ***Prohibition of the use of app developers' data by app store providers to compete with the app developer.*** This obligation could also more broadly prohibit app store operators from unreasonably sharing information from one part of their business to their app development business.

- ***Obligation to allow access to the app store and operating system features on fair, objective, reasonable and non-discriminatory terms.*** This obligation would level the playing field between all app developers, preventing Apple from applying different rules on different categories of app developers or cutting special deals with certain very large app developers.[52]

- ***Prohibition placed on app store and/or operating system providers from engaging in self-preferencing of their own apps or services or interfering with users' choice of preferences or defaults.*** This should comprise an obligation to allow users to choose the default settings, e.g., through the surfacing of choice screens.

52 For example, it has been reported that Apple cut a deal with Amazon in 2016 on the basis of which Apple would only charge a 15% fee on subscriptions purchased through the app, compared to the standard 30% fee that most developers must pay for IAP transactions. See Kim Lyons, "Documents show Apple gave Amazon special treatment to get Prime Video into App Store", *The Verge*, 30 July 2020, available at https://www.theverge.com/2020/7/30/21348108/apple-amazon-prime-video-app-store-special-treatment-fee-subscriptions.

- ***Obligation to allow the uninstallation of any pre-installed apps.*** The pre-installation of Apple's and Google's apps on iOS and Android devices gives them a competitive advantage over rival apps, given that consumers tend to stick to the pre-installed apps, rather than search for and install a similar third-party app. Worse, Apple does not allow the uninstallation of certain apps that come pre-installed on its iPhone. Such practices have harmful effects on competition and consumers and should therefore be prohibited by law. Given that Apple is expected to fight such a rule, invoking user "security" or "integrity" of the device, it is crucial that any limitations to such an obligation are strictly necessary, objective, proportional and duly justified.

- ***Obligation to implement a fair, transparent and non-discriminatory app review process.*** Such an obligation is important for both third-party apps that compete with Apple's and Google's own apps and in general for all app developers that distribute apps through the App Store and the Play Store.

- ***Obligation to be transparent about the rules and policies applicable to the app stores.*** App store providers should, for example, provide advance notice of changes and make available a quick and fair dispute resolution process.

B. <u>The development of codes of practice</u>

Another option considered by the ACCC is the adoption of codes of practice that would establish clear standards of acceptable conduct. Codes could potentially apply to a specific service offered by a digital platform or to one or more of their services. One of the key benefits of codes of conduct is their flexibility, as they can be tailored to suit different circumstances and issues and they can be more easily adapted as circumstances change (compared to prohibitions or obligations contained in legislation, for example).[53]

This approach is followed in the United Kingdom ("UK"), where a new regulatory regime for the most powerful digital firms, overseen by the Digital Markets Unit ("DMU"), will be centered around the adoption of a code of conduct for each firm found to have "Strategic Market Status" ("SMS") in a digital activity.

CAF believes that such a regulatory approach could work well, as it can be flexible and tailored to the specificities of each gatekeeping platform. However, it may be time-consuming to set up multiple codes of conduct and the process can also be prone to abuse by gatekeepers, which may seek to delay the adoption of the code that will be applicable to them. Therefore, if a regulatory approach relying on the adoption of codes of conduct is opted for, it is necessary to ensure that adoption will be timely and a mechanism will be put in place to deal with cases whereby a gatekeeper disrupts the process. In addition, it is of utmost importance that codes of conduct be mandatory and accompanied by strict and effective sanctions which will ensure that gatekeepers have an incentive to comply.

53 ACCC Discussion Paper, page 75.

Should the codes of practice approach be pursued, CAF believes that the same substantive obligations as those detailed in Section A above should be included in the codes that will apply to Apple and Google.

C. The conferral of rule-making powers on a regulatory authority

A further option considered in the Discussion Paper is to adopt legislation that would "provide the ACCC or another authority with the powers to develop and implement rules to achieve overarching objectives or principles contained in the legislation."[54] Such an approach could work, but it is of utmost importance that the enabling legislation (which will grant powers to the authority to develop and implement the rules that will bind digital gatekeepers) be adopted in a timely manner.

D. The introduction of pro-competition or pro-consumer measures following a finding of a competitive or consumer harm

A further option considered by the ACCC is the adoption of "a provision that would allow a pro-competition or pro-consumer measure to be put in place or imposed on a particular platform or set of platforms, following a finding of a competitive or consumer harm. Measures implemented in such a way could work together with any of the other approaches identified in this chapter."[55] Pro-competitive interventions are an element of the UK DMU regime complementing the adoption of codes of conduct. CAF believes that the possibility of adoption of such pro-competition interventions would be a significant element of the toolbox available to the regulator and an important complement to other regulatory tools.

VI. Response to question 5 of the ACCC consultation

The fifth question of the consultation seeks views on the extent to which a new regulatory framework in Australia should be aligned with those in overseas jurisdictions to promote regulatory alignment for global digital platforms and their users.

CAF believes that regulatory alignment makes sense, as many of the products and services offered by gatekeepers – as well as the harmful practices related to the offering of these products and services – are global in nature. Thus, the substantive rules and standard of conduct applicable to gatekeepers should be similar across the world (while enforcement could be tailored to each jurisdiction, provided that it is effective).

In the app economy, the South Korean legislator has already adopted rules regulating the practices of app store providers. In the EU, the DMA will soon be adopted and will impose a number of obligations and prohibitions on app store providers (along the lines as those described in Section A above). Therefore, if Australia decides to regulate the conduct of digital gatekeepers (which CAF

54 Id., page 77.

55 Id., page 78.

believes it should), it should seek to ensure convergence (at least at the substantive level) with EU rules, as well as rules that have already been adopted in other jurisdictions.

VII. Response to questions 6 and 7 of the ACCC consultation

The ACCC is considering to what digital platform services other than ad tech and general search services regulation to prevent anti-competitive conduct should apply, as well as which platforms should be captured by an *ex ante* regulatory regime.

CAF firmly believes that it is necessary to adopt a regulatory framework that will also cover app marketplaces. Apple and Google have gatekeeper power over app distribution on iOS and Android, respectively, which allows them to impose unfair terms and conditions on app developers and adopt abusive conducts. In addition, regulation should also address practices adopted by Apple and Google as the providers of the iOS and Android operating systems, which, alongside app store-related anticompetitive policies and conducts, further harm app developers and their users. After all, it is the effective duopoly Apple and Google have over mobile ecosystems that allows them to engage in a variety of conducts that harm consumers, competition and innovation.[56]

As to the question of what platforms should fall under the scope of a regulatory regime, CAF believes that *ex ante* regulation should apply asymmetrically – i.e., only capture these digital platforms that have a gatekeeper role, acting as indispensable gateways between businesses and consumers. It is this gatekeeper role that allows such platforms to adopt conducts that harm businesses and consumers. In addition, from an enforcement perspective, it is better to focus on a few companies whose practices harm competition and consumers rather than seek to regulate a large number of companies. As enforcement resources will inevitably be limited, it should be ensured that they are sufficient to address the practices of the companies whose conducts have the largest impact on the market.

Gatekeeper platforms could be designated on the basis of quantitative or qualitative criteria or, ideally, a combination of both. For example, the DMA proposal sets out a presumption that a digital platform is a gatekeeper if certain quantitative thresholds are met. However, the gatekeeper can rebut this presumption by arguing that, although it meets the quantitative thresholds, it is not a gatekeeper because of qualitative factors. In addition, according to the DMA proposal, it will be possible for a firm that does not meet the quantitative thresholds to be designated as a gatekeeper on the basis of a qualitative assessment, if it is considered that the firm acts as an unavoidable gateway between businesses and end users, it has an entrenched and durable position and a significant impact on the EU internal market.[57]

56 See CMA, "Mobile ecosystems market study interim report", 14 December 2021, available at https://www.gov.uk/government/publications/mobile-ecosystems-market-study-interim-report, paragraph 35.

57 See European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM(2020) 842 final, Article 3.

VIII. Response to questions 9 and 10 of the ACCC consultation

The ACCC is considering introducing measures that would limit data use in the supply of digital platform services in Australia.[58] CAF strongly supports the adoption of measures that would prohibit Apple and Google from using data they have received because of their role as the operators of their respective app stores, the mandatory use of their in-app payment systems, as well as the indispensable role of their devices to third-parties that need their products or services to connect electronically to these devices. As the ACCC rightly states, introducing measures to limit data use is a way of addressing the data advantages of some digital platforms, improving competition in the supply of some digital platform services and minimizing the potential for data-related self-preferencing that may enable some digital platforms to obtain a competitive advantage by accessing sensitive datasets in relation to their rivals.[59]

In relation to the operation of the app stores, CAF believes that it is necessary to separate the operation of the app store from other Apple or Google activities (e.g., their app development business), preventing Apple and Google from using non-public data of app developers to compete with them. CAF, however, recognizes that data separation remedies may pose considerable monitoring difficulties in practice. Thus, some form of operational or functional separation between Apple and Google's app development business and the rest of their activities may be easier to implement in practice.

IX. Response to question 11 of the ACCC consultation

The ACCC is assessing whether and what additional measures are necessary or desirable to adequately protect consumers against (a) the use of dark patterns online, and (b) scams, harmful content, or malicious and exploitative apps.

CAF is generally supportive of measures that would protect consumers against harm arising from the use of dark patterns as well as from scams, harmful content or malicious apps. However, CAF emphasizes the need to ensure that any measures adopted will not allow Apple and Google to engage in conducts, in the name of user security or privacy, that would harm third-party app developers, while leaving themselves unaffected (or even benefitting themselves).

CAF, therefore, believes that consumer protection measures should be clearly set and contain safeguards against abuse by gatekeepers (e.g., require gatekeepers to show that their conduct is strictly necessary, proportional and duly justified). In addition, it should be ensured that the implementation of any pro-consumer measures by gatekeepers would apply equally to third-party

58 The ACCC is also considering measures such as data portability, data interoperability, data sharing and mandatory data access. CAF does not have a specific view on the necessity and desirability of such measures, and thus will not address these in this submission. Instead, CAF will provide its views as to limitations in data use.

59 See ACCC Discussion Paper, pages 92-93.

services as well as their own services – and not be used by Apple or Google to disadvantage their rivals, while themselves being unaffected by such measures.

X. Response to question 13 of the ACCC consultation

In its thirteenth question, the ACCC is asking whether digital platforms that operate app marketplaces would need to be subject to additional obligations regarding the monitoring of their app marketplaces for malicious or exploitative apps.

Ensuring a high standard of security for app store users is important for CAF's members that rely on app stores to reach their user base. If the quality of app stores is reduced because of the presence of fraudulent apps that harm users, this will have spill-over effects, harming app developers that distribute legitimate apps through app stores.

It is true that the App Store is not the epitome of security, as it counts numerous fraudulent apps. An analysis carried out by *The Washington Post* found that out of "*the 1,000 highest-grossing apps on the App Store, nearly 2 percent are scams […]. And those apps have bilked consumers out of an estimated $48 million during the time they've been on the App Store.*"[60] It may, therefore, perhaps be necessary to take additional measures to ensure the security of app stores. However, it is of utmost importance that any requirements placed on Apple and Google to monitor their app stores for malicious or exploitative apps do not allow them leeway to adopt measures that harm developers of legitimate apps.

Apple has time and again used security and privacy as justifications for anti-competitive conduct, for example to restrict sideloading or alternative app stores on security grounds, while at the same time the App Store does not conform to strict security standards. In fact, it seems that how apps and developers are treated by Apple is heavily dependent on whether they pose a threat to Apple, with Apple having been accused of approving and distributing "scam apps" that target and deceive consumers so long as they do not compete with Apple's own apps.[61] It is, therefore, necessary that sufficient safeguards are put in place to ensure that any additional monitoring that takes place is truly to the benefit of App Store users, and that it is consistently and objectively enforced. Monitoring by an independent, external body will be important in this regard.

XI. Response to question 14 of the ACCC consultation

In its fourteenth question, the ACCC asks stakeholders' views on the types of fair-trading obligations that might be required for digital platform services in Australia. CAF believes that

60 Reed Albergotti and Chris Alcantara, "Apple's tightly controlled App Store is teeming with scams", *The Washington Post*, 6 June 2021, available at https://www.washingtonpost.com/technology/2021/06/06/apple-app-store-scams-fraud/.

61 Nick Statt, "Apple's App Store is hosting multimillion-dollar scams, says this iOS developer", *The Verge*, 8 February 2021, available at https://www.theverge.com/2021/2/8/22272849/apple-app-store-scams-ios-fraud-reviews-ratings-flicktype.

imposing fair trading obligations on digital gatekeepers, including Apple and Google as the operators of the two dominant app stores, is desirable. As rightly put by the ACCC, "[t]he bargaining power imbalance between gatekeeper digital platforms and their business users can lead to business users being charged prohibitive access fees or commissions or being required to accept other unfair or restrictive contractual terms."[62] Fair-trading obligations could, therefore, go a long way towards promoting competition and innovation to the benefit of consumers.

For example, an obligation should be imposed on app store providers to ensure access to their app stores on fair, reasonable and non-discriminatory ("FRAND") terms, as currently envisaged under the DMA. In addition to this "umbrella" obligation, specific fair-trading obligations could also be imposed, such as an obligation imposed on gatekeeper digital platforms to allow communications between businesses (e.g., app developers) and their users or an obligation to allow choice in payment options.

XII. Response to question 15 of the ACCC consultation

Question 15 set out in the Discussion Paper asks whether specific requirements should be imposed on (certain) digital platforms to improve aspects of their processes for resolving disputes with business users and/or consumers, and, if so, what sorts of obligations. This follows from the ACCC's finding that there is "persistent lack of accountability and effective redress for complaints and disputes arising on digital platforms, both for consumers, advertisers, and a range of business users of digital platform services."[63]

CAF agrees with the ACCC that the dispute resolution processes put in place by large digital platforms are not sufficient. For example, when it comes to the App Store, the only avenue for "redress" app developers which do not agree with the outcome of the app review process have is to submit an appeal to the App Review Board. The appeal process is, however, opaque and it is questionable whether it constitutes an effective dispute resolution mechanism: app developers do not have an active role in or real influence over this process, which lacks transparency and is often characterized by lack of communication between the app developer and Apple. In addition, it is Apple employees that carry out this process and have unfettered discretion over the decisions taken on the appeals.

CAF considers that specific requirements should be imposed on gatekeeper digital platforms as to the dispute settlement processes they have in place. Dispute settlement processes should be transparent, timely and efficient. Gatekeepers should clearly set out the rules and procedures to be followed. They should enable the meaningful participation of businesses in the process and allow them to communicate with an identifiable human representative to inquire about the status of this process and to ask for clarifications and explanations as to the process and/or any decisions taken.

62 See ACCC Discussion Paper, pages 98-99.

63 Id., page 100.

In addition, it may be necessary to have an external, independent arbiter to which businesses could have recourse if they believe that a decision taken internally by the gatekeeper is wrong.

*****