Appendix N: potential interventions to promote competition in native app distribution

Introduction

1. This appendix provides further details on our assessment of potential interventions aimed at opening up competition in native app distribution as described in Chapter 8. As described in Chapter 4, Apple and Google each have substantial and entrenched market power in the distribution of native apps within their ecosystems. The App Store has a total monopoly over downloads on iOS devices and the Play Store accounts for over 90% of native app downloads across Android, HMS, and Fire OS devices.

2. In this appendix, we have considered potential interventions to increase the competitive constraints on the App Store and Play Store posed by the two key potential sources of competition in the distribution of native apps: alternative app stores and sideloading. We set out our views on potential interventions to promote another potential source of competitive constraint (web apps) within Chapter 8.

3. In addition to assessing the potential benefits that opening up the App Store and Play Store to greater competition could deliver, we have considered whether the removal of existing restrictions on alternative app distribution models would be an effective remedy. Specifically, we have considered whether removing these restrictions should be complemented by additional interventions and safeguards to enhance their effectiveness whilst minimising any risks associated with opening up native app distribution to greater competition.

4. Given that the nature of alternative app stores and sideloading differ, we have considered their potential effectiveness, including feasibility challenges and technical considerations, separately. However, we have set out a joint assessment of the potential costs and implementation issues, as well as any available safeguards associated with these alternative native app distribution models, given the strong linkages and overlaps.

Options for promoting competition in native app distribution

5. This section sets out our assessment of the potential benefits and likely effectiveness of the two main options for opening up greater competition to the App Store and the Play Store for native app distribution. We do this for alternative app stores first, then for sideloading.

Alternative app stores

6. Requiring Apple to allow alternative app stores on iOS and widening their availability on Android could have the potential to improve competition in the distribution of native apps. Alternative app stores could be made available through sideloading from the web and Apple and Google could be required to allow app stores to be available for download from the App Store and Play Store.

7. Third-party app stores already exist on Android operating systems. In particular, device manufacturers' own app stores are often preinstalled and made available to users on their devices. However, as described in Chapter 4, we found that Google's Play Store only faces a limited constraint from alternative Android app stores including from new entrants.

8. In this section, we set out relevant background and stakeholders' views on the potential benefits that greater competition from alternative app stores could deliver for users and developers. We then provide our assessment of the nature and size of the potential benefits, prior to considering the various factors and design considerations that could influence the effectiveness of any interventions.

Potential benefits

9. Several stakeholders told us that improving access to alternative app stores on mobile operating systems could lead to a range of benefits for users and developers. In this section, we have grouped these benefits into the three following categories: (i) quality-based competition for users (ii) quality-based competition for developers and (iii) price competition.

Quality – user side

10. As described in Chapter 4, app stores enable consumers to search, install and review apps which have been assessed by operators of app stores against a set of policies in relation to quality, security, privacy, and legal requirements.

11. A number of stakeholders, including operators of app stores, expressed support for interventions that would enable alternative app stores to compete more effectively with the App Store and the Play Store and suggested that greater competition could improve outcomes for users, particularly in relation to quality and user experience.

12. For instance:

- Microsoft[1] suggested that improved access to alternative app stores could improve outcomes in relation to security, quality, discoverability and user experience;

- FlickType[2] told us that competing app stores could improve quality of user service and promote innovation in privacy and security features, such as fraud detection; and

- Epic[3] told us that alternative app stores would inject innovation and consumer choice into the mobile ecosystem.

13. However, whilst alternative app stores have the potential to deliver significant benefits through increased competition, certain risks were also raised in relation to promoting alternative app distribution models. In particular, Apple[4] told us that forcing it to allow alternative app stores would increase the risk of malware attacks which would put all users at greater risk. Apple also argued that these interventions would jeopardise its holistic approach to security and remove the competitive differentiation between Apple and Android, taking this valued element of choice away from users.

14. Apple's view on this subject was aligned with that of ACT | The App Association[5] which told us that allowing users to download apps through alternative app stores carries several significant risks and could lead to malicious apps being downloaded and negatively affecting consumer trust in the ecosystem. The risks associated with promoting alternative app distribution models and any potential safeguards to mitigate those risks are addressed in a separate section below.

Quality – developer side

15. The App Store and Play Store currently enable many hundreds of thousands of app developers to distribute and promote their apps to millions of users. Apple told us that it competes with other software distribution platforms to attract developers by offering them access to hundreds of thousands of APIs that simplify and accelerate their app development process. Apple told us that it is committed to providing further support to app developers and that it is

---

[1] Microsoft's response to our interim report.
[2] FlickType's response to our interim report.
[3] Epic Games' response to our interim report.
[4] Apple's response to our interim report.
[5] ACT | The App Association's response to our interim report.

constantly working to improve App Store functionality and associated search performance.

16. However, as described in Chapter 6, Apple's and Google's control over their respective mobile ecosystems has allowed them to set the 'rules of the game' for app developers who seek to use their app stores, allowing them to influence competition between app developers. We heard concerns that app review processes are opaque and rules appear to be inconsistently applied, resulting in delays and uncertainty which can add to development costs and hinder innovation by app developers.

17. Nonetheless, whilst we heard that greater competition in app distribution on iOS devices would increase Apple's incentives to deliver a better service to app developers (eg in terms of a more efficient and fair app review process), stakeholders also raised concerns that promoting competition in app distribution would be unlikely, on its own, to sufficiently improve outcomes for developers.

18. Furthermore, greater competition between app stores would not necessarily address concerns relating to accessing certain hardware functionality, such as contactless payments technology, which remains within the control of the operating system. For these reasons, we were told that these interventions should be considered alongside interventions in competition between app developers (set out in Chapter 8).

Price-based competition

19. As set out in Appendix C, we found that Apple and Google have earned high, persistent and growing profits in native app distribution. Much of their revenue is driven by the commissions charged to app developers on in-app payments, although the revenue generated from advertising within their app stores has also contributed to their profitability.

20. Apple argued that the 30% commission rate was determined by reference to PC gaming stores such as Steam and Handango which also charged a commission of 30%, as well as the comparative cost of distribution of hard goods and software which cost between 40-50%, and that it was selected under competitive conditions. Apple also submitted that it has generated considerable value for app developers across the board and lowered its commission in some cases. For instance, Apple told us that it had reduced the

commission rate for ‘small businesses’ from 30% to 15% from 1 January 2021.[6]

21. However, a number of stakeholders told us that the presence of alternative app stores would inject price competition and lead to lower commission fees. To substantiate its position, Epic pointed to its current commission of 12% charged to developers for games distributed via the Epic Games Store.[7] As set out in Chapter 4, we also observe a wide range of different commission rates below 30% being charged by other PC games stores.

22. With regards to whether any cost savings made by developers would be passed through to consumers in terms of lower prices, we heard mixed views from app developers. Epic told us that when it offered a direct payment option on iOS and Android for its popular game Fortnite, it did so with reduced pricing to users that chose Epic Games’ direct payment option, due to the lower distribution costs. However, some indicated that they would not pass through cost savings, at least not in full, although we would expect these savings to improve developers’ ability to innovate and could ultimately translate into lower prices for consumers (eg via app purchases and subscriptions).

Our assessment

23. There are a range of potential benefits that greater competition between app stores could deliver. Greater competition to attract users could lead to greater investment in quality and user experience. App stores could innovate to provide better ‘matchmaking’ between users and developers and there could be increased pressure to reduce the level of advertising that users currently face.

24. Increased competition between app stores could also lead to increased price competition and lower commission fees for developers. Any cost savings for developers could also potentially result in a reduction in prices for users and deliver a number of non-price benefits, if developers had a greater incentive and ability to invest in developing more innovative apps.

25. Greater competition between app stores could also lead to improved terms for developers. It is noteworthy that Microsoft[8] recently announced that it would implement a new set of Open App Store Principles that will apply to the Microsoft Store on Windows. These principles commit Microsoft to engage in

---

[6] Small businesses are defined as earning up to one million dollars in “proceeds” (defined as sales net of Apple’s commission and certain taxes and adjustments).
[7] Epic Games’ response to our interim report.
[8] Adapting ahead of regulation: a principled approach to app stores, Microsoft Blog, February 2022.

a number of pro-competitive practices which will benefit developers, such as to: (i) treat apps equally without unreasonable preferencing or ranking of Microsoft's apps; (ii) not require developers in its app store to use their payment system to process in-app payments; and (iii) not prevent developers from communicating directly with their customers through their apps for legitimate business purposes, such as pricing terms and product or service offerings.

26. Microsoft made this announcement in anticipation of new app store legislation being considered by governments around the world, including by the United States, the European Union and elsewhere. However, a more open and competitive ecosystem, where users have a broader choice of what app stores and services to use, could result in these principles being adopted by app store providers.

27. Nonetheless, the removal of restrictions on access to alternative app stores would be unlikely to resolve the concerns expressed by developers without complementary requirements, such as those to make switching easier. The Play Store faces limited competition on Android devices without Google imposing outright prohibitions on alternative app stores. We have therefore considered below what additional measures might need to be introduced to support this intervention, including whether they can be designed and implemented effectively in practice.

Effectiveness (feasibility and technical design considerations)

28. As described in Chapter 4, Apple prohibits all alternatives to the App Store for native app distribution on iOS, giving it a monopoly over native app downloads on its devices. Requiring Apple to allow alternative app stores to operate on its iOS would therefore be a necessary first step for any interventions to be effective on Apple devices.

29. However, the competitive conditions faced by the Play Store on Android devices, where some alternative app stores are available, suggests that removing restrictions on iOS would not be sufficient to ensure this becomes an effective competitive constraint. As described in Chapter 4, the following market features and practices would need to be overcome for alternative app stores to become an effective source of competitive constraint on iOS and Android devices:

    - **Google's agreements and policies** with manufacturers and app developers which limit the constraint from alternative Android app stores.

- **Compatibility and technical issues,** whereby the introduction of new distribution channels could affect developers' app design decisions which, in turn, could lead to additional costs for developers.

30. In this section, we set out some relevant background as well as stakeholders' views on the impact of these factors. We then consider what steps would be required for app store competition to be effective, including the extent to which it would be appropriate to devise a package of remedies to deliver the potential benefits described above. Whilst this assessment is focused on Android, the same principles would apply to iOS if it were to be opened up to greater competition in app distribution.

Google's agreements and policies

- *Agreements on the pre-installation and prominent display of the Play Store*

31. Several stakeholders told us that Google's agreements and policies with manufacturers make it more difficult for third-party app stores to succeed. In particular, our analysis found that Google's decision to license its first-party apps and proprietary APIs and make significant payments to device manufacturers conditional upon the preinstallation and prominent placement of the Play Store creates a significant barrier for rival providers of app stores.[9]

32. Google told us that its first party apps, including Google Search and Chrome, and Google Play Services rely on the presence of the Play Store to act as their trusted updater, for security and safety reasons. Given that, as of April 2022, [70-80]% of apps available on the Play Store use at least one Google Play Services API,[10] the presence of the Play Store is currently necessary to deliver the proper functioning of, and updates associated with, many native Android apps on its platform.

33. Further investigation would be required to understand whether the use of the Play Store is the most appropriate mechanism to deliver these updates. Indeed, as explained in Chapter 4, Google has not set out any technical reasons for the Google source delivering updates to necessarily be an app store. In any case, an intervention which prevented Google from making its search advertising revenue share payments and its licensing of its first-party

[9] Further, as explained in Chapter 4 and Appendix E, some revenue sharing agreements Google has in place with manufacturers include a requirement to set the Play Store as the default app store and not preload similar services to the Play Store, such as alternative app stores, launchers and apps not available on the Play Store, on their device. We consider potentially affects the take up of alternative app distribution channels.
[10] Google told us that while many third-party Android apps use at least one Google Play Services API, this is not a good indication of the effort/costs a developer would need to incur to port their app to an Android device that does not include Google Play Services because, among other reasons, that would depend on the number and complexity of the APIs the developer uses in its app.

apps and proprietary APIs conditional upon the 'prominent display' of the Play Store, could improve access opportunities for rival app stores without giving rise to concerns regarding the proper functioning of these apps.

- *Access to alternative app stores*

34. In the interim report, we suggested that making third-party app stores available on both the App Store and Play Store could materially widen users' access to alternative app stores and also provide a mechanism for alleviating security concerns. Google challenged the view that lack of availability of third-party app stores in the Play Store contributes to comparatively fewer users downloading a third-party app store.[11] Google also told us that it would be practically impossible for the Play Store to review a third-party app store and all the apps it distributes for security concerns.

35. However, Microsoft told us that Google could contractually require alternative app stores to comply with a minimum set of restrictions and requirements considered necessary to ensure security and quality.[12] There are already examples of third party app stores being allowed on other app stores – for example, we observe that a specialised games stores, Epic Games, is available on Samsung's Galaxy Store.[13,14] We discuss below the various security safeguards that the App Store and Play Store could implement to mitigate the risk associated with this step.

Compatibility and technical issues

- *Access to Google's APIs*

36. As described above, Google Search and Chrome are not the only apps which rely upon the presence of the Play Store to function effectively. As of April 2022, [70-80]% of apps available on the Play Store use at least one Google Play Services API. As such, the presence of the Play Store is currently necessary to deliver the proper functioning of, and updates associated with, many native Android apps on its platform.

37. In theory, if app developers had to reconfigure a wide range of features of their apps to ensure that they function effectively when distributed through other channels, this could pose a significant challenge for alternative app stores on Android devices. This concern would be exacerbated by the

---

[11] Google's response to our interim report.
[12] Microsoft's response to our interim report.
[13] Epic Games on Galaxy Store.
[14] We also note that third party app stores are available through official app stores on other operating systems. For instance, the Epic Games Store is available on the Microsoft Store.

presence of indirect network effects, whereby app stores need users to attract app developers and need app developers to attract users.

38. However, Google told us that the availability of Google Play Services' features, functionalities, and APIs does not depend on how an app is installed onto a Google Mobile Services (GMS) device. The availability of Google's Android App Bundles (AABs) on an open-source basis also means that other app stores, can decide to support this format. In fact, Huawei's AppGallery[15] and Amazon's Appstore[16] already support apps compatible with the AAB format.

39. Nonetheless, the Play Store itself also includes specific APIs which developers can use to perform certain functionalities. For instance, the Play Store's in-app review API[17] allows developers to prompt users to submit Play Store ratings and reviews without leaving the app or game. Therefore, if a developer is already distributing through the Play Store and decides to add a new distribution channel for their app, we have been told that the developer must strip out the Play Store-specific adjustments so the app can function on other distribution channels.

- *Automatic updates*

40. As described in Chapter 4, we also heard that alternative app stores have faced challenges ensuring that their apps get automatically updated, with the user having to manually update the app. If users do not receive the same level of experience on apps downloaded outside of the Play Store, this could give the Play Store an advantage relative to rivals.

41. Although we understand Google has introduced changes to the way in which apps can be updated with Android 12, we heard from F-Droid that these changes still have limitations and provide a 'second rate' experience. Moreover, this change will affect only a small number of Android devices in the short term because the majority of active Android devices use older versions of the Android operating system.[18]

Our assessment

42. We consider there to be a good case that the benefits from opening up competition through requiring alternative app stores to be supported on iOS

---

[15] App Bundle - HUAWEI Developer.
[16] Amazon Appstore support for Android App Bundle, July 2021.
[17] Google Play In-App Review API | Android Developers.
[18] According to StatCounter, in April 2022, there were only 21.8% Android devices using Android 12.0 in the UK. See Android Version Market Share United Kingdom | Statcounter Global Stats.

could outweigh the costs of intervening. Specialised app stores, in particular with respect of gaming, could provide new ways for users to identify, download and update apps and would also put competitive pressure on Apple's App Store. Such app stores are a common source for consumers seeking access to games on PCs.

43. To make this constraint effective on Android devices, some of the barriers that currently impede alternative app stores from competing effectively with the Play Store would also need to be tackled. An intervention which prevented Google from making its search advertising revenue share payments and its licensing of its first-party apps and proprietary APIs conditional upon the 'prominent display' of the Play Store could improve access opportunities for rival app stores without giving rise to concerns regarding the proper functioning of these apps.

44. Another policy that likely limits the constraint on the Play Store is that third-party app stores cannot be accessed through the Play Store. Although Google challenged the impact of this, we consider that the lack of access to this distribution channel cuts off a key gateway for third party app stores to access users (eg in terms of discoverability).

45. We also understand that app developers may need to reconfigure certain features of their apps to ensure that they function effectively when distributed through other channels. As described above, APIs housed within Google Play Services can be accessed irrespective of how an app is installed onto a GMS device. However, developers can also make use of APIs which are specific to the Play Store and as such, may need to remove or replace these functionalities using different APIs if they wanted to make their apps available outside of the Play Store.

46. We have reviewed the functionalities covered by these Play Store APIs, and they appear to be targeted at features which are specific to an app store and would benefit from being opened up to competition, such as payment processing and app ratings. Therefore, whilst replacing or adopting substitute APIs could increase costs to developers, it also invites differentiation and competition on a number of key features that could deliver benefits for developers and users.

47. Despite these potential benefits, the challenges faced by alternative app stores on Android devices in attracting a sufficient user base, which as we note in Chapter 4 may be exacerbated by Google's initiatives such as Project Hug, may be difficult to overcome. As such, we have also considered whether sideloading would have a greater prospect of imposing a competitive constraint on the Play Store than alternative app stores and if so, what steps

would be required for sideloading to be an effective native app distribution model.

Sideloading

48. Sideloading is another potential source of competition in the distribution of native apps. Sideloading refers to the process whereby users can install native apps directly from web browsers. Currently, Apple does not allow users to sideload native apps on its iOS devices and whilst sideloading is possible on Android devices, we found evidence that sideloading places only a very limited constraint on the Play Store.

49. In this section, we set out relevant background and stakeholders' views on the potential benefits that greater competition from sideloading could deliver for users and developers. We then consider the various factors and design considerations that could influence the effectiveness of any interventions, including the extent to which it would be appropriate to devise a package of remedies to deliver these potential benefits. Whilst this assessment is focused on Android, the same principles would apply to iOS if it were to be opened up to greater competition in native app distribution.

Potential benefits

50. The potential benefits associated with sideloading are similar to the benefits from greater app store competition. If sideloading were to increase the competitive pressures on the App Store and Play Store, it could lead to improved outcomes across the categories of benefits described above, notably improved quality of service for users and developers and enhanced price competition.

51. However, sideloading also presents additional potential benefits in terms of addressing the disintermediation between app developers and users. Specifically, this could allow developers to have a more direct relationship with users. We heard that it would allow developers to offer improved customer services and potentially offer more targeted or higher quality services.

52. Furthermore, sideloading has the potential to materially lower the distribution costs faced by those developers who currently pay significant levels of commission on revenues generated from in-app transactions. As with alternative app stores, we heard mixed views regarding whether any cost savings made by developers would be passed through to consumers. Nonetheless, sideloading has a greater prospect of reducing the overall distribution charges incurred by developers, which we would expect to

improve developers' ability to invest and innovate and could ultimately translate into lower prices for consumers (eg via app purchases and subscriptions).

Effectiveness (feasibility and technical design considerations)

53. Several stakeholders told us that sideloading had a greater prospect of success than alternative app stores at delivering improved outcomes for users and developers. The key reason given was that sideloading does not face the challenge of overcoming indirect network effects to be effective, nor would it be as affected by pre-installation and default biases. Nonetheless, the experience of sideloading on Android, where it is permitted, demonstrates that removing restrictions on iOS alone would not be sufficient to promote this source of competition.

54. Basecamp and Match submitted that the success of sideloading was dependent upon the removal of unnecessary friction or restrictions which currently dissuade users from using this distribution channel.[19] Google challenged this position and described its warnings as modest and necessary to safeguard against security risks.[20] Google also called on us to investigate whether its sideloading warnings were deterring users from downloading legitimate apps through this method.

55. As described in Chapter 4, sideloading is not perceived as a viable distribution channel or alternative to the Play Store by many developers due to the process users have to go through on Android devices to sideload apps. We were told that Google should be required to facilitate a streamlined app approval process for trustworthy apps, using certification, notarisation or similar processes to identify such apps.

56. An additional concern raised by stakeholders relates to the challenges that sideloaded apps faced to get automatically updated, with the user having to manually update the app. If users do not receive the same level of experience on apps downloaded outside of the Play Store, this could give the Play Store an advantage relative to rivals. As described above, although we understand that Google has introduced changes to the way in which apps can be updated with Android 12, this change only currently affects a small proportion of Android devices and we heard from F-Droid that these changes still have limitations and provide a 'second rate' experience.

[19] Basecamp's response to our interim report.
[20] Google's response to our interim report.

Our assessment

57. Overall, we consider that opening up competition through requiring sideloading could deliver a number of benefits and faces fewer challenges than alternative app stores in its effectiveness. As set out in Chapter 6, at least a fifth of app downloads were directed to Apple's and Google's respective app stores from web browsers or other apps. This finding suggests that if sideloading was adopted by developers and was more easily available for users, its take-up could be high since users would be able to download apps directly from the developers' website, rather than having to direct users to app stores. In turn, this constraint could put greater competitive pressure on app stores to improve their service to attract users and improve their terms of access for developers.

58. We would expect that, if the choice architecture was less onerous and alarming, more users would choose to access native apps directly from the developer, as is the case on other desktop devices. This, in turn, would also mean that developers may be more inclined to make their apps available to sideload and promote them with their users.

59. However, we accept that sideloading gives rise to increased security concerns. Given the need to preserve the integrity of the operating system, any interventions which removed such obstacles must facilitate other means of certifying that apps meet minimum security standards. The introduction of potential safeguards to achieve this objective is discussed in the next section.

Risks associated with promoting alternative app distribution models

Security

60. Although promoting alternative app distribution models could deliver a range of benefits, several risks have been raised in relation to these interventions. In particular, we were told that promoting alternative app distribution models could give rise to security risks because apps downloaded outside of the App Store and Play Store may not have been through a process which screens for malicious software ('malware') and ensures that they are only provided with access to data or functions that are necessary for their purpose.

61. In this section, we have summarised the views provided by stakeholders on the scale of the security concerns and impact of any interventions. We then explore the nature and scale of potential security risks associated with introducing new app distribution models before providing relevant background

on the application model adopted by mobile operating systems and the extent to which the security models adopted on iOS and Android differ in nature.

Box N.1: Key security findings in relation to app distribution

App installations can give rise to cybersecurity threats for users of mobile devices:

- while high-value software vulnerabilities tend to be reserved for high-value targets, there are risks from harmful and insecure apps that affect the average consumer; and
- the use of alternative distribution channels may give rise to increased security risks on iOS and Android devices, unless appropriate safeguards are introduced.

The security models of Apple and Google are broadly similar. In both systems, many different components work together to provide 'defence in depth' from potential attacks. For instance:

- the operating system protects the system when malware is executed by limiting the range of data and services that an app can access;
- digital signatures can be used to limit the installation and update of apps from a specific app store or developer; and
- app review reduces the risk that malware gets installed on the device.

The app review process provides an important security safeguard. App stores are effective at reducing the prevalence of harmful apps, with a lower incidence of malware and insecure apps being identified in the app stores of Apple and Google compared to third party app stores.

Interventions should therefore retain appropriate security checks to mitigate risks from apps installed through alternative channels. Importantly, it is not necessary for the app review process to be tied to a specific distribution channel. As a result, when apps are distributed through alternative channels, the app review can be conducted by platform operators or certified third parties. For instance:

- app review could be delivered by third-party app stores or other third parties, whose processes could be reviewed by Apple and Google; and
- alternative app distribution providers could be contractually required to comply with a minimum set of standards and requirements considered necessary to ensure security and quality.

Alternatively, Apple and Google's existing app review process could be made available to sideloaded apps or apps available on third party app stores. Whilst this approach should be effective at addressing security risks, it would offer more limited potential for differentiation and improvements both in security and in apps themselves.

62. We then describe the various processes adopted across operating systems, such as app review processes, and code signing, to help mitigate these risks. This assessment has been informed by an independent expert, Alastair Beresford, Professor of Computer Security at University of Cambridge. However, our assessment is still preliminary in nature and further exploration of these issues is likely to be required in taking interventions forward.

63. Our key findings on these issues are summarised above in Box N.1.

Stakeholders' views

64. We heard a wide range of contrasting views regarding the security risks that potential interventions in app distribution could give rise to. Apple[21] told us that a number of the potential interventions highlighted in our report would fundamentally change the iPhone and have huge implications for consumers, including in terms of Apple's industry-leading privacy and security standards. In particular, Apple argued that the interim report significantly downplayed the security risks associated with forcing it to allow alternative app stores or sideloading which it argued would increase the risk of malware attacks that would put all users at greater risk.

65. Apple also submitted that every Apple device combines hardware, software and services designed to work together for maximum security and privacy and a transparent user experience in service of the ultimate goal of keeping personal information safe. It argued that interventions would jeopardise its holistic approach to security, which it told us is significantly more effective than Android.[22] Apple has also published a paper which found that mobile malware and the resulting security and privacy threats are increasingly common and predominantly present on platforms that allow sideloading.[23]

66. Apple's view on this subject were aligned with that of ACT | The App Association[24] who told us that allowing users to download apps through sideloading or alternative app stores carries several significant risks. According to the ACT | The App Association, it could lead to introduction of additional app stores that are less privacy-focused than the incumbents, which would disadvantage small developers and startups, and referenced

---

[21] Apple's response to our interim report.
[22] Apple referred to Nokia's 2020 Threat Intelligence Report finds that devices that run on Android had 15 times more infections from malicious software than the iPhone, see Report - Threat Intelligence Report 2020 (nokia.com).
[23] Building a Trusted Ecosystem for Millions of Apps, A threat analysis of sideloading, Apple, October 2021
[24] ACT | The App Association's response to our interim report.

reports[25] which found that third-party app stores have fewer security safeguards in place and could lead to malicious apps being downloaded and negatively affecting consumer trust in the ecosystem. Google also warned against misjudged interventions that could have severe consequences for the security and privacy of Android users, as well as for the integrity of the Android ecosystem.

67. However, a number of stakeholders told us that Apple's security arguments were overstated and that safeguards were available to mitigate any increased security risks associated with widening the distribution channels through which native apps could be accessed. For instance:

- FlickType[26] told us that Apple's security arguments should carry no weight for several reasons. In particular, FlickType submitted that sideloading is not necessarily insecure, as it is currently made available by Apple on its Mac devices, after going through Apple's 'notarization' screening process which ensures users download safe apps on macOS, and there is no reason why this functionality could not be extended to iOS. FlickType also argued that nothing would prevent Apple from imposing security standards to app stores wishing to be made available on the App Store.

- Match Group[27] described Apple's security and privacy arguments as overblown and argued that they should not be taken at face value. Whilst Match Group submitted that a framework should be put in place to ensure the security of users and the integrity of the device, it argued that sideloading and alternative app stores could operate within that framework and referenced a paper which describes alternative approaches that would protect user security, including extending the notarisation process currently available on MacOS to iOS platforms.[28]

- Epic[29] submitted that Apple and Google's security arguments are often pretextual or exaggerated. Epic also pointed to the notarisation process on MacOS as a demonstration that these concerns could be overcome. Epic argued that the choice between competition and security is not binary and that greater competition in the distribution of applications on mobile devices would also spur innovation and improvements in security and privacy offerings.

---

[25] For instance, this report from RiskIQ: 2020 Mobile App Threat Landscape Report.
[26] FlickType's response to our interim report.
[27] Match Group's response to our interim report.
[28] Should iOS users be allowed to download app through direct downloads or third-party app stores? Coalition for App Fairness.
[29] Epic Games' response to our interim report.

68. Microsoft has stated publicly that it believes that it is possible for governments to adopt new tech regulation that promotes competition in app distribution while also protecting fundamental values like privacy and national and cyber security.[30] Microsoft also submitted that Apple should be permitted to require that alternative iOS app stores comply with a minimum set of restrictions and requirements, although it warned against this process being used to introduce unnecessary and burdensome obligations which harm alternative app stores from competing effectively.

69. Finally, Microsoft stated that Apple currently permits what amounts to sideloading through Apple Enterprise Management[31] which, in its view, demonstrates that the security, privacy and quality of the iOS ecosystem can be preserved using measures that are less restrictive than an outright prohibition on sideloading.

Security risks

70. According to an independent expert who we consulted, the complexity of software on mobile devices, coupled with the constant provision of new features and services, means that there will always be latent vulnerabilities waiting to be discovered and an accompanying risk that malware can be executed on devices through harmful or vulnerable apps. The software that underlies mobile platforms constantly evolves, and so some level of risk is unavoidable.

71. Vulnerabilities can be exploited to carry out serious attacks. Apple and Google have their own bounty programs to manage vulnerabilities that could fall into the wrong hands.[32,33] High-value vulnerabilities, when found by security researchers, are usually reported to Apple or Google or sold on the grey market.[34]

72. We have heard from experts (RET2, Alastair Beresford) that while attacks which exploit software vulnerabilities are possible, it is rare that they affect average consumers. When an exploit is widely used, it is more likely to be found by developers and reported to Apple or Google, who then secure their system, with the result that the vulnerability can no longer be used. As a

[30] Adapting ahead of regulation: a principled approach to app stores, Microsoft Blog, February 2022.
[31] We understand Apple Enterprise Management to refer to Apple's Developer Enterprise Program, described further here.
[32] Google and Alphabet Vulnerability Reward Program (VRP) Rules.
[33] Apple security bounty.
[34] Zerodium Exploit Acquisition Program.

result, severe attacks that depend on high value vulnerabilities tend to be reserved for high-value targets and consumers are not affected in most cases.

73. The main security issue faced by users of app stores is malware, which is any kind of software that can damage computer systems, networks or devices.[35] Even though consumers are rarely exposed to severe cyberattacks that fully compromise their devices, there are a number of risks that come from insecure and intentionally harmful apps,[36] as evidenced when they have been installed on devices.

74. Malware can be embedded within apps and used to attempt to extract money or steal data from the user. SMS trojans like Joker malware send text messages from the victim's phone to purchase content, thus extracting money from the user.[37] It has been estimated Joker malware have been downloaded 200,000 times from the Play Store.[38] Trojan malware can also steal data from user's phones and displays adware, an example being PhantomLance.[39]

75. Consumers may also be harmed when apps process data insecurely, are fake or cloned, or carry out in-app payment fraud. Fraudulent copies of existing apps, which may charge users subscription fees, have been identified on iOS devices. For example, a copy of the app, FlickType, was made available on iOS[40] and a number of apps have been removed from the App Store for misleading users into purchasing premium services.[41]

Security models of Android and iOS

76. The security models of Apple and Google are broadly similar. In both systems, many different components work together to provide 'defence in depth' from potential attacks. These elements include the operating system, app review and digital signing of code to verify its source.

Operating systems

77. The Android and iOS operating systems have similar features in place to provide security.[42] The operating system is the main component of the

---

[35] Threat report on application stores, National Cyber Security Centre (2022).
[36] Wei, F., Li, Y., Roy, S., Ou, X., Zhou, W. (2017). Deep Ground Truth vAnalysis of Current Android Malware. In: Polychronakis, M., Meier, M. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2017. Lecture Notes in Computer Science, vol 10327. Springer, Cham.
[37] Android security: Six more apps containing Joker malware removed from the Google Play Store, ZDNet, 2020.
[38] New Joker malware detected on Google Play, 500.000+ users affected, Pradeo, 2022.
[39] Hiding in plain sight: PhantomLance walks into a market, Secure List, 2020.
[40] Apple's App Store is hosting multimillion-dollar scams, says this iOS developer, The Verge, 2021.
[41] Demystifying Removed Apps in iOS App Store, Lin, F, 2021
[42] Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions, Zinkus M, Jois T M, Green M, 2021.

software on the device and manages system resources. From a security perspective, the operating system aims to prevent attackers from compromising the system to run code or steal data from the device. In the case where malware is executed on the device, the operating system acts to preserve the integrity of the system. The operating system achieves this in part through limiting the actions that apps and websites can perform. Some limits are applied to all apps and websites, whereas others are conditional.

78. A second way that the operating system provides security is by keeping the operation of apps separate from each other. Apps cannot modify files or access data from other apps unless they have been explicitly granted permissions to do so, for instance through user consent. The functionality which provides separation between apps is referred to as the application sandbox. The application sandbox is currently specific to mobile devices and provides additional security over desktops, where less separation is enforced between applications. Limitations are also placed on how apps communicate with each other, with dedicated mechanisms in place in both ecosystems.

App Review

79. In Apple's and Google's ecosystems, an extra layer of security is provided by app stores.[43,44] The App Store and Play Store allow Apple and Google to analyse the content of apps and their behaviour through the app review process before they are offered on the app store. From a security perspective, app review aims to exclude apps that harm users from app stores, and thus provides a filter which prevents such apps from being installed.

80. Academic studies of apps have shown that popular apps that can be harmful have been made available in Apple's and Google's app stores.[45,46] However, overall, these studies of app review demonstrate that app stores have been relatively effective at screening for malware and that more established app stores have a lower prevalence of harmful apps.[47,48]

81. For the majority of iPhone users, all apps on iOS undergo Apple's app review. There are two exceptions. Firstly, through the Apple Developer Enterprise Program, large organisations can develop and deploy proprietary, internal-use

---

[43] App Store Review Guidelines, Apple, 2022.
[44] Google Play Developer Policy Centre, Google, 2022.
[45] A Longitudinal Study of Removed Apps in iOS App Store, Lin F, Wang H, Wang L, and Liu X, 2021.
[46] Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets, Wang H, Liu Z, Liang J, Vallina-Rodriguez N, Guo Y, Li L, Tapiador J, Cao J, and Xu G, 2018.
[47] Android Security & Privacy 2018 Year In Review, Android, 2019.
[48] We note that direct comparisons are not available in certain cases. For example, third-party app stores app review cannot be directly compared to App Store app review on iOS since third-party app stores are not permitted on iOS. A study of apps removed from Apple's App Store did not find any malware (Lin et. al., 2021). This suggests that the prevalence of malware on iOS may be low.

apps to their employees, without review.[49] Secondly, we have been told that Apple allows owners of macOS devices to use the developer tools to compile, build and install iOS apps onto iOS devices connected locally via USB cable. In this sense, sideloading is possible on Apple devices.

82. On Android, apps downloaded through the Play Store are reviewed, whereas apps downloaded through sideloading, or other app stores, do not necessarily undergo an app review by Google prior to installation. Neither Apple nor Google provide public-facing documentation on the specifics of the analyses that are performed during the app review process.[50] From existing research and expert opinion, we can infer that app review is likely to involve a combination of static and dynamic analysis.[51,52]

83. Static analysis involves an examination of the files that are submitted. For example, static analysis software can be used to scan app files for logical errors and misuse or exploitation of APIs. Dynamic analysis involves examination of the app's behaviour when it is run in a test environment. Dynamic analysis can find suspicious behaviours that emerge only when the code is run. Both static and dynamic analyses are likely to use a combination of human review and automated tests.

Digital signatures

84. Digital signing of code contributes to security by verifying the source of code that is executed on the device and data included in the app. Digital signatures ensure that the software is authentic and has not been modified since it was signed. Verification of digital signatures is applied by app stores during app submission and updates, and each time an app is loaded on the operating system. When an app is submitted or updated through an app store, the operating system verifies that the app comes from the app developer and not a different source.

85. Apple mandates that all code executed on iOS be signed using Apple-issued certificates.[53] For apps submitted to Apple's App Store, Apple verifies the developer's signature using a certificate and then signs the app with Apple's signature. Google told us that Android requires developers to cryptographically sign their apps with a certificate before they are installed on

---

[49] Apple Developer Enterprise Program, Apple, 2022.
[50] Information on app review and developer concerns that have been voiced is provided in Chapter 6 of this report.
[51] Static analysis of android apps: A systematic literature review, Information and Software Technology, Li L, Bissyandé T F, Papadakis M, Rasthofer S, Bartel A, Octeau D, Klein J, and Traon L., 2017.
[52] Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions, Umara U, Al-rimy B, Zainal A, Ghaleb F, and Rassam M, 2022.
[53] App code signing process in iOS and iPadOS, Apple Platform Security, 2022.

a device or updated. This allows the identity of the app developer to be verified, in order to, for example, ensure that updates to the app are genuine, and protect users from malicious updates.[54]

86. Epic Games also told us that apps can go through a similar signing process on the Windows operating system, without having to use Microsoft's own malware scanning service. Developers can rely on a third-party certification authority to generate digital signatures for its apps, which serve the same source-identification purpose as the signature that Apple's notarisation tools help developers generate.

87. Code signing is therefore an important feature of security on mobile operating systems. If the remedies we suggest were implemented, Apple and Google would continue to be able to enforce code signing, with code either being signed by themselves or by certified third parties.

Software update delivery in Android and iOS

88. While the security model of Apple and Google's systems is similar, including operating systems with similar design, the provision of app review, and mandatory code signing, Apple's ecosystem is more vertically integrated than Google's more open system, with consequences for security due to how software updates are delivered to system software and applications.

89. Google oversees a diverse system. Google designs and supplies the operating system and makes this widely available to device manufacturers. Due to the variety of different device manufacturers that use Android as their operating system, responsibility for ensuring device security is shared between Google and the device manufacturers. Apple, on the other hand, provides a fully integrated system, where the hardware and all accompanying software are produced by Apple. Therefore, responsibility lies solely with Apple to ensure that iPhones are secure.

90. This difference in the level of vertical integration means that there is more diversity in the frequency and delivery of updates on Android devices. Therefore, we understand that vertical integration is likely to be responsible, at least in part, for differences in the security of system software on Android and iOS devices.

91. Software updates are crucial for securing mobile devices.[55] Cyberattacks which have affected consumers have used vulnerabilities in out-of-date

---

[54] Use Play app signing - Play Console Help.
[55] Device Security Guidance, National Cyber Security Centre, 2021.

software.[56,57] Software security updates enhance security and patch vulnerabilities which could be used by attackers. Consumers can be subjected to attacks where vulnerabilities are present simply because software is out of date.

92. On Android, responsibility for system software updates is distributed across Google, network operators, and the device manufacturers. The security of Android devices depends strongly on the manufacturer and their effectiveness in rolling out system security updates to users' phones. Therefore, known vulnerabilities may have been fixed in the Android source code, but these updates have not been integrated by all manufacturers or delivered as updates to individual devices.

93. In addition, Android devices may only receive updates for a limited period which is defined by the device manufacturer. As a result of this, less than a quarter of popular Android phone models use up-to-date system software.[58] This contrasts with Apple's ecosystem where the provision of updates is largely under Apple's control. As a consequence, the majority of iPhones run on up-to-date system software.[59]

94. If implemented, interventions aimed at allowing new app distribution channels on iOS would not impact vertical integration between Apple's hardware and operating system. Therefore, Apple would retain full control over iOS and hardware irrespective of whether new app distribution channels are introduced on iOS.

95. Furthermore, we recognise the distinction between system software updates and application updates. Application updates are also important for device security. While system updates appear to be delivered more frequently and on more iOS devices than on Android devices, conversely, some individual apps may be updated more frequently on Android. For example, as is examined in Appendix F, updates to Google Chrome's browser engine, Blink, through Google Play may provide more frequent updates than Safari's browser engine WebKit, which are delivered alongside operating system updates.[60]

---

[56] Assess Your Risk From Ransomware Attacks, Powered by Qualys Research, Qualsys, 2021.
[57] Investigation: WannaCry cyber attack and the NHS, National Audit Office, 2017.
[58] According to StatCounter, in April 2022, there were only 21.8% Android devices using Android 12.0 in the UK. See Android Version Market Share United Kingdom | Statcounter Global Stats.
[59] 72 percent of all devices introduced in the last four years use iOS 15, as measured by devices that transacted on the App Store on January 11, 2022, Apple Developer Support, 2022.
[60] See Table F1 and Figure F8, Appendix F.

App distribution

App review on iOS can be delivered by third parties

96. As described above, the app review process provides a further layer of security, which helps protect devices from malware. Screening of apps on iOS, however, does not necessarily need to be delivered by Apple's app review process. An app review process delivered through an alternative app store could, in theory, be as effective as Apple's app review.

97. An alternative app store could take on the role of reviewing apps and managing payments for apps downloaded from their store. This is already permitted in Google's ecosystem, an example being Samsung's Galaxy Store. This would require the alternative app store to develop suitable technical and human review processes and complaints handling procedures. These processes could be reviewed by Apple to ensure that security standards are maintained, while ensuring that such processes do not unnecessarily burden third-party app stores.

98. It is also possible for the app review process to be delivered through other certified third parties. For example, anti-virus software could be integrated within app stores to provide assurance to users that apps are secure prior to installation. Indeed, such products already exist and have been developed for integration with Google's Play Store by the anti-virus software company, Norton.[61]

99. Compliance with a Code of Practice, such as a recent proposal set out by DCMS, described further within Box N.2, could also play an important role in ensuring that users are better protected from malicious and poorly developed apps.[62] This approach could lead to the creation of a set of baseline principles for any operator to ensure that users can securely benefit from more choice without compromising their device's security or their own privacy.

100. Cooperation between app developers and operating system providers could also lead to certain developers obtaining a trusted status from the perspective of the platform provider.[63] Developing security standards for app developers could lead to a set of transparent principles and security practices to follow

[61] Norton Mobile Security for Android, Norton, 2022.
[62] App Security and Privacy Interventions, Department for Digital Culture, Media and Sport, May 2022.
[63] We note that, through the Apple Developer Enterprise Program, large organisations can already develop and deploy proprietary, internal-use apps to their employees, without review. Organisations which satisfy certain conditions can apply to the program using an Apple ID and, following a verification interview, can distribute apps to their employees using enterprise certificates issued by Apple.

during app development, as well as standards relating to acceptable app behaviour.

Box N.2: DCMS code of practice for App Stores

In May 2022, DCMS published a Call for Views on App Security and Privacy interventions, following a review of the app store ecosystem. The review found that the availability of malicious and poorly developed apps on app stores is putting users' security at risk. Although the review recognised the leadership of Apple and Google in defining current best practice, it also found that prominent app store operators could do more to protect users.

To address these concerns, DCMS has initially proposed the introduction of a voluntary Code of Practice for all app store operators and app developers which would ensure that the security and privacy of users is prioritised, thereby reducing the threat from malicious apps.

The proposed scope of the code covers a range of practices for app store operators and app developers to implement in order to protect users. Areas that are covered range from the provision of important information on apps to users to the provision of mechanisms for disclosing code vulnerabilities to app developers. The code also sets out the recommendation to keep apps updated to protect users, involving responsibilities for both app store operators and developers.

Security checks could be applied to apps from alternative channels

101. Since app review is a standalone element of security, app review is not tied to one app distribution channel. This separability means that app reviews and automated checks could potentially be applied to apps installed through alternative channels. Apple already applies an automated review process to apps on macOS, which can then be distributed through sideloading. Notarisation is used to perform automated checks on software downloaded outside of the App Store.[64]

102. Apple's Craig Federighi (its Senior Vice President of Software Engineering) has also stated the following: 'we have a level of malware on Mac that we don't find acceptable, and it is much worse than iOS.'[65] Apple asserted that it had to make the iPhone considerably more secure and reliable due to: (i) the breadth and sensitivity of the personal data on mobile devices that exceeds computers; (ii) the fact mobile devices can be a user's lifeline in an emergency and is integral to how users live, work and communicate; (iii) the iPhone's size and portability meaning it may be more likely to be misplaced or

[64] Notarizing macOS Software Before Distribution, Apple, 2022.
[65] See Epic Litigation Trial Transcript 3389.

stolen; (iv) the fact that the large size of the iPhone user base would make an additional appealing and lucrative target for cybercriminals and scammers.[66]

103. Despite these assertions, developers of macOS apps can use Apple's notary service to obtain a digital signature or 'ticket' which certifies that their app has been checked for malicious components by Apple. This 'ticket' allows macOS devices to cryptographically check that an app distributed outside the Mac App Store has been checked by Apple's notary service and is intended to give users confidence that the app is not malicious.

104. From a technical perspective, the same conceptual idea could be used for iOS applications to enable distribution of notarised apps outside the App Store. As currently formulated, this would remove the human review from the analysis, however the process could be modified to include a human review element if this was deemed necessary to preserve the same level of assurance.

On-device checks

105. On-device checks, such as those used by anti-virus software like Norton, Avast, and BitDefender, as well as those offered by platforms like Google Play Protect can also be used to mitigate some of the risk from apps installed through alternative channels. Google quantifies this in their Android Security Year in Review by stating that Google Play Protect prevented 73% of potentially harmful app installation attempts in 2018.[67]

106. Although this means that 27% of these installations succeeded, Google's definition of 'potentially harmful apps' is broad and includes some apps which users actively want and are not necessarily harmful. Nonetheless, since app review is imperfect, as highlighted through some examples above, on-device checks could play an important additional role in monitoring devices for malware.

Our assessment

107. There are several security features of mobile operating systems, including app reviews, which make an important contribution to security and can mitigate the risk of malware being downloaded onto users' devices. However,

---

[66] Apple submitted that its focus on ensuring the iPhone was as secure as possible was reflected in its announcement of SDKs in October 2007 where Apple said '[i]t will take until February to release an SDK because we're trying to do two diametrically opposed things at once—provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc.' See Apple - Hot News (archive.org).
[67] Android Security & Privacy 2018 Year In Review, Android, 2019.

we accept that opening up app distribution to greater competition would likely require a framework to be put in place to safeguard the security of users and the integrity of mobile devices.

108. We have explored various options to address these concerns. Digital signatures of apps verify the source of all code executed on the device. Since app review is not necessarily tied to an individual app distribution channel, apps could be distributed through multiple channels, such as an alternative app store or sideloading, whilst providing a digital signature or 'ticket' which assures the operating system that the app has undergone an app review process.

109. Alternatively, alternative app stores could be contractually required by the device manufacturer to comply with a minimum set of standards and requirements considered necessary to ensure security and quality. The Code of Practice, proposed by DCMS, could lead to the creation of a set of baseline principles for any app store operator to ensure that users can securely benefit from more choice without compromising their device's security or their own privacy.

110. Based on our review, there appear to be several safeguards available that could be used to support the implementation of our objective of greater competition in native app distribution whilst preserving the safety and security of users' devices. As such, our current view is that these security concerns should not be insurmountable or disproportionately costly, although we recognise that further investigation on this subject is required.

Incentives to innovate

111. In its response to our interim report, Apple[68] strongly defended its existing terms of access and argued that existing charges cover more than the cost associated with running the App Store and compensate Apple for providing the tools, technology, distribution, and other services which allow developers to leverage iOS. Apple argued that amending its terms of access could lead to developers free riding on its significant investments into its mobile ecosystem since they would continue to utilise Apple's proprietary technologies and intellectual property.

112. We agree that, in principle, free riding is a legitimate concern. If developers use alternative distribution models, they may benefit from Apple and Google's

[68] Apple's response to our interim report.

investments in their mobile operating systems without contributing towards their development and maintenance costs.

113. However, several stakeholders strongly challenged Apple's position and argued that Apple already derives significant value from app developers' investments in their products and software. These investments lead to higher quality apps being made available on iOS which contributes to the success of the iPhone. Contrary to Apple's view, these stakeholders also argued that competition would likely lead to greater incentives to invest and innovate.

114. In our view, there are several reasons to suggest that Apple will retain incentives to innovate, even if it is required to allow alternative app stores on iOS. For instance:

- Our profitability analysis of Apple's App Store suggests that Apple will be strongly incentivised to remain active in app distribution and will be incentivised to compete with rivals to retain and attract users.

- It is accepted that app developers contribute to Apple's ecosystem, which Apple is able to monetise through its sale of devices. Our analysis of Apple's financial performance suggests that Apple earns very high returns on its investments into its mobile ecosystem, including its devices. As a result, Apple would continue to have incentives to innovate as it has in the past in order to maintain its market position in devices.

- Google and Microsoft have continued to invest in their respective operating systems and app stores without imposing outright prohibitions on the presence of alternative app distribution models.

115. As such, we consider that Apple would be likely to retain its incentives to maintain investment in iOS and the App Store. In fact, these incentives may become even stronger if it needs to attract users and developers with alternative options.

Other potential costs and unintended consequences

116. We also recognise that there are other potential costs and unintended consequences from interventions in mobile ecosystems to be taken into account in our assessment. Many of these have been highlighted by Apple and Google but also by other stakeholders who may be affected.

Implementation costs

117. As described above, in order to be effective, it is likely that a package of remedies would be required to promote competition in app distribution. These interventions could involve the establishment of new processes to certify that apps meet minimum security standards and requirements, which could introduce new costs to operating system providers, app stores and developers.

118. Furthermore, we understand that Apple and Google may have to undertake technical adjustments to their operating systems to support alternative app distribution models. Implementing these adjustments, as well as any new security safeguards, could result in additional costs being borne by these platforms. However, we consider that, given the scale of potential benefits that these interventions could deliver, any additional costs from increased competition would be outweighed by the resulting benefits.

119. Finally, as discussed above, app developers may need to reconfigure certain features of their apps to ensure that they function effectively when distributed through other channels. However, at present, the APIs housed within Google Play Services can be accessed irrespective of how an app is installed onto a device with GMS. We also consider that the Play Store-specific APIs appear to be targeted at features which are specific to app stores and would benefit from being opened up to competition, such as payment processing and app ratings. Therefore, whilst replacing or adopting substitute APIs could increase costs to developers, we would not expect these costs to be material and it should deliver benefits to users and developers by inviting differentiation and competition on a number of key features of these products.

Circumvention risk

120. We have heard from a number of stakeholders that facilitating competition through alternative app distribution models would be the most pro-competitive approach to tackling Apple and Google's most restrictive terms and high commission fees. However, opening up official app stores to competition will only address these concerns where the terms of access to the operating system are fair and reasonable in supporting effective competition.

121. Google does not currently charge alternative app stores to operate on Android devices or charge app developers seeking to make their products available through sideloading. Similarly, third-party app stores on Windows do not pay access fees, such as through a commission, to Microsoft for access to their operating system. Developers can also securely distribute Mac apps outside

of the App Store on MacOS without being subject to the same policies imposed on the iOS App Store.

122. Nonetheless, through their control of access to iOS and Android, Apple and Google could seek to impose terms of access on apps and app stores which restrict their ability to compete effectively in app distribution. Albeit in the context of more narrow remedies, Apple and Google have demonstrated in other jurisdictions that they can, and will, collect commission fees where interventions have forced them to remove restrictions that are currently in place.[69] Based on this experience, several stakeholders have called for explicit rules that would prevent Apple from having the freedom to adopt alternative rules that are equally harmful to competition.

123. We consider that a set of principles akin to Microsoft's new set of Open App Store Principles[70] would be effective at fostering competition in app distribution. We would not expect third-party app stores to face additional fees associated with access to Apple's and Google's ecosystems that are not incurred by Apple's and Google's own app stores, other than any fees that reflect the incremental costs associated with managing the interoperability between the operating system and these app stores.

124. The reasonableness of any terms and conditions applied by Apple or Google, including requirements to protect against security risks, should form part of the broader remedy design and implementation assessment. If the proposed terms were unduly onerous and effectively led to the self-preferencing of Apple and Google's own app stores, this should be addressed as part of the implementation.

Impact on price of devices

125. As described in Chapter 4, Apple also argued that the commission it charges in relation to in-app payments and subscriptions generates an incremental revenue flow which gives it an incentive to lower the price and increase the quality of its devices. This is described as a waterbed effect.[71]

126. We acknowledge that there may be some waterbed effect as Apple has some incentive to lower the price of its devices or to increase quality in order to capture more app distribution revenue in the App Store. However, Apple has

[69] For instance, in the Republic of Korea and the Netherlands, Apple and Google still charge a commission on in-app payments even where their own in-app payment systems are not used.
[70] Adapting ahead of regulation: a principled approach to app stores, Microsoft Blog, February 2022.
[71] In support of this Apple has submitted a theoretical model which supports this waterbed effect under a number of conditions; and also submits that, while its margins on the iPhone have continuously decreased since 2012, App Store revenues have grown.

not provided any empirical or documentary evidence to substantiate its claims that pricing decisions made by Apple at the device level are affected by service revenues such as the revenue from the App Store.

127. Furthermore, even if there was some waterbed effect, this does not necessarily offset concerns associated with its high profits in app distribution. Our finding that Apple faces limited effective competition in mobile devices and operating systems dampens its incentive to pass through price decreases at the device-level since its existing scope for increased sales through price reductions is limited. As such, any waterbed effect that results from the implementation of these remedies is likely to be limited, and consequently there should be a limited impact on the price of Apple's devices.

Our overall assessment

128. We have assessed the benefits and costs associated with potential interventions aimed at improving competition in native app distribution. Alternative app stores could provide new ways for users to identify, download and update apps. Measures could be introduced which remove some of the barriers that currently impede alternative app stores from competing effectively with the Play Store and the App Store. In turn, these options would provide more flexibility for users and increase the competitive pressures in app distribution.

129. We would expect that if competition by third party app stores was more effective, it would also be likely to result in entry by specialist app stores, in particular in respect of gaming. Such app stores are a common source for consumers seeking access to games on PCs and we were told that these app stores would also operate on mobile devices, if current restrictions were removed. However, we recognise that some of the challenges faced by alternative app stores on Android devices in attracting sufficient user base may be difficult to overcome.

130. By contrast, sideloading could deliver a number of benefits and faces fewer challenges to be effective. We would expect that, if the choice architecture was less onerous and alarming, developers would be more inclined to make their apps available to sideload and promote this distribution channel to users. In turn, the potential take-up of sideloaded apps could be high since developers would no longer require an intermediary for users to download their native apps.

131. However, there could be additional security risks associated with these app distribution models, particularly sideloading. One strong safeguard may be the extension of Apple's and Google's existing app review process for apps

downloaded directly or through third party app stores. A requirement for Apple or Google to make their app review process available in this way should be effective at addressing security risks but has a number of downsides, in particular it could result in more limited potential for differentiation and improvements both in security and in apps themselves. Alternatively, alternative app distributors could be contractually required to comply with a minimum set of standards and requirements considered necessary to ensure security and quality.

132. The broader terms on which users interact with sideloading or third-party app stores will also be relevant to their success. We therefore consider that the following interventions would need to be considered on Android, with the same principles applied to iOS if it were opened up to greater competition in app distribution:

- restrictions on the format of warning messages to users, either generally or where apps are able to demonstrate appropriate security safeguards; and

- changes to the terms on which Google is able to give its own Play Store a prominent position, to make it easier for alternative app stores to access users.

133. Finally, there is a risk that through their control of access to iOS and Android, Apple and Google could seek to impose terms of access on apps and app stores which restrict their ability to compete effectively in app distribution. The reasonableness of any terms and conditions applied by Apple or Google, including requirements to protect against security risks, should form part of the broader remedy design and implementation assessment. Under the appropriate conditions, we consider that these alternative app distribution models could deliver significant net benefits for users and developers.