31 August 2021

APPLE COMMENTS ON CMA MARKET STUDY STATEMENT OF SCOPE

A. Introduction

1. Apple welcomes the opportunity to provide comments on the CMA's statement of scope for the market study into mobile ecosystems (the "SoS").

2. The CMA acknowledged that it has "deliberately cast its net wide" so that it can genuinely understand the Apple (and Google) business models and the differences between them, both from an end-user perspective and also with regards to generation of revenue (including how the provision of services such as operating systems, app stores, browsers, and other apps relate to each company's primary sources of revenue). Apple recognises that a proper understanding of its business model will require the CMA to obtain information across a variety of areas.

3. Apple is keen to stress, however, that whilst the CMA's market study may need to explore various areas, Apple does not consider that this should be taken as an indication that there are either competition or consumer concerns with Apple's practices in those areas. Since Apple launched the iPhone in 2007, Apple's investment in that ecosystem has brought about huge innovation to the benefit of both consumers and developers alike. Apple depends on innovation by third-party app developers to compete, as the App Store is a key feature of iPhone. Indeed, when Apple first introduced the iPhone, it had no App Store. The only apps available to users were a limited selection of Apple's own apps. Soon thereafter, Apple recognized that consumers' enjoyment of the iPhone would be enhanced by unlocking the power of third-party developers. Apple has made clear since launching the first-of-its-kind App Store that its purpose "is to add value to the iPhone."[1] Apple's incentives are to give consumers choice, while ensuring that its consumers are not exploited. And Apple has done so whilst maintaining reliability, safety, security and privacy. As Steve Jobs noted in 2007 "*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. This is no easy task*."

4. Despite this, Apple is aware that it has some vociferous (and well resourced) detractors campaigning against it in the UK and elsewhere. These detractors appear to be given significant weight in the SoS and in relation to the preliminary description of Apple's business model and practices. Apple is confident that the CMA's in-depth investigation will reveal how many of the statements from third parties repeated in the SoS are self-serving, misrepresent Apple's business model and are not grounded in competition law. Apple is keen to assist the CMA to develop a proper understanding of how its ecosystem is designed and operates.

5. Apple is conscious that the purpose of the market study is to contribute to the CMA's broader programme of work in the context of its Digital Markets Strategy and that it "*hope[s] to deliver a step-change in the regulation and oversight of competition in digital markets and in turn drive dynamic innovation*". The SoS also sets out an overview of potential future remedies.

---

[1] Steve Jobs Introduces the App Store – iPhone SDK Keynote, YouTube (Mar. 13, 2008), https://www.youtube.com/watch?v=xo9cKe_Fch8.

6. The CMA should be mindful of the potential downsides and difficulties in attempting to substitute a regulator's judgment for that of the business with respect to individual commercial issues. Changes mandated to one area of the Apple ecosystem in the belief that they may allegedly favour competition in a certain way are highly likely to have knock-on effects on other parts of the ecosystem, which may ultimately harm competition or consumer choice. The ecosystem should be analysed and understood as a whole. Apple is keen to engage proactively with the CMA to avoid any such inadvertent negative consequences being made more likely through the findings of the market study.

7. Apple is keen to assist the CMA to develop a proper understanding of how its ecosystem is designed and operates, and will do so by addressing the allegations set out in the Statement of Scope in its responses to the CMA's requests for information. Apple is confident that that a proper understanding of its business model will demonstrate that its activities are pro-competitive and pro-consumer. However, in this submission, Apple addresses a number of issues that are critical to understanding Apple's business model.

B. Apple's Detractors Misrepresent the Fundamental Business Relationship Between Apple and Developers and Challenge Standard Business Terms

8. Many of the CMA's concerns appear to be underpinned by arguments from a select few developers and organisations that Apple has, and is attempting to exploit, market power in relation to app distribution and that it is somehow stifling competition. In fact, the industry is characterized by increasing output (e.g., developers, apps, downloads, billings) and continuous reductions in price (e.g., app store commissions), both indicia of a highly competitive market. As set out above, Apple is confident that the CMA's investigation will bear this out.

9. Nonetheless, it is important for the CMA to understand from the outset that what these detractors are arguing for is a fundamental overturning of the commercial relationship between Apple and developers. The essentials of this relationship have been clear from the outset: if a developer charges for software purchased in the App Store, it pays a commission to Apple. If a developer offers its software for free on the App Store or adopts a business model that depends entirely on advertising, or when it benefits from the Reader Rule or Multi-platform Rule, it pays no commission to Apple. As Steve Jobs explained in 2011: "*Our philosophy is simple – when Apple brings a new subscriber to the app, Apple earns a 30% share; when the publisher brings an existing or new subscriber to the app, the publisher keeps 100% and Apple earns nothing.*"[2]

10. These commercial terms were significantly more favourable than other platforms were offering when the App Store launched, when the App Store unquestionably lacked market power over the distribution of software applications. Today, competing platforms charge the same commission as Apple, or more. Over time, Apple has fostered growth and competition on the App Store by allowing certain categories of apps or developers to pay a reduced commission (e.g., 15% for subscriptions beginning in year 2; the Small Business Program). These exceptions are applied equally to all developers. Further, Apple has gone out of its way to facilitate developers' access to iOS users through alternative platforms, in particular through the Reader Multi-Platform Rules, which allow users to access digital content purchased outside of the app through an iOS app.

[2] Apple Press Release, Apple Launches Subscriptions on the App Store (15 February 2011).

11. What must be understood, however, is that the App Store is not a generic utility for third parties to exploit however they please on whatever terms they please, no matter how loudly a small number of disgruntled developers seeking to improve their own profits object. Apple has invested billions of dollars and years of development work to bring iPhones and the App Store to market and constantly improve them. In return, Apple charges a commission for the sale of digital content (i.e. digital goods and services which exist entirely within the four corners of the iPhone and Apple's developer tools) through the App Store, which is how Apple earns a return on this investment. The commission is collected through IAP. Despite some adjustments in wording, the principles of the IAP mechanism has remained unchanged overtime.

12. Apple applies an "Anti-Circumvention Rule" to ensure that developers do not free-ride on its enormous investments by deliberately encouraging customers to circumvent IAP within the app. Apple does not apply any general marketing restriction and app developers are entirely free to advertise their services as they see fit. The narrowly tailored anti-circumvention rules seek to address in-app communications intended to re-direct iOS customers to purchase content and services outside of the App Store. These are standard business terms, and they are no different than the policies of virtually any other retailer, both brick-and-mortar or online. No retailer, for example, would allow Apple to include messaging on the boxes of Apple products sold in its stores or on in-store signage encouraging its customers to purchase the iPhone at the nearby Apple Retail Store or allow a customer to walk out of its store with an Apple product so they may pay for it separately on the Apple Online Store.

13. Apple's detractors ignore these fundamental business realities and purport to use competition rules to overturn Apple's approach to IAP and the App Store. It is vital that the CMA recognises the self-serving, commercial interests behind many of the concerns raised by third-parties. As with any other store, digital or physical, suppliers should not be entitled to force their products onto the shelves without abiding by reasonable rules, or pay only what the supplier decides to pay; the mere fact that Apple is a large and profitable company - or that, thanks to its commitment to innovation, consumers like Apple products and purchase them repeatedly - does not mean that Apple should be subjected to such tactics.

C. The Role of Sideloading Prevention in the Apple Ecosystem

14. One point that Apple considers critical for the CMA to appreciate from the outset is that in order for the Apple ecosystem to continue to deliver the extraordinary benefits to consumers and developers that have been seen since the launch of the iPhone in 2007, Apple must balance the benefits and value of providing third-party developers access to the iOS ecosystem with the need for reliability, safety, security and privacy that Apple's customers value so much.

15. An example of this is "sideloading." Apple does not allow sideloading of apps onto its devices. The SoS sets out concerns that Apple may be using this to exploit consumers or app developers and/or to "entrench its market power in the distribution of mobile apps". Whilst the CMA notes in passing that Apple's restrictions "may also have some beneficial impacts in terms of security", the reason for Apple's sideloading restriction appears not to be fully understood or appreciated.

16. Sideloading is a recognized security threat:

> "*Use the official application marketplace only. Users should … not [download applications] from third-party sources, to minimise the risk of installing a malicious application. Users should not sideload applications if they do not originate from a legitimate and authentic source.*"
> European Union Agency for Cybersecurity (ENISA), 2016

> "*The best practices identified for mitigating threats from vulnerable apps are relevant to malicious and privacy invasive apps. Additionally, users should avoid (and enterprises should prohibit on their devices) sideloading of apps and the use of unauthorized app stores.*"
> U.S. Department of Homeland Security Report, 2017

17. Apple has always been focused on ensuring that the iPhone is as secure as possible to avoid the experience with personal computers where malware, viruses, security and interoperability were a continuous challenge. And it has succeeded in this enterprise so far to a very large extent. This is vital given the breadth of applications covered by the iPhone, which contains a wealth of private and sensitive data to an extent that far exceeds computers, including photos, contact details, location-data, activity data, credit card information, usernames and passwords health information and personal correspondence. As Apple has stated:

> *Today, our phones are not just phones; they store some of our most sensitive information about our personal and professional lives. We keep them with us wherever we go, and we use them to call and text with loved ones, take and store photos of our children, give us directions when we're lost, count our steps, and send money to friends. They are with us in happy times, and in times of emergencies.*[3]

18. The large size of the iPhone user base would make an additional appealing and lucrative target for cybercriminals and scammers. Allowing sideloading would spur a flood of new investment into attacks on the platform. Malicious actors would take advantage of the opportunity offered through additional distribution channels by devoting more resources to develop sophisticated attacks targeting iOS users, thereby expanding the set of weaponized exploits and attacks – often referred to as a "threat model" – that all users need to be safeguarded against. Key risks that users would face are:

    - Exposure to scammers who exploit apps to mislead users, attack iPhone security features, and violate user privacy. This can be seen on other platforms: some Android apps aimed at children were discovered to be engaging in data collection practices that violated privacy and, despite being removed from the Google Play Store, are still available and targeting Android users on third-party app stores.[4]

    - Exposure to "ransomware" that locks users out of their phone or targets their photos, unless they agree to pay a ransom. Examples of ransomware that have been found on Android include:
        i. fake versions of apps like Netflix and Candy Crush that, if installed, can spy on Android users via the microphone, take screen shots of their devices, view location, text

[3] See: https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf.

[4] See https://techcrunch.com/2020/10/23/google-removes-3-android-apps-for-children-with-20m-downloads-between-them-over-data-collection-violations/#:~:text=The%20three%20apps%20in%20question,the%20violations%20to%20its%20attention.

messages and contacts, steal users' login credentials, and make changes to users' phones[5] or even steal banking details.[6]

ii. an app masquerading as a COVID-19 contact tracing app that, if installed, encrypts all personal information, leaving an email address to contact if the user wants to rescue their data.[7]

- Reduction in the utility of important features such as Ask to Buy, a parental control feature that allows parents to control their children's app downloads and in-app purchases, and Screen Time, a feature to manage their and their children's time with their devices. Malicious developers would have the opportunity to mislead children and parents by obfuscating the nature of their apps, making both features less effective.

19. This increased risk of malware attacks puts all users at greater risk. The App Store is designed to detect and block today's attacks, but changing the threat model would bypass these protections from more sophisticated attacks. Scammers would then use their newly developed tools and expertise to target third party stores as well as the App Store, which would put all users at greater risk, even those who only download apps on the App Store. Allowing sideloading would open the door to a world where users may not have a choice but to accept these risks, and scammers could trick users into thinking they are safely downloading apps from the App Store when that is not the case. This latter point is important, as arguments that users can make an informed choice simply ignore the fact that a large proportion of users are not in a position to make authoritative decisions as to whether an app available via a link they have received is downloadable from the App Store or some other location deliberately intending to infect a user's device.

20. In addition, developers would become more vulnerable to threats from malicious actors who could offer infected developer tools that contain and propagate malware. Developers would also be more vulnerable to piracy, undermining their ability to get paid for their work. Third-party sources indicate that app piracy, where "pirates steal a mobile game or app, insert ads from an ad network account that pays them -- not the original owners -- publish the app to a third-party app store, and sit back to enjoy their stolen treasure", cost developers billions of dollars in revenue each year.[8]

21. More generally, users who are worried about their security and privacy are more likely to download fewer apps or to delete apps.[9] A less secure ecosystem, in which users do not feel safe downloading apps, could mean users are less likely to try out innovative new apps or take a chance on apps coming from new or lesser-known developers. This could blunt the growth of the app economy, further harming developers and depriving users of choice.

---

5 See https://www.welivesecurity.com/2021/03/18/beware-android-trojan-posing-clubhouse-app/; https://www.zscaler.com/blogs/security-research/spynote-rat-posing-netflix-app

6 See https://www.zdnet.com/article/this-android-trojan-malware-is-using-fake-apps-to-infect-smartphones-steal-bank-details/

7 See https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

8 See https://www.forbes.com/sites/johnkoetsier/2018/02/02/app-publishers-lost-17-5b-to-piracy-in-the-last-5-years-says-tapcore/?sh=bb718b474139

9 See https://www.jpmorgan.com/merchant-services/insights/reports/Japan-2020; https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-risk-privacy-index-150519.pdf;

22. Apple takes a multi-layered approach to security to protect iOS users from malicious apps and provide the world's best platform security.[10] This approach is significantly more effective than Android, which allows third-party app stores and sideloading. Indeed, the Nokia Threat Intelligence Report 2020 finds that devices that run on Android had 15 times more infections from malicious software than iPhone, with a key reason being that Android apps "can be downloaded from just about anywhere" unlike the iPhone.

23. Further, Apple's approach to security is an important competitive differentiator, providing a genuine choice to users who are concerned about the security of their devices and consider it important to limit the opportunities for malware and harmful and malicious apps to find their way onto their devices.

24. In light of the above, Apple is keen to emphasize that, as the CMA carries out its market study and considers whether remedial action may be warranted, it should therefore be aware of the very significant potential consequences on user welfare, developer opportunities, and consumer choice that sideloading poses.

D. Privacy

25. The CMA proposes "to explore whether Apple and Google are taking on quasi-regulatory functions within their ecosystems and may be setting the rules in relation to matters such as privacy and user security in ways that advantage themselves over their rivals." In this area also, the SoS refers to ill-founded complaints from well-known Apple detractors. Whilst the CMA notes that Apple's actions to reduce consumer tracking across companies may also have beneficial impacts in terms of user privacy, as many stakeholders and regulators recognize,[11] Apple's efforts with respect to privacy do not appear to be fully appreciated.

26. Since even before the introduction of iPhone and across all product categories, Apple has adopted an approach of "privacy by design", which reflects Apple's stance to respect user privacy. Apple's belief is that users should not be subjected to invasive data collection practices without their knowledge or consent. Whilst Apple's detractors claim that Apple could change its practices in the future and reduce its privacy protections, the reality is that the protection of users' privacy is wholly embedded within Apple's DNA and its brand. As Apple frequently emphasizes in public statements: *Privacy is a fundamental human right*.[12]

27. As a result, 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. Importantly, given the importance of privacy as a core value,

---

[10] A summary of this multi-layered approach can be found in: https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf

[11] For example, the French Data Protection Agency (the Commission nationale de l'informatique et des libertés or "CNIL") has stated that ATT can be of genuine benefit to both users and app publishers. In its opinion, the ATT prompt "would give users more control over their personal data by allowing them to make their choices in a simple and informed manner … and by technically and/or contractually preventing app publishers from tracking the user without their consent" (Deliberation n° 2020-137 of 17 December 2020 of CNIL in the context of the complaint filed by certain online advertising professional associations against the company Apple Inc. before the Autorité de la concurrence).

[12] https://www.apple.com/privacy/

Apple applies the same high privacy standards, or higher privacy standards, to itself as to third-party apps. Apple's position is simple: If Apple does not require data, Apple processes it on user devices exclusively; if data is needed to make a service work, as much as possible Apple associates the collection with random identifiers and not the user's identity. For example:

- Apple Maps associates user data with random rotating identifiers and not the user's Apple ID, and Apple doesn't keep a history of where users have been;
- Apple's Photos app uses machine learning to organise photos on the device, so the people, places and things that users search for are not shared with Apple;
- On Messages, every blue-bubble message, picture, Animoji and video is encrypted while being sent between devices and smart suggestions in Messages, like pulling up photos to send based on who the user is messaging, are all done on the device and not in a way that Apple can see unless the user stores the photos in iCloud;
- Siri was designed from the beginning in 2011 to associate the things that users said to Siri with a random identifier and not their Apple ID. In recent years, Apple has added many Siri functions, such as reading messages and contacts, solely on user devices.
- For ApplePay, Apple doesn't store credit or debit card numbers or share them with merchants. Instead, a unique Device Account Number is created every time a user adds a card to Apple Pay.

28. Apple has introduced significant innovations over the years, including Touch ID, Face ID, keychain and password innovations; all of which are aimed at improving the security of devices and the information held on them. Similarly, in 2019, Apple introduced "Sign in with Apple." This feature allows users to securely log-in to apps and websites in one click while also "hiding" their real email addresses from developers if they choose, reducing the ability of third-party sign-in services to track and share users' personal data, and Apple also does not track users' activity in the app or website. In fact, Apple does not collect such activity at all. Apple only has a record of the apps and websites that a user has chosen to connect to via Sign-in with Apple, and that is simply to allow the user to disconnect if they choose.

29. A key concern from a data privacy perspective is the extent to which consumers' data is collected, combined, and mined to a degree that few can understand or have predicted. Many consumers simply do not know about the maze of hidden practices companies use to collect vast volumes of data. Apple has tried to educate users about the invasive nature of such data collection practices by publishing a report titled "A Day in the Life of Your Data," which describes how companies build and harvest extensive data profiles of users through "tracking."[13]

30. Tracking of users frequently occurs without their knowledge or consent. Companies can combine user-specific data collected from different entities and mine the aggregated data to generate targeted advertisements and advertising measurement – all without the user ever knowing it. Sometimes the data is aggregated and resold by data brokers, who are third parties the user has never interacted with, or even heard of. Tracking can be highly invasive and often takes place without meaningful user awareness or consent. Whilst Apple is not opposed to all forms of data-aided advertising, it operates under the principle that tracking should be done in a transparent manner and under the user's control. This is what Apple gives users.

[13] The report is available here: www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf

31. In 2020, Apple introduced two new initiatives:
    - **Privacy nutrition labels**. Apple launched "privacy nutrition labels" in the App Store. These labels provide users with information about how an app tracks, collects, and uses data, similar to the way nutrition labels list ingredients and caloric content of food. Industry observers have praised this feature as "good for users, developers and the enterprise" and noted that it helps developers who collect and handle data responsibly compete more effectively against those that seek to exploit users' data.[14]

    - **App Tracking Transparency.** Apple also announced and has now implemented the App Tracking Transparency ("ATT") feature. ATT gives users the ability to choose whether to allow a developer to track their activity across other companies' apps and websites or not by using the identifier for advertisers ("IDFA") or other similar means. This innovation empowers consumers by presenting them with information about their privacy options and giving them the power to choose. ATT was welcomed by numerous developers[15] and a broad range of organisations. For example, the Brookings Institute welcomed the move and noted that it was "time to create more tools and legal protections that enable individuals, the creators of data, to decide for themselves how it is used".[16]

32. As with other privacy features, with ATT, Apple holds its own services to at least the same standard of data protection and user privacy as it requires third-party app developers to follow. The ATT requirement applies to all apps equally, including Apple's own apps. If Apple's apps do not display the ATT prompt, that is only because Apple does not track users across different companies' apps or websites or access their IDFA. Apple serves ads in the App Store, on Apple News and in Stocks. In doing so, Apple does not access user data from Apple services like Apple Pay, Maps, Siri, iMessage, and iCloud. Like many developers, Apple may use first party data to provide personalized ads. But Apple goes further by holding itself to a higher standard: Apple's advertising platform is limited from using even first-party information about the user for ad personalization if Personalized Ads is turned off on the user's device. Many developers do not offer this choice to their app users. Apple's advertising platform may use account information and purchase and download history to serve relevant search ads in the App Store. In Apple News and Stocks, ads may also be generated based on what a user has read or followed in Apple News. Furthermore, as set out above, such reading activity is tied only to a random identifier and not to a user's Apple ID or IDFA.

33. Apple's approach to targeted ads demonstrates that privacy-focused advertising is possible when companies put user control at the forefront. The ATT prompt reflects Apple's principled dedication to privacy innovations, and, in that respect, is no different than the other iOS-based permissions that allow a user to control an app developer's access to their photos, contacts, calendar and location.

---

[14] See e.g. https://www.computerworld.com/article/3600998/apples-privacy-nutrition-labels- available-now-and-good-for-business.html

[15] See https://www.youtube.com/watch?v=oN_kacGveQE; https://www.cnbc.com/2021/02/05/snap- ceo-spiegel-says-apples-iphone-privacy-change-is-good-for-consumers.html

[16] See https://www.brookings.edu/techstream/the-disturbing-implications-of-increasingly-narrow- political-ad-targeting/

E. Conclusion

34. Security and privacy are two sides of the same coin. They are intertwined in that security controls dictate the level of privacy enforced, and privacy technologies can promote a higher degree of security. For the reasons discussed above, in section C, therefore, changes that reduce the level of iOS security would also likely degrade users' privacy. It would also reduce consumer choice by removing the possibility for consumers to select devices and systems that offer a level of privacy protection suited to their needs. Apple again requests that the CMA bears this in mind as it carries out the market study.

* * * *