February 7, 2022

KPAW's observations on the Interim Report of the CMA's Market Study on Mobile Ecosystems

I. Introduction

KPAW is grateful for the opportunity to share its views on the Interim Report of the Mobile Ecosystems Market Study ("**Interim Report**"), published by the Competition and Markets Authority ("**CMA**") on 14 December 2021.

KPAW would like to congratulate the CMA for its extremely thorough investigation of the Apple and Google mobile ecosystems, as well as the challenges faced by app developers when dealing with these gatekeepers. **Many of the findings made in the Interim Report with respect to Apple's anticompetitive practices are in line with KPAW's experience with Apple and its App Store.** As we have not dealt with Google, our submission will focus on Apple and builds on our earlier submission made to the CMA in April 2021.

Our observations on the Interim Report are divided in eight sections. **Section II** introduces KPAW and its leading app FlickType. **Section III** summarizes KPAW's April 2021 submission. **Section IV** argues that Apple's claims that alternative distribution mechanisms should not be allowed for security reasons should carry no weight as they are exaggerated and pretextual in nature. More competition in the market for app distribution is needed. **Section V** discusses FlickType's experience with the App Store review process. **Section VI** explains that Apple's access to APIs is discriminatory. **Section VII** explains why KPAW strongly supports the interventions suggested by the CMA to address the concerns expressed in this submission. Finally, **Section VIII** concludes.

II. KPAW and its leading app FlickType

KPAW is a California-based company operated and co-owned by Ashley and Kosta Eleftheriou. Mr. Eleftheriou has solid experience in developing and launching successful apps since the very beginning of the App Store. For instance, he developed the iSteam app, with over a million downloads in its first week on the App Store and generating more than $100,000 in its first three months. He later developed a revolutionary smartphone typing technology called "BlindType", which enabled users to type on touchscreens without even looking at their screen and was acquired by Google. Between 2011 and 2016 he developed "Fleksy", an alternative text input system with millions of downloads later acquired by Pinterest.

KPAW's most important app is **FlickType** developed in 2018. FlickType provides an accessible keyboard for Apple's mobile devices and the Apple Watch. The app allows the user to quickly type text messages by using keyboard algorithms to ensure correct, predictable, and reliable typing results, something not previously possible on the Apple Watch. **FlickType has been**

designed to accommodate the special needs of low vision users. The press praised the FlickType app. For instance, Forbes mentioned that "… *FlickType provides an extra way to respond that is simple, enjoyable and highly effective.*"[1]

FlickType is based upon a freemium business model. The app can be downloaded for free, and to access extended premium features the user needs to make a one-time purchase via Apple's In-App Payment system ("In-App-Purchase" or "IAP"). With respect to FlickType, Apple took the stance that the service constitutes a digital service consumed within the app, and is thus subject to IAP. Where an app developer is required to use IAP to accept in-app payments, it must pay Apple a 30% commission on the transaction value, the so-called IAP commission.

Interestingly, on 14 September 2021 Apple announced the new Apple Watch Series 7, which now includes a built-in keyboard for the first time – a feature that was shown prominently during their keynote video. It thus now appears that ever since attempting to launch a watch keyboard and getting repeatedly rejected, **FlickType was also competing with Apple's own planned Apple Watch offering** – which was certainly under development at the time. This is a further example of "**Sherlocking**", the phenomenon of Apple releasing a feature that supplants third-party software it has shamelessly copied.[2]

III. KPAW's submission of April 2021

KPAW made a submission to the CMA in April 2021 after it learned that the CMA had decided to investigate Apple's App Store practices.[3] We thought that the struggle of a small app developer to have its innovative app distributed on the App Store would assist the CMA investigation.

In our April 2021 submission, we explained that:

- **FlickType experienced significant difficulties and delays in its dealings with Apple and in particular Apple's App Review process**, which is incredibly opaque and arbitrary with Apple authorizing itself to block apps developed at great expense based on vague or unwritten rules. Apple's review system lacks the most elementary form of due process, with apps being rejected through cryptic messages which automatically disappear when Apple considers that the matter has been "resolved". Apple's conduct resulted in a year-long delay before FlickType was finally permitted to launch its watch keyboard app.

---

1 David Phelan, "Apple Watch FlickType Gesture Keyboard App Makes Typing A Breeze: Is It Any Good?", *Forbes*, 2 March 2019, available at https://www.forbes.com/sites/davidphelan/2019/03/02/apple-watch-flicktype-gesture-keyboard-app-makes-typing-a-breeze-is-it-any-good/ (last accessed: 1 April 2021).

2 See, e.g., Whilliam Gallagher, Apple strikes again: Which developers got 'Sherlocked' at WWDC, Apple Insider, 8 June 2021, available at https://appleinsider.com/articles/21/06/08/apple-strikes-again-which-developers-got-sherlocked-at-wwdc

3 Investigation into Apple AppStore, 4 March 2021, available at https://www.gov.uk/cma-cases/investigation-into-apple-appstore

- Contrary to the justification Apple regularly uses to explain why it does not tolerate alternative distribution mechanisms on iOS devices and why it charges a hefty 30% commission, **the App Store is neither secure nor app developer friendly**. While it blocks well-functioning, innovative, and safe apps for long periods of time, it allows a wide variety of fraudulent apps on the App Store whose visibility is boosted by thousands, or even tens of thousands of fake reviews. Even when Apple is warned of such scam apps, Apple takes a long time or in some cases does nothing to remove them from the App Store, hence hurting genuine apps and exposing iOS users to fraud. In fact, scam apps competing with FlickType have generated over $1,000,000 to date and are still negatively impacting KPAW's business.

- While Apple claims that it treats all app developers equally, KPAW's experience is that it does not. While KPAW's FlickType app was rejected by Apple because the Apple Watch was allegedly not intended to be used as a keyboard, competing apps offering this feature were admitted to the App Store, including apps integrating FlickType's own technology. **This behaviour is not only discriminatory, but it also now appears exclusionary since Apple is now offering its own keyboard for the Apple Watch.**

The present observations will not repeat our April 2021 submission, but engage with the findings made by the CMA in the Interim Report.

IV. Apple's claims that alternative distribution mechanisms should not be allowed for security reasons should carry no weight

Apple's favourite argument to discourage regulators from taking measures that would loosen its grip on its ecosystem is that **such measures would harm the security of its devices and of its iOS users**.

While app developers care about security (as an insecure ecosystem would negatively impact their user base and thus their ability to generate revenues), Apple's security claims should be taken with scepticism for the following reasons.

First, **it would be wrong to assume that Apple's ecosystem is necessarily safe**, and that the App Store review process does a good job weeding out bad apps. As shown in our April submission, the App Store contains many scams that are taking advantage of iOS users, and even when Apple is made aware of the presence of these apps, it often takes months or even years for Apple to exclude them from the App Store – or worse, it does nothing. The sad reality is that because these apps charge extortionary amounts from users, they are also profitable for Apple. For instance, as has been reported in the press, Mr. Eleftheriou recently identified a music app named AmpMe, which has an in-app purchase that enables a $10 per week subscription that runs $520 per year, with the business built around thousands of fake App Store reviews.[4] The app remains available despite the company publicly admitting that its App

[4] Oliver Haslam, Scam app AmpMe rakes in $13 million on the back of thousands of fake reviews, iMore,12 January 2022, available at https://www.imore.com/scam-app-ampme-rakes-13-million-back-thousands-fake-reviews; Sarah Perez, Music app AmpMe lowers pricing after accused of being an App Store

Store page is filled with fake reviews. AmpMe has generated over $13,000,000 on the back of such fraudulent practices, but it is only one of many examples of scams[5] that routinely make their way to the App Store, despite Apple's claim that its restrictions on sideloading and alternative app stores are necessary to protect iOS users from cybercriminals. In fact, by continuously touting the App Store as trustworthy and safe[6], Apple is giving users a false sense of security – thus making them much more susceptible to scams than they would otherwise be. Based on our extensive research, we estimate that **fraudulent App Store revenue amounts to billions of dollars**.

Second, even if Apple's app review process was flawless, which it is not, **there is no reason to believe that alternative app distribution mechanisms are necessarily insecure**:

- **Sideloading is not necessarily insecure**. After all, sideloading is allowed on Apple Mac computers, which Apple touts as extremely safe[7], and **there is no reason why Apple's automated "notarization" screening process which ensures users download safe apps on macOS cannot be extended to iOS.**[8] Additionally, under this process, iOS can remain significantly more secure than macOS. Mac computers can optionally run apps with escalated "root" privileges, which is specifically what most malware relies on – but such option is not necessary on mobile devices, thus security would not be compromised. If Apple considers that this process is not sufficiently secure, which is hardly credible considering that it was satisfied with it until such time these practices became subject to litigation and investigation, it should aim at improving it.

- **Alternative app stores are not necessarily insecure**. **Nothing would indeed prevent Apple from imposing security standards to app stores wishing to be made available on the App Store.** As Apple relies on an extremely wide range of suppliers (including for the processing of payments made via its in-app payment solution, IAP, as Apple itself is not a payment processor), it must be able to impose security standards on them, which in case of non-compliance would lead to the exclusion of their app store from iOS. It seems hard to believe that third-party app stores are by essence incapable of doing a good job.

Third, there is good reason to believe that the introduction of alternative app distribution mechanisms would **stimulate innovation in privacy and security features**. Apple does not

---

scammer, 12 January 2022, available at https://techcrunch.com/2022/01/12/music-app-ampme-lowers-pricing-after-accused-of-being-an-app-store-scammer/

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

6 App Store: "The apps you love. From a place you can trust." available at https://www.apple.com/app-store/

7 macOS Security: "Now apps from both the App Store and the internet can be installed worry-free." available at https://www.apple.com/macos/security/

8 See Notarizing macOS Software Before Distribution, available at https://developer.apple.com/documentation/security/notarizing_macos_software_before_distribution

have the monopoly of knowledge, and as noted above, its own App Review process has glaring flaws.

For these reasons, Apple should have the burden of proof to show that the restrictions on alternative methods of iOS app distribution that Apple justifies on the grounds of security and privacy are not only strictly necessary, but also proportionate to the objective pursued.

V. The App Store review process

As we explained in our submission of April 2021, FlickType's experience with the App Store review process has been horrible:

- First, this process is not only **slow and cumbersome, but it is inconsistent**. FlickType was successfully accepted in the App Store, to then be suddenly taken down, repeatedly rejected for months, and accepted again without any reason.

- Second, the App Review process is **discriminatory**. While FlickType was repeatedly excluded from the App Store, other competing apps, as well as third-party apps using FlickType's own technology, were accepted by Apple – something KPAW even repeatedly brought to Apple's attention. This illustrates the lack of consistency in Apple's review process.

- Third, there is a **total lack of due process**. If an app developer disagrees with the outcome of the app review process, it may submit an appeal before the App Review Board, which also consists entirely of Apple employees. Reviews and appeals are handled through an electronic channel, with developers having little or no visibility in the process.

Thus, we are not surprised when the Interim Report observes:

> "With regard to Apple, the majority of developers that we requested information from had negative experiences with the app review process. Developers variously described Apple's app review process as 'obscure', 'arbitrary', 'capricious' and 'kafkaesque'."[10]

The adjectives used by other app developers to describe the review process are completely in line with FlickType's.

We also agree with the Interim Report when it concludes that:

> "Apple's operation of the app review process for the App Store, in particular its inconsistent interpretation of rules and lack of clear explanation of reasons for rejections, creates uncertainty, costs, and delays for app developers. This in turn is liable to hinder innovation and **may be used to the advantage of Apple's own apps**.

[10] Interim Report, section 6.60.

> We do not see any reason that such concerns should necessarily arise from an app review process aimed at ensuring quality and security."[11]

The fact that the app review process can be used to favour Apple's own apps is illustrated by the fact that while Apple was rejecting apps for pretextual reasons, it was working on its competing offering. This is manifestly the case when we see the reasons that were invoked by Apple to reject FlickType:

24 January 2019: *We noticed your app does not satisfy the requirements outlined in the Apple iOS Human Interface Guidelines. Specifically, the app is a keyboard for Apple Watch. For this reason, your app will be removed from sale on the App Store at this time.*

4 March 2019: *Your Apple Watch app is only a keyboard and did not have have pre-loaded content.*

30 March 2019: *We noticed an issue in your app that contributes to a lower quality user experience than Apple users expect: Specifically, your app uses Apple Watch as a keyboard which is not an intended use of Apple Watch.*

12 April 2019: *Upon further review, your app was found to be out of compliance with App Store Review Guidelines 4.0. Specifically, your app uses Apple Watch as a keyboard which is not an intended use of Apple Watch.*

15 April 2019: *As previously communicated, your app does not comply with Guideline 4.0 of the App Store Review Guidelines, which states apps should be "simple, refined, innovative, and easy to use." Full keyboard apps are not appropriate for Apple Watch. The Apple Watch and its display is not optimized or intended for full keyboard-type apps – such apps create a poor user experience and are not "easy to use." Pre-set phrases, emojis, and other quick input-type keyboard apps are permissible for Apple Watch.*

1 May 2019: *The App Review Board evaluated your app and determined that the original rejection feedback is valid. Please note that all appeal results are final.*

These pretextual objections while Apple was developing its own keyboard demonstrate that the rules Apple applies to itself are different than those it applies to others.

This confirms the need to introduce alternative app distribution channels, as competition would force Apple to be more user friendly on pain of losing apps to other channels. What is also frustrating with Apple is the poor quality of the service that is offered to app developers, considering the huge amount of revenues it generates on their back (or at least those selling digital goods or services). Like a classic monopolist, Apple keeps its commission at a supra-competitive level, while it maintains the quality of its app distribution service at a minimum level.

---

[11] Interim Report, Section 6.77 (emphasis added).

VI. Apple's discriminatory access to APIs

Although Apple regularly claims that it offers developers the same native APIs and tools that it uses internally, the reality is that **Apple places insurmountable obstacles on developers who try to compete with some of Apple's own offerings**.

In our experience, these obstacles range from providing developers with inferior tools, to **imposing artificial limitations that outright prevent developers from creating apps of equivalent quality or functionality as Apple's own offerings**. For example, Apple denies third-party keyboards critical functionality such as communicating with or using resources from their own container application, accessing the microphone, or playing custom sounds, unless the user performs a highly convoluted and misleading process to enable so-called "Full Access." Most users are unlikely to do this process due to the sheer number of steps involved and privacy warnings they receive, even if the keyboard does not require access to the network at all and poses no risk to users. Additionally, a critically useful API to request "Full Access" directly from the keyboard, as Craig Federighi demonstrated during the 2014 Worldwide Developers Conference, has never been made available. Moreover, even if the user chooses the "Full Access" option, Apple constrains third-party keyboards in other critical areas, such as in their usage of available memory, their ability to gather enough textual context to provide better predictions, their ability to be used in password fields, and their ability to show visual elements above the top edge of the keyboard. These features are essential to create a robust keyboard experience, and **none of these limitations exist in Apple's own keyboard. Thus, Apple ensures that third-party keyboards cannot compete fairly with Apple's own offering**. In fact, even when setting a third-party keyboard as default, users are frequently presented with Apple's own keyboard. As one online magazine, TechCrunch, stated: "It's almost as if Apple is trying to bury the option to play away from the native keyboard."[12]

Similarly, the APIs and tools Apple offers to developers for Apple Watch apps are notoriously slow, unreliable, and often do not work at all. However, **Apple uses special internal software and hardware tools that do not suffer from these problems**. Third-party Apple Watch apps often fail to install for end-users, resulting in developers getting blamed for the issues through negative ratings on the App Store. Apple's own apps do not suffer from failed installations or negative ratings, because Apple preinstalls its own apps on the Apple Watch, and up until a few months ago Apple prevented their own apps from being rated on the App Store. Apple also provides no analytics data for third-party Apple Watch apps. As a result, developers cannot track some of the most basic metrics of their apps, such as engagement, retention, and crash rates. But Apple can track metrics for its own apps to evaluate the impact of product changes and guide future product decisions, and can even track metrics for all third-party apps.

---

[12] Natasha Lomas, Everything You Need To Know About iOS 8 Keyboard Permissions (But Were Afraid To Ask), Tech Crunch, 4 October 2014, available at https://techcrunch.com/2014/10/04/everything-you-need-to-know-about-ios-8-keyboard-permissions-but-were-afraid-to-ask/.

We therefore share the CMA's concern that Apple's "*restrictions on access to APIs may give a competitive advantage to [its] own apps and services*."[13]

VII. Interventions

One of the most valuable parts of the Interim Report is that it proposes a range of interventions to address the concerns it has identified when it comes to Apple and Google's practices.

Our observations hereafter focus on the interventions that would best address the concerns we have expressed above, i.e. those of a small app developer that has struggled to have its app distributed on the App Store.

Remedy area 1: interventions relating to competition in the supply of mobile devices and operating systems

In this area, the CMA proposes various interventions to inject competition between mobile ecosystems, in particular by facilitating switching between them. Now, whatever the nature of the measures adopted, it is likely that most users will remain loyal to their ecosystems, which often extend well beyond their mobile device. In particular, we do not anticipate that the reduction of barriers to switching would induce enough iOS users to switch to Android devices.

What is important for app developers like us is to have the opportunity to compete fairly on the App Store with other apps, including Apple's own apps. For many developers the App Store remains the most attractive venue, as iOS users typically have greater purchasing power and thus have a greater capacity to make in-app purchases. According to Sensor Tower research, users spent $133 billion on apps in 2021, with Apple's App Store alone accounting for over $85 billion of this market.[14]

Remedy area 2: interventions relating to competition in the distribution of native apps

Under remedy area 2, the CMA is considering requiring Apple to (i) allow alternative app stores on iOS devices (currently prohibited); (ii) allow sideloading of native apps on iOS (also prohibited); and (iii) support web apps on iOS (currently severely limited).

We support these interventions because we consider that **greater competition in app distribution on iOS devices will force Apple to deliver a better service to app developers (e.g., in terms of a more efficient and fair app review process) and hopefully to lower its fees**. In addition, we consider that Apple's security justifications to keep their grip on the app distribution market are pretextual and overblown, especially considering that Apple already offers safe sideloading on macOS, and Apple's efforts to weed out App Store scams have proven insufficient for over a decade. To the contrary, we think that additional competition

---

13 Interim Report, Section 6.27.

14 See https://9to5mac.com/2021/12/07/users-spend-133-billion-with-apps-in-2021-app-store-has-higher-revenue-than-google-play/

will stimulate innovation in fraud detection, resulting in a meaningfully better service for both developers and users.

Remedy area 4: interventions relating to the role of Apple and Google in competition with app developers

Under this area, the CMA is exploring interventions relating to the role of Apple and Google in competition with app developers.

We are strongly supportive of interventions aiming to constrain the ability of Apple to harm fair competition through the operation of its App Store. In particular, **we support measures designed to ensure that Apple does not unreasonably restrict third-party access to its APIs and implements a fair and transparent review process**. As long as the App Review process is conducted in an opaque, arbitrary, and discriminatory manner, competition between Apple's apps and third-party apps will be impeded, and the CMA's effort to open competition within the Apple ecosystem will come to naught.

In this respect, we strongly support the operational separation between Apple's app development business and its App Store activities, including their review process. In the absence of such separation, Apple will retain the ability and its incentives to discriminate third-party apps to the advantage of its own apps.

VIII. Conclusions

KPAW once again commends the CMA for its extraordinarily detailed assessment of the Apple and Google mobile ecosystems. We strongly support interventions designed to stimulate competition in these ecosystems, with a particular focus on the Apple App Store. While Apple has turned the App Store into a cash cow, the quality of services it delivers to both users and app developers – such as app review and policing of scams – have been not only below par, but frankly detrimental in many respects for far too long.

****