ACT | The App Association feedback to the United Kingdom Competition and Markets Authority's consultation on the statement of issues regarding the mobile browsers and cloud gaming market investigation

About ACT | The App Association

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. App Association members are located around the world, including the UK, all 27 member countries of the European Union, and all 435 congressional districts of the United States, showing that with coding skills and an internet connection, an app maker can succeed from anywhere.

I. Comments on industry background and scope

The App Association welcomes the opportunity to provide comments to the Competition and Market Authority's consultation on the statement of issues relating to its market investigation into mobile browsers and cloud gaming. In its analysis concerning the suspected features of concern in the supply of mobile browsers and cloud gaming in the UK, the CMA covers a broad range of potential barriers to competition. We are concerned that parts of the CMA's analysis seem to ignore important perspectives.

We consider the scope of the statement of issues sufficient. Covering the supply of mobile browsers and mobile browser engines and the distribution of cloud gaming services through app stores on mobile devices (and supply of related ancillary goods and services) makes it appropriate to exclude desktop browsers and cloud gaming on other devices such as consoles and computers.

II. Comments on the CMA's hypotheses or theories of harm

One of the concerns the CMA lists is that both Google and Apple have high shares of supply in mobile browsers and browser engines in their mobile ecosystems. We note that market share alone does not equal abuse of market power. Thus, the CMA should focus on actively anti-competitive behaviour in its analysis. What looks like competitive constraints, e.g. Apple's requirement that other browsers on its iOS operating system use WebKit, may be beneficial for consumer privacy and business users' security, as well as making it easier for small businesses to develop web apps or in-app browsers. The WebKit requirement means that smaller app development companies only need to develop for one browser engine, rather than for several different ones. This ability puts them on a level playing field with bigger companies that potentially have the resources to develop their applications for various browser engines. Further, considering the role of pre-installation and default settings, we point out that consumers reasonably expect phones to come with default settings and pre-installed apps. Apple and Google both develop

several apps that are not pre-installed on devices but available for download from platforms. We also note that is now easier to uninstall pre-installed apps and change default settings.

The CMA's preliminary analysis also states that Apple and Google may be able to use their market power in mobile browsers and browser engines to reinforce or strengthen their position in advertising and are likely to retain this market power without intervention. Without a thorough investigation, we believe this is hard to predict and such mere assumptions should not trigger broad interventions that could disrupt the market overall. Additionally, we are concerned by the CMA's notion that Apple has the incentive to undermine the ability of cloud gaming providers to access iOS users to retain its market power in native app distribution on iOS. This statement seems to ignore the strong incentives Apple has to want to provide the best possible user experience for its device and app store users. If Apple device users truly face inferior experiences compared to those of Android device users when browsing or using cloud gaming services, they will most likely switch to another device. Similarly, while device sales are important for Apple, it seems unlikely that an increase in cloud gaming popularity would decrease the importance of high-quality mobile devices. Consumers want high-quality mobile devices for other reasons, such as camera functions, which apps are available, and the speed of the device.

While we agree that web apps have the potential to disrupt or challenge the status quo for native app distribution, we note that the current development and usage of web apps are mostly complementary to native apps. They are not a dying non-alternative to mobile native apps. Web apps fulfil an important role in offering choices for different situations and preferences. Popular app makers like Meta, Airbnb, and Alphabet offer both a web and a mobile version of their app(s), and different users can use them interchangeably.

III. Comments on potential remedies

Generally, our members are likely too small to be *directly* affected by solutions the CMA may choose to resolve any anti-competitive behaviour that may exist in the supply of mobile browsers. However, we note that any remedy the CMA introduces should explicitly consider SMEs and the indirect impact such a remedy may have on SMEs to ensure a well-intended intervention does not disadvantage them.

The potential remedies the consultation document lists could have far-reaching consequences, and we urge the CMA to consider all potentially affected stakeholders in its evaluation of the proposed actions. Removing Apple's restrictions on competing browser engines on iOS devices could, for example, make it more tedious for small developers to develop in-app browsers or web apps if they have to support several engines rather than just one to reach customers. Further, mandating access to certain functionality for browsers (including supporting web apps) and requiring Apple and Google to provide equal access to functionality through application programming interfaces (APIs) for rival browsers should consider all security implications of mandating such access. While requirements that make it more straightforward for users to change the default browser within their device settings seem reasonable, we strongly oppose

choice screens as a remedy, as we do not support giving large brands that already rely less on the benefits of the app stores an additional opportunity to get ahead of smaller developers.

We are currently seeing this play out in the Digital Markets Act (DMA) in the European Union, where Art. 6(3) requires a gatekeeper to prompt users to choose the default apps for online search engines, virtual assistants, or web browsers by offering a limited list of the most popular third-party alternatives. Such 'choice screens' give consumers the impression that only a few apps exist for a certain service when, in fact, there may be dozens or hundreds of alternatives. Unlike larger actors, small developers cannot afford to buy a spot for their apps on the list of choice screen options. They also may appear lower in rankings than larger competitors, even if they offer better services, because their apps have fewer end-user ratings. The App Association believes that the only developers that will benefit from this obligation are those large enough to be an option on the list of choice screens, making this an artificial choice for consumers. Whether fees or rankings determine the list of choice screens, such an intervention would only disadvantage small developers further or lock them out of the market entirely as they are unlikely to be included in the list of choice screen options. We urge the CMA to investigate the impact such choice screens would have on competition for small businesses.

The CMA should also thoroughly investigate the effects of requiring Apple and Google to provide greater access to functionalities, i.e. access to specific APIs and increased interoperability with their operating systems. Such a requirement may effectively allow third parties (business users) to access a device's or an operating system's core features without any kind of review. Without sufficiently strong safeguards, this remedy could unintentionally facilitate malicious third-party attempts to reach and exploit sensitive device features. Current browser engines are integrated with the OS to provide safeguards that prevent web apps from harming consumers and devices, i.e. specific features like installing an app on the home screen or allowing a website to access system functions have additional safeguards and permission prompts built into them that prevent malicious actors from taking advantage of consumers and device vulnerabilities. For example, in a poorly implemented browser engine, via access to certain APIs and functionalities of the OS, bad actors could access cameras, contact lists, or virtual private networks without end-user permission, or track other devices in the same facility and hijack the functionality of other apps, risking end users' security and privacy. Merely visiting a website through a browser engine without sufficient safeguards can execute code that could cause or create several attack opportunities on users' data and privacy. App Association members rely on the safe environment that platforms provide to keep bad actors out of the app ecosystem, gain consumer trust, and innovate. This remedy, thus, may unintentionally hurt them by making the app ecosystem less secure and decreasing consumer trust, and the CMA must investigate these potentially negative impacts.

Concerning the installation and effective use of third-party software apps or app stores on end users' devices (also known as mandated sideloading), the App Association strongly believes that this remedy would force mobile platform operators to allow unvetted sideloaded software—which could include malware, spyware, and apps that only exist to cause harm—onto consumer

devices by default. We reiterate that consumers are willing to trust the apps they download from app stores because of years of positive experiences with safe and well-functioning apps.

Unchecked sideloading would allow apps to be available for download without a thorough investigation into their inner workings, making it easier for bad actors to pirate apps or install malware on consumers' devices accessing sensitive data and sensors on the device. As a result, consumers may stop trusting apps from unknown brands, which would be devastating for smaller app developers. Reducing security and trust in the app ecosystem will only 'level the playing field' for gatekeepers and large developers that have established brands, while further widening the gap between large and small actors. Small developers who rely on the platforms to gain consumer trust and who do not have the resources to compete with the big brands will suffer. The CMA should especially monitor the practical implications of the EU's DMA implementation of sideloading obligations in its investigation of these issues.

IV. Conclusion

The App Association welcomes the CMA's interest in mobile ecosystems and supports its efforts to maintain the UK's fair and competitive digital economy. We share the CMA's ambition to preserve competitive digital markets and support the effort to identify specific market failures and assess structural issues in detail before determining policy recommendations. This path of action will help to avoid implementing remedies that would unintentionally negatively impact SMEs.

We further urge the CMA to consider security and trust implications as a priority as it continues to investigate the market for mobile browsers and cloud gaming and determines potential remedies. Without trust, consumers will not download SMEs' apps, sticking to apps from known and established brands. It is, therefore, crucial to the success of SMEs and startups that we keep out bad actors by preserving the current security environment of the app economy.

Sincerely,

Mike Sax
Founder and Chairperson

Anna Bosch
Senior Policy Associate (EU & UK)